Australian Government

Office of the Australian Information Commissioner

Privacy Act Review – Discussion Paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

23 December 2021

OAIC

Contents

Abbreviations

Term	Description
ACAPS	Australian Community Attitudes to Privacy Survey
ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ACSC	Australian Cyber Security Centre
ADHA	Australian Digital Health Agency
ADM	Automated decision-making
AER	Australian Energy Regulator
AHRC	Australian Human Rights Commission
AI	Artificial intelligence
AIC Act	Australian Information Commissioner Act 2010 (Cth)
ALRC	Australian Law Reform Commission
AMA	Australian Medical Association
APEC	Asia Pacific Economic Cooperation
APP	Australian Privacy Principles
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
CBPR	Cross Border Privacy Rules
CDR	Consumer Data Right
DPI	Digital Platforms Inquiry
EDPB	European Data Protection Board
EDR	External Dispute Resolution
EM	Explanatory Memorandum
EU	European Union
FCC	Federal Circuit Court
FOI	Freedom of Information
FOI Act	Freedom of Information Act 1982 (Cth)
FPO	Federal Privacy Ombudsman
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
MHR	My Health Record
MHR Act	My Health Records Act 2012 (Cth)
MOU	Memorandum of Understanding
NDB	Notifiable Data Breach
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Cooperation and Development
Online Privacy Bill	Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth)
PIA	Privacy Impact Assessment
SCCs	Standard Contractual Clauses
TFN	Tax File Number
UK ICO	United Kingdom Information Commissioner's Office

Executive Summary

The Australian Government's Review of the *Privacy Act 1988* is intended to ensure that our privacy framework empowers consumers, protects their data and best serves the Australian economy.

Through the review, the Government is seeking to identify opportunities to improve consumer privacy protection and ensure Australia's privacy regime operates effectively for all elements of the community while allowing innovation to thrive in the digital economy.

The Attorney-General's Department's Discussion Paper sets out proposals and options for reform of the Privacy Act that are designed to achieve these outcomes, based on feedback received in response to its earlier Issues Paper.

The Issues Paper prompted 200 submissions from a diverse range of stakeholders, including private sector organisations, academics and research centres, industry peak bodies, consumer and privacy advocates, and Commonwealth and state and territory public sector agencies and individuals. These canvassed a wide variety of issues related to the scope and application of the Privacy Act, notice and consent, the introduction of additional protections, and regulation and enforcement.

As the Discussion Paper notes, there was broad support in submissions for retaining the flexible, principles-based approach of the Privacy Act. Other key themes included providing individuals with greater control over their personal information through new mechanisms to withdraw consent, request erasure and seek redress for interferences with privacy. There was also support for increasing transparency requirements while avoiding overreliance on notice and consent mechanisms.[1]

Submissions generally also endorsed the introduction of additional protections around the collection, use and disclosure of personal information, such as a new requirement to handle personal information fairly and reasonably and greater organisational accountability obligations. Another common theme was the need for effective mechanisms to encourage compliance with the Privacy Act and remedy non-compliance, including strengthened powers for the Commissioner.[2]

We welcome the well-considered and reasoned proposals and options put forward in the Discussion Paper that have been informed by this consultation.

The OAIC's recommendations in this submission build on these proposals and are aimed at supporting the outcomes sought by government in this review.

In responding to the Attorney General's Department's proposals and options, we have drawn on our regulatory experience to inform our observations about how these potential reforms would operate in practice, and which options are likely to support the OAIC to achieve its regulatory objectives into the next decade for the benefit of the Australian community. Our recommendations reflect our support for the proposals, and make suggestions about enhancements or areas where these proposals could be built on further to ensure that the objectives expressed in the Discussion Paper can be fully realised.

[1] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 22 December 2021, pp 7-8.

[2] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 22 December 2021, pp 7-8.

Importantly, our recommendations seek to strengthen the privacy framework to prevent harms to individuals, including through measures that enhance organisational accountability, and that benefit the community and the economy overall.

Protecting privacy in the digital environment

The use of data – including personal and sensitive information – is an increasing focus for government and businesses in Australia and globally.

The government's Digital Economy Strategy aims for all businesses to be digital businesses by 2030. The Australian Data Strategy sets out how the government will enhance effective, safe and secure data use over the next four years. Business is using data to innovate with new products and services, participating in global data flows, and servicing a community that is increasingly online.

A move to a digital economy brings great opportunities, but also creates increased risks.

Many of these risks have emerged due to the dramatic increase in the amount of data and personal information collected about individuals by online platforms and services, and the subsequent use and disclosure of this information in ways users may not understand or expect. In particular, the personalisation of data for commercial purposes is driving the delivery of content online and contributing to certain privacy harms.

For instance, a key purpose for which data is collected online is for targeted advertising. While there are benefits to some consumers from targeted advertising, entities employ increasingly sophisticated and privacy-invasive methods such as profiling and cross-device tracking to more accurately personalise and target individuals with marketing material, which may outweigh the benefits.

This shift is taking place at a time of increased threats to cyber security and online safety, and the rise of activities such as ransomware.

In this complex environment, it is no longer sustainable to expect individuals to be on constant guard to protect the security and integrity of their personal information. Australia's privacy framework – and organisations entrusted with personal information who operate within it – must protect this data upfront.

To this end, the OAIC's recommendations to the Review of the Privacy Act seek to ensure Australia's privacy regime operates effectively for all and promotes innovation and growth by:

- protecting consumers from individual and collective privacy risks and harms
- empowering consumers to take control of their personal information through new rights and enhanced transparency requirements
- enhancing the framework of organisational accountability and personal information handling to ensure regulated entities are confident to innovate and use data within the boundaries of the law, informed by community expectations
- establishing a regulatory framework that supports proactive and targeted regulation, strategic enforcement, efficient and more direct avenues of redress for individuals, and appropriate deterrents against mishandling of personal information

- supporting global interoperability and minimising friction to ensure consistency of protection across the economy and to protect personal information wherever it flows.

Our recommendations preserve the flexibility of the Privacy Act to work in both the online and offline environments – from large digital platforms to small health care providers and childcare centres – and enable entities to take a risk-based approach to compliance.

They also respond to calls for greater certainty in the law by enhancing the Commissioner's ability to make codes and binding guidance. This will allow targeted requirements to be applied to particular sectors or information handling practices as needed.

Overview of OAIC recommendations

Higher standards of personal information handling to support privacy self-management

Our recommendations recognise the importance of transparency and individual choice and control to the Privacy Act framework. However, these mechanisms are limited in their ability to restrain harmful activities. It is unrealistic and unfair to expect individuals to consider and understand every collection notice and privacy policy, and to take steps to protect themselves from privacy harms.

For consent to be meaningful, individuals need to be provided with genuine choices around how their personal information will be handled, and those choices need to be inherently fair. Meaningful consent also requires an individual to be properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent.

Entities in the digital economy are collecting more information than ever before, and many are basing their business model around the collection and disclosure of personal information. Data handling is increasingly complex, making it difficult for individuals to understand everything that is happening with their information. A large proportion of all school, work and social activities are taking place in the online environment, which means that individuals cannot opt out of digital services if they want to continue engaging meaningfully in society.

These issues can be addressed by raising the general standard of personal information handling across the economy. This includes making APP entities more accountable for their information handling practices by requiring them to proactively ensure their activities are appropriate.

By raising the standard of data handling, individuals can have greater confidence that they will be treated fairly when they choose to engage with a service. This would prevent consent being used to legitimise handling of personal information in a manner that, objectively, is unfair or unreasonable.

Increased accountability for regulated entities

Establishing a positive duty on organisations to handle personal information fairly and reasonably will require regulated entities to take a proactive approach to meeting their obligations, as the parties best equipped to understand their complex information handling flows and practices.

The OAIC views this reform as providing a new keystone of the Privacy Act.

This central obligation to collect, use and disclose personal information fairly and reasonably would provide a new baseline for privacy practice that meets community expectations and helps to restore and build trust.

In concert with our recommended changes to privacy self-management mechanisms like notice and consent, these reforms will raise the standard of data handling to help prevent harms and remove the privacy burden from individuals by providing the same assurances to people who share their personal data as those provided through well-established workplace and consumer safeguards.

This will allow individuals to engage with products and services with confidence that – like a safety standard – privacy protection is a given. It also provides the flexibility needed by entities to innovate and contribute to a thriving digital economy.

This new fair and reasonable obligation will need to be supported by enhanced organisational accountability measures, similar to those under the European General Data Protection Regulation and the Privacy (Australian Government Agencies – Governance) APP Code 2017, including an express obligation to undertake a 'privacy by design' approach to privacy compliance.

This will specifically require entities to consider how their activities will impact individuals, and whether there are less privacy intrusive options for new projects, activities or initiatives.

These enhancements will also require regulated entities to implement actions and controls that demonstrate their compliance with the privacy regulatory framework.

By embedding strong accountability measures, entities can build a reputation for strong and effective privacy management, which is essential for realising the benefits of the personal information they hold and meeting their corporate social responsibilities.

A contemporary regulatory framework

To operate effectively, this framework needs to have the right regulatory tools on hand to respond effectively to privacy harms emerging through the digital environment. 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.

We have therefore recommended changes to the Privacy Act enforcement framework to give the OAIC effective tools to uphold the law and respond to emerging threats in a proportionate and pragmatic way.

This can occur through a simplified civil penalty regime, supported by infringement notices as a quick and cost-effective way to stamp out non-compliant behaviour and have a deterrent effect without the need for court proceedings.

The proposals in the Discussion Paper that contemplate a different structure for the OAIC and the complaints handling system under the Privacy Act also provide an important signal about the need for a shift in regulatory posture for the OAIC.

These changes would be supported by the introduction of a direct right of action and statutory tort of privacy that would give individuals access to additional options to protect their privacy rights.

Harmonisation and global interoperability

An overarching theme of this review and Australia's shift to a digital economy is to ensure global interoperability – put simply, making sure our laws continue to connect around the world, so our data is protected wherever it flows and the burden on businesses operating globally is reduced. The need for harmonisation within Australia has also been a guiding theme with the privacy response to the COVID-19 pandemic.

Our recommendations to the Review are designed to shape a system that supports global interoperability and minimises friction to help drive economic growth and innovation. Such a system will also help to foster confidence and encourage digital participation by Australians.

At the same time, we need to consider the unique circumstances and expectations of Australians. Interoperability doesn't just mean adopting overseas laws in Australia.

For data flowing out of the country, we have made recommendations aimed at ensuring it is a seamless process for entities to protect Australian's data offshore. Our recommendations support the measures proposed in the Discussion Paper to assist with this, such as standard contractual clauses and certification.

As well as considering the importance of personal information flowing from Australia internationally, we need to consider the importance of Australia's privacy framework in facilitating the flow of personal information into Australia, to Australian businesses.

Our recommendations to the Review are designed to ensure that our privacy framework is comparable with international frameworks so that Australian businesses can receive personal information from overseas companies and remain competitive.

Our recommendations are summarised below and examined in more detail in the following chapters.

Recommendations

Recommendation 1 – Amend the first object in s 2A of the Privacy Act to state that the predominant object of the legislation is to protect individuals by promoting the privacy of their personal information and recognising that there is a public interest in privacy.

Recommendation 2 – Adopt proposal 2.1 to replace the word 'about' with 'relates to' in the definition of personal information.

Recommendation 3 – 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, rather than the Privacy Act.

Recommendation 4 – Consider alternative solutions for meeting the objectives of proposal 2.3, including requiring entities to have regard to OAIC guidelines when carrying out their functions or activities.

Recommendation 5 – Adopt proposal 2.4 to clarify that collection under the Privacy Act captures information obtained from any source, including inferred information.

Recommendation 6 – Implement proposal 2.5 to replace the term 'de-identified' with 'anonymised' in the Privacy Act.

Recommendation 7 – 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 8 – 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 9 – Introduce a prohibition on APP entities taking steps to re-identify information that they collected in an anonymised state that is subject to clear and appropriate exceptions including research involving cryptology, information security and data analysis and in order to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information.

Recommendation 10 – 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 11 – Include a new provision that would require APP entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

Recommendation 12 – Adopt proposal 3.1 to amend the Act to allow the Commissioner to make an APP code on the direction or approval of the Attorney-General in either of the following two scenarios:

- where it is in the public interest to do so without first having to seek an industry code developer, or
- where there is unlikely to be an appropriate industry representative to develop the code.

Recommendation 13 – Adopt proposal 3.2 to amend the Act to allow the Commissioner to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.

Recommendation 14 – Ensure that the proposed amendments to enable the Commissioner to issue a temporary APP code stipulate that the consultation requirements in relation to APP codes do not apply.

Recommendation 15 – Adopt proposal 3.3 to amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:

- entities, or classes of entity
- classes of personal information, and
- acts and practices, or types of acts and practices.

Recommendation 16 – Adopt proposal 3.4 to amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

Recommendation 17 – 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 18 – If the small business exemption is not removed, further exceptions to the small business exemption should address privacy risks across the information lifecycle and be clear in scope.

Recommendation 19 – If additional types of businesses that engage in high privacy risk acts and practices are prescribed as exceptions to the small business exemption, these should include small businesses that:

- hold personal information of a large number of individuals
- hold any sensitive information, regardless of the number of records
- engage in restricted or prohibited practices.

Recommendation 20 – If the small business exemption is not removed, remove the consent provisions in ss 6D(7)(a) and 6D(8)(a)(i).

Recommendation 21 – Remove the employee records exemption and consider whether it is appropriate to add additional exceptions to specific APPs to address the particular business needs of employers.

Recommendation 22 – Remove the political parties exemption by:

- amending the definition of 'organisation' under the Privacy Act to include a 'registered political party', and
- repealing section 7C of the Privacy Act which exempts political acts and practices for political representatives and affiliates of political parties.

Recommendation 23 – If considered necessary for abundant clarity, include a provision in the Privacy Act that provides that the Act does not apply to the extent that it would infringe on the constitutional doctrine of implied freedom of political communication.

Recommendation 24 – Amend the journalism exemption to confine it to journalism that is, on balance, in the public interest, as recognised in existing journalism privacy standards.

Recommendation 25 – Amend the journalism exemption to require media organisations to comply with the security requirements under APP 11, with appropriate exceptions to data breach notification obligations.

Recommendation 26 – Adopt proposal 8.1 for APP 5 notices to be clear, current and understandable.

Recommendation 27 – Adopt proposal 8.2, which should be expanded to include the following matters for inclusion in an APP 5 notice:

- if the individual may not be aware that the APP entity has collected the personal information, the fact that the entity so collects, or has collected, the information and the circumstances of that collection
- if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection)
- whether the APP entity is likely to disclose the personal information to overseas recipients
- the right to withdraw consent where consent has been required for the personal information handling
- any purposes the information will be collected, used or disclosed for that the individual is likely to find concerning, including where it will be collected, used or disclosed for a restricted practice.

Recommendation 28 – Adopt proposal 8.3 for standardised privacy notices to be considered in the development of APP codes, such as the OP code, including standardised layouts, wording and icons, with consumer comprehension testing required to ensure the effectiveness of the standardised notices.

Recommendation 29 – Retain the current wording of APP 5.1 or introduce additional exceptions to proposal 8.4 to limit notice for recurring collections or where there is a legitimate public interest reason not to provide notice.

Recommendation 30 – Adopt proposal 9.1 for consent to be defined in the Privacy Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

Recommendation 31 – Elevate OAIC guidance on withdrawing consent into the Privacy Act.

Recommendation 32 – Adopt proposal 9.2 for standardised consent to be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies, with cross sector alignment to the extent practicable, supported by consumer comprehension testing.

Recommendation 33 – Adopt proposal 10.1 to amend APP 3 and APP 6 to require that the collection, use or disclosure of personal information must be fair and reasonable in the circumstances.

Recommendation 34 – Adopt proposal 10.2 to introduce legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances.

Recommendation 35 – Include the following legislated factors:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances
- The kinds, sensitivity and amount of personal information being collected, used or disclosed
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity
- Whether the individual's loss of privacy is proportionate to the benefits
- If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child
- Whether the collection, use or disclosure of personal information is lawful
- Whether the collection, use or disclosure of personal information will have a foreseeable impact on the public interest in privacy.

Recommendation 36 – Include the following issues in the explanatory memorandum to this amendment as relevant when considering the factor about ensuring the individual's loss of privacy is proportionate to the benefits:

- whether the collection, use or disclosure intrudes to an unreasonable extent upon the personal affairs of the affected individual
- whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits
- any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.

Recommendation 37 – Adopt proposal 10.1 alongside the existing APP 3.1, 3.2 or 6.2(a) requirements.

Recommendation 38 – Subsume APP 3.5 within the overarching fair and reasonable requirement of proposal 10.1.

Recommendation 39 – Ensure that proposal 10.1 applies to collections, uses and disclosures of personal information.

Recommendation 40 – Clarify that the fair and reasonableness test applies in addition to where an individual has consented to the specific information handling under APPs 3.3 and 6.1(a).

Recommendation 41 – Adopt proposal 10.3 to include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Recommendation 42 – Consider alternative solutions for meeting the objectives of proposal 10.4, including adopting:

- the OAIC's recommendation to include a new provision that would require APP entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act
- the OAIC's recommendation to amend APP 3 to expressly require entities to determine, at or before the time of collection, each of the known specific purposes for which the information is to be collected, used or disclosed and to record those purposes
- proposal 10.1
- the additional enforcement powers proposed in the Discussion Paper and recommended in Part 24 of this submission.

Recommendation 43 – Adopt option 1 of proposal 11.1 to introduce a restricted practice regime that requires APP entities that engage in proscribed practices to take reasonable steps to identify privacy risks and implement measures to mitigate those risks.

Recommendation 44 – Introduce requirements for APP entities undertaking restricted practices to seek a periodic independent audit of the privacy risks identified in relation to the activity and measures implemented to mitigate those risks.

Recommendation 45 – Introduce the power for the Commissioner to create an APP code clarifying the steps required to mitigate risks for specific restricted practices, modelled on proposal 3.1 which allows the Commissioner to make an APP code on the direction of the Attorney-General.

Recommendation 46 – Adopt the following restricted practices:

- Direct marketing, including online targeted advertising
- The collection, use or disclosure of sensitive information on a large scale
- The collection, use or disclosure of children's personal information on a large scale
- The collection, use or disclosure of location data on a large scale
- The sale of personal information

- The collection, use or disclosure of personal information for the purposes of online personalisation and delivering targeted advertising
- The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects
- Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.

Recommendation 47 – Introduce prohibited practices into the Privacy Act, subject to appropriate public interest exceptions including in relation to:

- Profiling, online personalisation and behavioural advertising using children's personal information
- Inappropriate surveillance or monitoring of an individual through audio or video functionality of the individual's mobile phone or other personal devices
- The collection, use or disclosure of personal information that is unlawful
- The commercial use of automated biometric identification systems
- Personal information scraping from online platforms

Recommendation 48 – Introduce prohibited practices in relation to the scaping of personal information through a requirement that online platforms and other appropriate websites must proactively take reasonable steps to prevent it.

Recommendation 49 – Introduce the ability to prescribe additional prohibitions by regulation.

Recommendation 50 – Adopt option 1 of proposal 12.1 to amend the Privacy Act to require privacy settings to be set to privacy protective by default except for the collection, use or disclosure of personal information that is reasonably necessary to provide the particular product or service.

Recommendation 51 – Adopt proposal 13.2 to require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child*.

Recommendation 52 – Adopt proposal 14.1 to introduce a right to object, with the following recommended elements:

- an absolute right to object to direct marketing
- an absolute right to object to the sharing, disclosure or otherwise making available of an individual's personal information to third parties for a benefit (monetary or otherwise), and particularly where the personal information relates to a child
- a reasonable steps test to apply to the collection, use or disclosure of personal information for all other purposes
- appropriate exceptions to the general right to object.

Recommendation 53 – Adopt proposal 8.2 to require APP entities to notify individuals about their right to object and the purpose(s) for which the entity is collecting and may use or disclose the personal information, and require similar information to be included in APP 1 privacy policies.

Recommendation 54 – Introduce the following procedural elements in relation to a right to object:

- APP entities must respond to objection requests within 30 days (for agencies) or within a reasonable period (for organisations)
- Responses to individuals following an objection request must include information about:
  - the consequences of the individual's objection
  - the entity's reasons for not taking action, if a request is not acted upon
  - the individual's complaint or appeal rights.
- Before an APP entity refuses an objection request, it must provide 'reasonable assistance' to individuals to reframe their request and provide them with a reasonable opportunity to revise a request.

Recommendation 55 – Adopt proposal 15.1 and 15.2 to introduce a general right to erasure that includes a right to de-index search results and a requirement for APP entities to take reasonable steps to carry out an erasure request, subject to exceptions including:

- where erasure would hinder law enforcement
- where erasure would be contrary to the public interest and freedom of expression
- where personal information is required for a transaction or contract
- where the personal information sought to be erased is contained in a Commonwealth record
- where the entity is required to retain the information by or under an Australian law, or court/tribunal order
- where a request is 'frivolous or vexatious', consistent with APP 12
- where erasure would have an unreasonable impact on the personal information of another individual
- where erasure would pose a serious threat to the life, health or safety of any individual, or to public health and safety
- where personal information is required for the purposes of occupational medicine or for the management of health or social care systems or services
- where the information is required for archival, research or statistical purposes in the public interest
- where the information relates to existing or anticipated legal proceedings between the entity and the individual.

Recommendation 56 – Adopt proposal 8.2 to require APP entities to notify individuals about their right to erasure and require similar information to be included in APP 1 privacy policies.

Recommendation 57 – Adopt proposal 15.3 to require an APP entity to respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

Recommendation 58 – Provide that the right to erasure extends to erasure of:

- any copy of the record
- any previous version of the record
- any back-up version of the record
- any inferred personal information unless it has been de-identified
- personal information that is no longer 'held' by an entity, so that APP entities are required to notify others of the erasure request where personal information has been made public.

Recommendation 59 – Adopt proposal 16.1 that the right to object would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing.

Recommendation 60 – Adopt proposal 16.4 to repeal APP 7 in light of existing protections in the Act and other proposals for reform.

Recommendation 61 – Consider alternative solutions for meeting the objectives of proposal 16.2, including:

- implementing additional requirements to address the privacy risks associated with tracking and profiling individuals for the purposes of targeted online advertising through the OP code
- adopting proposal 10.1
- adopting proposal 11.1
- adopting option 1 of proposal 12.1
- adopting the OAIC's recommendation to amend APP 3 to expressly require entities to specifically determine, at or before the time of collection, each of the known purposes for which the information is to be collected, used or disclosed and to record those purposes.

Recommendation 62 – Consider whether the objectives of proposal 16.3 could be achieved through the proposed OP code.

Recommendation 63 – If proposal 16.3 is adopted, consider how the obligations to include the relevant information in an APP privacy policy could be framed to ensure they do not have unintended consequences or require disproportionate effort by entities to meet the requirements.

Recommendation 64 – Extend proposal 17.1 to require APP entities engaging in ADM to include a meaningful explanation of these automated decisions in privacy policies and APP 5 notices. This

could include information about the types of personal information being used in an automated decision, how that information is weighted and, where appropriate, information about how any ratings given to an individual relate to other information or decisions.

Recommendation 65 – Consider whether these explanations should include more technical information that may assist individuals to contest these decisions and, if so, whether appropriate exceptions are necessary to protect any trade secrets in respect to the ADM system being used.

Recommendation 66 – Ensure that additional protections for ADM apply to AI informed decision-making that has a legal or similarly significant effect.

Recommendation 67 – Introduce clarification around the concept of a decision with 'legal or similar significant effect' in the legislation or explanatory materials.

Recommendation 68 – Adopt proposal 18.1 that an organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

Recommendation 69 – Adopt proposal 18.2 to introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:

- the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.

Recommendation 70 – Adopt proposal 18.3 to clarify the existing access request process in APP 12 to the effect that:

- an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature, and
- where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.

Recommendation 71 – Amend the Privacy Act to require APP entities to keep personal information that it has published online accurate, up-to-date and complete, and to correct it upon request – to the extent that the entity retains control of the personal information.

Recommendation 72 – Consider alternative solutions for meeting the objectives of proposals 19.1 and 19.2, including requiring entities to have regard to OAIC guidelines when carrying out their functions or activities and adopting proposal 3.1 to provide the Commissioner with greater flexibility and discretion to develop APP codes.

Recommendation 73 – Adopt proposal 19.3 to amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.

Recommendation 74 – Amend APP 1 to expressly require APP entities to:

- implement a risk-based privacy management program
- implement a 'privacy by design' approach
- appoint a privacy officer or privacy officers
- provide the Commissioner, on request, with evidence of the steps taken to ensure compliance with the APPs and any registered APP code.

Recommendation 75 – Include a note in the explanatory memorandum that will accompany the amending Bill that PIAs are central to facilitating a 'privacy by design' approach.

Recommendation 76 – Amend APP 3 to expressly require entities to determine, at or before the time of collection, each of the known specific purposes for which the information is to be collected, used or disclosed and to record those purposes.

Recommendation 77 – Consider whether the potential benefits of a controller/processor regime would be outweighed by increases to complexity in compliance and regulation.

Recommendation 78 – If the controller/processor distinction is introduced into the Act:

- require that processors are subject to organisational accountability obligations under APP 1 and security requirements under APP 11, at a minimum
- introduce requirements for certain mandatory terms in contracts between controllers and processors, modelled on Article 28 of the GDPR.

Recommendation 79 – Adopt proposal 22.1 to introduce a mechanism for Government to prescribe countries and certification schemes under APP 8.2(a).

Recommendation 80 – Adopt proposal 22.2 to make SCCs for transferring personal information overseas available to APP entities. The SCCs should support the requirement to take reasonable steps in APP 8.1.

Recommendation 81 – Adopt proposal 22.3 to remove the informed consent exception in APP 8.2(b).

Recommendation 82 – Adopt proposal 22.4 to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in an entity's up-to-date APP privacy policy required to be kept under APP 1.3.

Recommendation 83 – Adopt proposal 22.5 to introduce a definition of 'disclosure' that is consistent with the current definition in the APP guidelines.

Recommendation 84 – Consider alternative solutions for meeting the objectives of proposal 22.6, including requiring entities to have regard to OAIC guidelines when carrying out their functions or activities.

Recommendation 85 – Adopt proposal 23.1 to progress implementation of the CBPR system, with the preliminary step of conducting a gap analysis between the CBPR and the Privacy Act.

Recommendation 86 – Adopt proposal 23.2 to introduce a voluntary domestic privacy certification scheme in a way that draws on best practice and works alongside other certification schemes, including the CBPR.

Recommendation 87 – Ensure that the voluntary domestic privacy certification scheme:

- is flexible and enables an entity to seek enterprise-wide certification for all of its operations, or certification for specific products, data types or business processes
- enables the OAIC to develop and publish accreditation requirements for certification bodies and certification criteria for the scheme
- ensures 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.

Recommendation 88 – Adopt a modified version of proposal 24.1 that:

- introduces a single civil penalty under s 13 with a maximum fine commensurate with the increased penalties proposed in schedule 2 of the exposure draft of the OP Bill.
- repeals s 13G
- introduces a broader infringement notice power for any interference with privacy containing a tiered approach to penalty amounts, commensurate with the infringement notice framework of the ACCC.

Recommendation 89 – Adopt proposal 24.3 to make civil penalty provisions in the Privacy Act subject to investigation under Part 3 of the Regulatory Powers Act in addition to the Commissioner's current investigation powers.

Recommendation 90 – Make assessments under the Privacy Act subject to monitoring under Part 2 of the Regulatory Powers Act in addition to the Commissioner's current assessment powers.

Recommendation 91 – Adopt proposal 24.4 to allow the Commissioner to undertake public inquiries and reviews into specified matters.

Recommendation 92 – Adopt proposal 24.5 to amend paragraph 52(1)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss.

Recommendation 93 – Adopt proposal 24.6 to give the Federal Court the express power to make any orders it sees fit.

Recommendation 94 – Adopt proposal 24.7 to introduce an industry funding model for the OAIC that is supported by appropriate supplementary budget appropriations for functions and activities not funded by a levy.

Recommendation 95 – Adopt proposal 24.8 to amend the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.

Recommendation 96 – Adopt elements from each of the options in proposal 24.9 to amend the current regulatory framework to enable the OAIC to shift to a more strategic, proactive regulator, subject to the considerations outlined in this submission.

Recommendation 97 – 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 98 – Expand s 41(dc) to instances where a complaint has already been adequately dealt with by an EDR scheme.

Recommendation 99 – 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 100 – Adopt proposal 25.1 to create a direct right of action with the following design elements:

- The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.
- The action would be heard by the Federal Court or the FCC.
- The claimant would first need to make a complaint to the OAIC (or FPO) and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.
- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.
- The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.

Recommendation 101 – 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 102 – 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 103 – Adopt proposal 26.1 to introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123, rather than alternative proposals 26.2 and 26.3, which would leave the development of a tort of serious invasion of privacy to the common law.

Recommendation 104 – New state and territory data breach reporting schemes should, to the extent possible, align with the requirements of the NDB scheme under the Privacy Act to reduce regulatory fragmentation and increase certainty for regulated entities.

Recommendation 105 – The NDB scheme should remain the baseline for data breach reporting requirements at the federal level and any separate scheme should seek to increase, not replicate, those reporting requirements where warranted.

Recommendation 106 – Adopt proposal 27.1 to amend subsections 26WK(3) and 26WR(4) of the Act to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

Recommendation 107 – Adopt proposal 28.1 to develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations or that otherwise seek to override the APPs.

Recommendation 108 – Ensure that the privacy law design guide addresses the following issues:

- The Privacy Act and the APPs should remain the baseline for privacy protection at the federal level and any new Commonwealth laws that propose to implement new privacy obligations should seek to increase, not replicate, those baseline requirements (where warranted).
- If privacy protections are included in other legislative regimes, the Commissioner should have full jurisdiction over enforcing those protections and all entities subject to those protections, to ensure that privacy regulation is clear, consistent and effective.
- If an agency is developing legislation that seeks to rely on the required or authorised exception to the APPs (such as legislation authorising the use or disclosure of personal information), they should consider whether the proposed legislation is reasonable, necessary and proportionate to achieving a legitimate public policy objective. A PIA can assist agencies to undertake this assessment, which may also assist with the development of Human Rights Compatibility Statements for legislative projects.

Recommendation 109 – Consult the Commissioner in the development of the privacy law design guide.

Recommendation 110 – Adopt proposal 28.2 to encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

Recommendation 111 – 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 112 – Ensure that the privacy protections in any state or territory laws that purport to address privacy issues are commensurate with those under the Privacy Act.

Recommendation 113 – Adopt proposal 28.3 to establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

Part 1: Objects of the Privacy Act

1.1 Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:

(a) to promote the protection of the privacy of individuals *with regard to their personal information*; and

(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities *undertaken in the public interest*.

1.1 Privacy has its basis in international law and is acknowledged as a fundamental human right.[3] In Australia, these privacy rights have been given effect as a data protection statute to prevent the personal information of individuals from being subject to arbitrary interferences and protect them from harm stemming from its misuse. The Privacy Act also incorporates the Organisation for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) (OECD Guidelines), which were adopted to address concerns around increased use of personal information and the risks to economies that may result from limiting the flow of personal information across borders.[4]

1.2 The potential harms to individuals that the Privacy Act is intended to address have been amplified through the increased use of data in the digital economy. Innovations in technology and service delivery have resulted in a dramatic increase in the amount of data and personal information handled by business and government. Alongside this significant shift in data handling practices has come an increase in community expectations that their personal information will be protected.

1.3 As noted in our submission to the Issues Paper, the OAIC considers that the Review presents an opportunity to place greater emphasis on the rights of individuals and the obligations of entities to protect those rights, and to recognise that there is significant public interest in privacy protections.

1.4 We therefore support the aim of proposal 1.1 in the Discussion Paper to make clear that:

- the Privacy Act is concerned with informational privacy
- the protection of privacy is properly balanced against the protection of other public interests.

1.5 To more fully achieve these aims, we recommend that amendments are made to proposal 1.1 to recognise that:

[3] 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] See the preamble of the Privacy Act and Organisation for Economic Co-Operation and Development, *The OECD Privacy Framework*, OECD, 2013, accessed 21 December 2021, p 19.

- the first and predominant object of the Privacy Act is to protect Australians by promoting the privacy of individuals with regard to their personal information
- there is a public, as well as personal, interest in privacy.

1.6 The OAIC's recommendation is intended to achieve and elevate the aims of proposal 1.1 to more broadly recognise the importance of privacy and the regulation of personal information in the digital age.

1.7 Recognising the public interest in privacy and the important role that the Privacy Act plays in protecting individuals would help to frame the application and interpretation of the rights and obligations in the legislation, including the proposed fair and reasonable test (as discussed in Part 10 of this submission). It will also guide and inform the Information Commissioner's regulatory priorities and discretion in exercising their powers and selecting regulatory outcomes.

1.8 These recommended amendments to s 2A are discussed in more detail below.

Promoting the privacy of individuals

1.9 Recognising that the object of the Privacy Act is to protect Australians by promoting the privacy of individuals with regard to their personal information would clarify that the Act is concerned with information privacy, and would also ensure that the individual, and the impacts that personal information handling have on the individual, is at the centre of the Privacy Act.

1.10 Elevating this to be the predominant object of the Act will make clear that, where the interests of individuals in the protection of privacy and interests of APP entities in undertaking their functions or activities are not aligned, greater weight should be given to protecting individuals by promoting their privacy. This would address the concerns of some submitters to the Issues Paper that in circumstances where the interests of individuals and APP entities are not aligned, 'the balance is now always weighed against individuals'.[5]

1.11 This proposed amendment does not mean that the protection of privacy will prevail in all circumstances; merely that in circumstances where the balance is evenly struck, there is an inherent bias towards the protection of personal information. The OAIC's recommended amendment would acknowledge that the main aim of the legislation is to empower and protect individuals by attaching rights and obligations to their personal information rather than to simply protect the information itself.

1.12 This approach has precedent in comparable domestic legislation. Section 2 of the *Competition and Consumer Act 2010* states that 'the object of this Act is to enhance the welfare of Australians through the promotion of competition and fair trading and provision for consumer protection.' This recognises that the central purpose of this regime is the welfare of individuals, pursued through the promotion of competition and fair trading and provision of consumer protection.

[5] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 7 December 2021, p 18.

Public interest in privacy

1.13 Recognising that there is a public interest in privacy separates these important public interest considerations from the functions and activities of APP entities. This is important because the Privacy Act will at times facilitate a balance between competing interests. These include the interests in individual privacy, collective privacy and the interests of APP entities. The objects should acknowledge that there is a public interest in individual and collective privacy, which may facilitate or limit the personal information handling functions or activities of APP entities depending on the circumstances.

1.14 We broadly agree with the Discussion Paper that it is desirable for the proposed amendment to s 2A(b) to make it clearer that the subjective interests of entities may be less relevant if their functions and activities are not in the public interest. However, there may be a risk that the Discussion Paper proposal will permit an overly broad interpretation of public interest. It is open to interpret the public interest in the economic wellbeing of the country as conceivably capturing any commercial practices, which may undermine the benefits of the proposal.

1.15 The OAIC's recommended amendments to s 2A are intended to enhance the recognition in the Privacy Act that strong data protection and privacy rights are necessary to 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.

Recommendation 1 – Amend the first object in s 2A of the Privacy Act to state that the predominant object of the legislation is to protect individuals by promoting the privacy of their personal information and recognising that there is a public interest in privacy.

Part 2: Definition of personal information, de-identification and sensitive information

2.1 Change the word 'about' in the definition of personal information to 'relates to'.

2.2 Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

2.3 Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.

2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

In practice, what information would the proposed definition of personal information capture which are not presently covered?

What do APP entities estimate are the costs and benefits of amending the definition of personal information in the manner suggested?

Would the proposed definition of personal information pose any unintended consequences for APP entities? How could these be mitigated?

Would the proposed definition of collection have any unintended consequences for APP entities? How could these be mitigated?

In practice, what information would the proposed definition of personal information capture which are not presently covered?

What do APP entities estimate are the costs and benefits of amending the definition of personal information in the manner suggested?

2.1 As a key threshold concept in the Privacy Act, the definition of personal information delineates the scope of what is regulated and sought to be protected under the Act. As stated in our submission to the Issues Paper, it is important that this definition is flexible and neutral in its application to different technologies.

2.2 We welcome the Discussion Paper's proposals aimed at modernising the definition of personal information to ensure that it remains relevant in the digital age and is interoperable with relevant domestic laws and comparable international privacy jurisdictions. We recommend several enhancements to these proposals to help to ensure that the definition is fit for purpose now and into the future.

Information that 'relates to' an individual

2.3 We support proposal 2.1, which will address issues caused by overly narrow interpretations of the term 'about' and assist in resolving other key matters raised in the Discussion Paper.

2.4 Proposal 2.1 will promote greater clarity about the circumstances in which information will be covered by the Privacy Act. It will also promote interoperability with comparable definitions under the Consumer Data Right (CDR) and COVIDSafe system, as well as internationally with the EU General Data Protection Regulation (GDPR).[6]

2.5 The existing test of identifiability will continue to apply, so that information will only be personal information if it relates to an identified individual or an individual who is reasonably identifiable. As such, we consider that the regulatory impacts of this amendment on APP entities will be low.

Information capable of being personal information

2.6 We support the aims of proposal 2.2 to provide more clarity around the scope of the definition of personal information to ensure that it captures technical information.

2.7 There has been some uncertainty in whether the definition of personal information captures technical information since *Privacy Commissioner v Telstra Corporation Ltd* (the Grubb case).[7] The uncertainty identified by submitters is concerning given that online and device identifiers are increasingly being used to track individuals and are rivalling names and addresses as key identifiers.[8]

2.8 We recommend that these uncertainties are resolved by adopting proposal 2.1 and introducing further clarification in the explanatory memorandum that the definition of personal information is intended to capture certain types of technical information. This could be modelled on the explanatory materials for the *Treasury Laws Amendment (Consumer Data Right) Bill 2019*.

2.9 Our recommended approach to this issue seeks to address the aims of proposal 2.2 while also retaining the flexibility of the definition and ensuring that it will not become out-of-date as technology changes.

2.10 The definition of personal information is technology-neutral meaning that, in practice, the type of information that is personal information is unlimited and can vary widely. Questions around whether the definition of personal information captures technical information stem from the Grubb case and uncertainty arising from the interpretation of the term 'about'.

2.11 A non-exhaustive list in the definition of personal information would have to be sufficiently broad to ensure the definition remains flexible, future-proofed and will not result in the listed categories being given undue weight when interpreting the definition. In practice, this will limit the extent to which this non-exhaustive list provides additional certainty. For example, the list

[6] See the definition of personal data at *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) [2016] OJ L 119/1* (GDPR)*, art 4(1)*

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

[8] See for example UK Information Commissioner's Office *Update Report into adtech and real time bidding*, ICO, United Kingdom Government, 20 June 2019, 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.

of factors suggested in the Discussion Paper would still need to be supplemented with OAIC guidance.

2.12 We therefore reiterate recommendation 5 in our submission to the Issues Paper to include a non-exhaustive list of technical data that may be captured by the definition in the explanatory memorandum, rather than in the legislation itself. This recommendation achieves the aims of proposal 2.2 while also addressing the risks of this approach.

Reasonable identifiability factors

2.13 Reasonable identifiability is an important concept in the definition of personal information. To ensure the definition is appropriately flexible, this concept is necessarily context dependent. Where it is unclear whether an individual is 'reasonably identifiable', OAIC guidance suggests that an APP entity should err on the side of caution and treat the information as personal information.[9]

2.14 The inclusion of the term 'reasonably' in the definition means that an APP entity must not only consider whether it is possible to identify an individual from the available information, but also whether the process of identification is reasonable to achieve.

2.15 To assist entities in applying this concept to their particular circumstances, the OAIC has extensive guidance on the scope of reasonable identifiability.[10] This guidance highlights particular factors that must be considered when assessing whether an individual is reasonably identifiable from information, including:

- the nature and amount of information held
- the context of the information, including who will hold and have access to it
- the other information that is available, and the practicability of using that information to identify an individual, including the cost and time required to identify an individual, the operational capacity of, and technology available to, the entity that holds the information as well as its motivation to attempt to identify anyone.

2.16 In practice, this means that even though it may be technically possible to identify an individual from information, if doing so is so impractical that there is almost no likelihood of it occurring, the information would not generally be regarded as 'personal information'.

2.17 Proposal 2.3 and the objective factors being proposed will effectively elevate this guidance into the legislation. However, the difficulties that APP entities may have in assessing reasonable identifiability do not appear to stem from uncertainty in the legal principles underpinning this term but rather from the practical application of these principles in specific contexts. In this respect, including these factors in the legislation may only provide limited clarity in practice.

[9] OAIC, 'Chapter B – Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 December 2021.

[10] OAIC, *What is personal information*, OAIC website, 5 May 2017, accessed 3 November 2021.

2.18 Given that difficulties in applying this concept do not stem from uncertainty around the legal test, establishing these factors in law may detract from the principles-based nature of the Privacy Act and the flexible, outcomes-focused approach it provides.

2.19 As an alternative to proposal 2.3, we consider that our recommendation in Part 3 of this submission to require entities to have regard to OAIC guidelines when carrying out their functions or activities will provide the necessary clarity about the interpretation of this term. These guidelines could be easily amended to reflect the Commissioner's increasing number of determinations. The Discussion Paper's proposed changes to the OAIC's powers, structure and funding, as well as the introduction of a direct right of action, will also facilitate increased decision making and enforcement actions in the courts, which would be reflected in OAIC guidance.

Recommendation 2 – Adopt proposal 2.1 to replace the word 'about' with 'relates to' in the definition of personal information.

Recommendation 3 – 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, rather than the Privacy Act.

Recommendation 4 – Consider alternative solutions for meeting the objectives of proposal 2.3, including requiring entities to have regard to OAIC guidelines when carrying out their functions or activities.

Additional considerations in relation to proposals 2.2 and 2.3

2.20 While our primary recommendations on proposals 2.2 and 2.3 are set out above, we have set out additional issues that we suggest the Review consider if these proposals are adopted in their current form.

2.21 The example list of technical information provided in the Discussion Paper appears to be derived from the definition of personal data in the GDPR. However, this list of information is not framed in the GDPR as different types of personal data. Rather, the definition states that personal data can include *any* information relating to an identified or identifiable natural person. The assessment of who is an identifiable natural person turns on whether one can be directly or indirectly identified, in particular *by reference* to the categories listed in the definition.

2.22 If proposals 2.2 and 2.3 are adopted, we consider that the amendments to the Privacy Act should be more closely modelled on the GDPR. This would likely mean adapting proposal 2.3 to state that individuals can be identified directly or indirectly by reference to the factors in the GDPR. The Review may also wish to consider other categories of information, such as device identifiers and internet or other electronic network information that may be used to identify or reasonably identify an individual but is not specifically an identifier (for example, browser or

search history). It may be appropriate for the explanatory memorandum to state that these types of data are types of online identifiers.[11]

Defining collection

2.23 While privacy risks attach to the handling of all personal information, inferred information may carry even greater risks, particularly as it is often about sensitive information that an individual would not expect has been collected and may not have disclosed voluntarily. This is true even when an APP entity has used proprietary software to generate this information.

2.24 The current definition of personal information is sufficiently broad to capture inferred information about an identified or reasonably identifiable individual. However, given the risks associated with this information, it is particularly important that the Privacy Act is clear in its application to inferred information.

2.25 We support proposal 2.4, which will clarify that collection under the Privacy Act captures information obtained from any source, including inferred information. As stated in our submission to the Issues Paper, technology is allowing for the creation of increasingly accurate inferences and predictions about individuals. Given that this is elevating the OAIC's existing guidance on this term into law, we anticipate that most APP entities will already be treating the inferred information that they hold as personal information.

2.26 This proposal will be supported by our recommendations about organisational accountability in Part 20 of this submission. In particular, these recommended obligations would require APP entities to consider the risks that they might infer or generate personal or sensitive information before undertaking these activities. Entities will then be able to seek consent to the extent appropriate if there is a reasonable risk of generating this information.

Recommendation 5 – Adopt proposal 2.4 to clarify that collection under the Privacy Act captures information obtained from any source, including inferred information.

Sensitive information

What would be the benefits and risks of amending the definition of sensitive information, or expanding it to include other types of personal information?

What further information or guidance would assist APP entities when classifying biometric information, biometric templates or genetic information as 'sensitive information'?

[11] See for example recital 30 of the GDPR, which clarifies that '*[n]atural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*'.

2.27 The Privacy Act defines several categories of personal information as 'sensitive information'. This is because this information is ordinarily seen as highly personal and has the potential to give rise to unjustified discrimination.[12] As highlighted by the Discussion Paper, information may be deemed sensitive information where it clearly implies a category of sensitive information defined in the legislation.

2.28 Sensitive information is generally afforded a higher level of privacy protection under the APPs. These protections include consent requirements and additional limitations on secondary uses and disclosures. This recognises that inappropriate handling of sensitive information can have adverse consequences for an individual or those associated with the individual.

2.29 This does not mean, however, that personal information will always be less 'sensitive' than the defined categories of sensitive information. Depending on context, personal information may be highly sensitive to an individual or capable of causing harm. The APPs are flexible and may require higher standards of protection where the relevant context means that personal information is of increased sensitivity. This flexibility to adapt to context will be enhanced by the reforms proposed in this Discussion Paper, particularly proposal 10.1 to introduce fairness and reasonableness requirements.

2.30 The OAIC's general position is that decisions to extend the categories of sensitive information should be made with care. APP entities are often required to obtain consent before handling sensitive information and it is important that this privacy self-management tool is retained for situations that generally carry higher privacy risks. Equally, extending these consent requirements may not be proportionate where a type of personal information is routinely and necessarily used and shared.

2.31 The Discussion Paper considers various categories of information that could potentially be classified as sensitive information under the Privacy Act. These are discussed further below.

Financial information

2.32 Financial information is commonly seen as sensitive by the community and its misuse has a clear potential to cause economic and other harms to individuals. The community concern around financial information is clearly reflected in OAIC guidance, which requires higher compliance standards when handling this data. For example, our guidance on eligible data breaches lists financial loss through fraud as an example of serious harm that may necessitate notification.[13] Similarly, our Guide to securing personal information notes that while it is not sensitive information, people often expect that financial information will be given a higher level of protection for the purposes of APP 11.[14]

2.33 While we consider that financial information should often be subject to increased protections given the clear harms that may arise for individuals if this data is misused, we do not suggest it

[12] Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice (ALRC Report 108),* ALRC, 12 August 2008, accessed 3 November 2021, [6.95]

[13] OAIC, *What is personal information*, OAIC website, 5 May 2017, accessed 3 November 2021

[14] OAIC, *Guide to securing personal information*, OAIC website, 5 June 2018, accessed 3 November 2021

is appropriate to legally categorise financial information as sensitive information under the Privacy Act.[15]

2.34 In Australia's digital economy, financial information is routinely shared by individuals. In many circumstances, individuals will have no real choice to provide their financial information because the information may be required to provide the service or because it is required by one of the several regulatory regimes that require the collection, use, disclosure or record of financial information. These other legal frameworks often impose additional protections and limitations on this information in addition to the APPs, particularly where the handling of this information poses higher risks. An example of this are the additional requirements on the handling of credit information in the Privacy Act.

2.35 With this context, imposing additional consent requirements on the handling of financial information may have limited impact as a privacy protection in the majority of circumstances. In circumstances that are not already subject to additional consent requirements, this may create friction in the handling of information that is routinely shared or create misaligned expectations for the community around the ability to meaningfully consent to the handling of this information, in circumstances where many APP entities are required by law to collect this information.

2.36 There will be circumstances where financial information is handled in a manner beyond what is specifically required or authorised by law or reasonably necessary to provide a service. However, the risks stemming from these activities will be context-specific and may vary significantly. As set out above, our view is that the flexibility of the APPs, enhanced through reforms such as fairness and reasonableness obligations, provide a more appropriate and proportionate regulatory response.

Location information

2.37 The collection, use and disclosure of information about where a person is or has been has significant privacy risks. This highly intrusive information can be used to infer sensitive information such as religious or health information, may be very difficult to anonymise and can even create safety risks, particularly for vulnerable individuals.

2.38 The Australian community shares these concerns about location information, with two-thirds of Australians being uncomfortable with online businesses tracking their location, and nearly half considering location tracking to be one of the biggest privacy risks today. Importantly, only 25% of individuals felt that their location information was well protected by law.

2.39 As recommended in our submission to the Issues Paper, however, we do not consider that categorising location data as sensitive information is the best approach to protecting this information.[16] In our view, other proposals in this Discussion Paper will provide stronger

[15] We also note that this issue was considered in ALRC (2008), *For Your Information: Australian Privacy Law and Practice (ALRC Report 108),* report prepared by the ALRC, Australian Government, 6.107. The ALRC did not recommend that financial information be included as sensitive information because it does not relate to physical attributes or personal beliefs of an individual in the same way as the existing categories of sensitive information.

[16] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, p. 42

protections for the handling of location information. For example, proposal 10.1 to introduce a fair and reasonable test to the collection, use and disclosure of personal information will require APP entities to consider the greater risks around handling location information and the risks of harm that may occur if it is mishandled. At the same time, this test is flexible and scalable and will not prevent activities that are common and widely understood by individuals, such as the use of location information to provide services such as food delivery, maps or ride sharing mobile apps. Additionally, Chapter 17 of the Discussion Paper proposes a specific restricted purpose in respect of location information. This provides an opportunity for the Review to consider whether specific protections around this information are appropriate.

2.40 This will also ensure that the existing categories of sensitive information retain their consistent focus on information that may lead to unjust discrimination. Additionally, location data will already be considered sensitive information if it can be used to clearly infer sensitive information.

Biometric information and biometric templates

2.41 Under the Privacy Act, the definition of 'sensitive information' extends to two particular kinds of biometric information: 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification' and 'biometric templates.'

2.42 The use of biometric information like fingerprints to identify individuals is not new. However, in recent times we have seen the capability to carry out automated biometric verification or identification continue to grow. While the most prominent of these technologies is facial recognition technology, this type of automated identification can be undertaken using a growing number of characteristics such as a person's hand geometry, gait or keystroke pattern.[17] Associated with this is the increasing ability to create biometric templates, which are digital or mathematical representations of an individual's biometric information.[18] These characteristics cannot normally be changed, are persistent or unique to an individual and can often be used to infer other sensitive information about individuals. Technological developments have also allowed large amounts of biometric information to be collected indiscriminately and without any direct involvement or even knowledge of individuals. The potentially significant privacy risks associated with biometric information and automated biometric verification and identification are considered in more detail in Part 11 of this submission.

2.43 Given the evolving nature of this capability, we do not recommend defining biometric information or biometric templates in the Privacy Act. This will ensure that the definition is able to flexibly adapt to changing technologies. If a definition is to be included, we suggest that it should be non-exhaustive and sets out categories of biometric information rather than a more specific list of examples. These categories of biometric information could be modelled on similar domestic jurisdictions, which use language such as physical, physiological, biological

[17] *Commissioner-initiated investigation into Clearview AI Inc* (Privacy) 2021 AICmr 54, [122]; *Commissioner initiated investigation into 7- Eleven Stores Pty Ltd (Privacy)* [2021] AICmr 50, [47]; Office of the Victorian Information Commissioner, *Biometrics and Privacy*, OVIC website, July 2019, accessed 3 November 2021; International Organization for Standardisation, (N/A) *Standard ISO/IEC 2382-37: 2017(en)*, ISO website, n.d., accessed 3 November 2021

[18] *Commissioner-initiated investigation into Clearview AI Inc* (Privacy) 2021 AICmr 54, [123]; *Commissioner initiated investigation into 7- Eleven Stores Pty Ltd (Privacy)* [2021] AICmr 50, [49]

and behavioural features.[19] A list of specific types of behavioural information could be included in the explanatory memorandum.

2.44 We appreciate submitters' concerns that additional clarity from the regulator in relation to these terms would be useful. The Information Commissioner's recent determinations in relation to 7-Eleven Stores Pty Ltd[20] and Clearview AI, Inc.[21] consider these definitions in detail, and we expect these will be of significant assistance to APP entities that are considering collecting this sensitive information.

2.45 The OAIC can also provide additional practical guidance on these areas in light of these recent determinations.

De-identified, anonymised and pseudonymised information

2.5 Require personal information to be anonymous before it is no longer protected by the Act.

2.6 Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

2.46 Data is increasingly being used to create benefits for individuals, business and government through data-driven decision-making and the development of innovative, evidence-based products and services. However, many of these activities also involve large amounts of personal information, which may create significant privacy risks. As part of their existing organisational accountability requirements, the OAIC expects APP entities undertaking higher privacy risk activities to consider measures that can be implemented to mitigate these risks and ensure their acts and practices comply with the APPs. These risk mitigation measures will also be important for entities to ensure that their activities meet the fairness and reasonableness requirements at proposal 10.1. Additionally, under proposal 11.1, entities will be required to identify and take reasonable steps to mitigate privacy risks for certain defined restricted practices.

2.47 In appropriate circumstances, de-identification of personal information[22] can be an important privacy protective measure to assist in managing risk. APP entities should consider de-identification as a key data minimisation technique, particularly when undertaking data sharing activities or other projects involving large amounts of personal information. When carried out appropriately, it can allow APP entities to harness the benefits of data use in a privacy protective way, while building trust with the community. However, this must be balanced against the risks of re-identification and the difficulties in robustly de-identifying personal information in some circumstances.

---

[19] See for example Department of Home Affairs, *National Identity Proofing Guidelines*, Department of Home Affairs website, 2016, accessed 3 November 2021, p. 24

[20] *Commissioner initiated investigation into 7- Eleven Stores Pty Ltd (Privacy)* [2021] AICmr 50

[21] *Commissioner-initiated investigation into Clearview AI Inc* (Privacy) 2021 AICmr 54

[22] De-identified is defined at s 6 of the Privacy Act as follows:

> *de-identified: personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.*

2.48 We welcome the Discussion Paper's consideration of the de-identification framework under the Privacy Act and consider the proposals in more detail below.

De-identification and anonymisation

2.49 Proposal 2.5 to replace the term de-identified with anonymised will help to overcome the lack of clarity arising from the dual meaning of the term 'de-identified'. As stated in our submission to the Issues Paper, this term has a distinct meaning under the Privacy Act and a slightly different meaning when used to describe a technical process. This dual meaning has the potential to lead to confusion when interpreting this term.

2.50 The Discussion Paper observes that the word 'anonymous' could signal to APP entities that they are required to meet a higher, irreversible standard reflected by this term.[23] While the proposed amendments to the definition of personal information will naturally have an impact on the required standard for rendering information anonymous, we caution against requiring irreversible anonymisation to meet this definition.

2.51 The legal framework around de-identification under the Privacy Act must provide for sufficiently robust de-identification to manage the risks to individuals. Under the current framework, information will be de-identified 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.

2.52 This approach allows APP entities to take a risk-based approach to de-identification and means that different standards will be required depending on the context in which the information is held. There will be times where APP entities will be required to irreversibly anonymise information before it can be said that this data is no longer personal information. For example, where personal information, particularly sensitive information, is being released publicly, a higher standard of anonymisation will be expected. At other times, a more proportionate response to the specific risks may be to institute appropriate controls or apply technical processes to ensure that information is not personal information in that specific context. While this type of anonymisation may still carry residual re-identification risks, it will also have considerable privacy benefits.

2.53 We are concerned that uniformly applying an irreversible anonymisation standard risks disincentivising this privacy-protective measure where the costs of de-identification are not proportionate in the circumstances. We understand that irreversible anonymisation can be costly and require a high level of sophistication. Uniformly requiring this standard may cause APP entities to not consider using de-identified information because the cost of irreversible anonymisation is disproportionate to the privacy risks in the particular circumstances.

2.54 We recommend that the term 'de-identified' is replaced with 'anonymised', however we do not recommend that this standard should be interpreted as requiring APP entities to irreversibly anonymise information to meet this threshold.

[23] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 3 December 2021, p 30.

Introducing additional obligations for anonymised information

2.55 Where information is only anonymised in a specific context, the test is relative and must apply differently over time, taking into account technical developments and whether the context in which that information is held changes. New re-identification risks may arise if the information is shared or published, misused or subject to a data breach. As such, the OAIC expects ongoing due diligence over this type of information to manage the residual risks.

2.56 We reiterate the recommendations in our submission to the Issues Paper that will help to address the residual risks stemming from a contextual approach to anonymisation and provide greater certainty as to the steps entities should take:

- 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 (see an example of purposes that may be included under this recommendation in relation to the use of AI technologies in Part 17 of this submission).
- 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

2.57 These recommended obligations would require APP entities to manage the risks that arise where the relevant information context changes whilst retaining the benefits of a contextual approach to anonymisation.

Privacy Amendment (Re-identification) Offence Bill 2016

2.58 We support proposal 2.6 to reintroduce the Privacy Amendment (Re-identification) Offence Bill 2016 (Re-identification Offence Bill), subject to several key amendments.

2.59 The OAIC's submission to the Senate Legal and Constitutional Affairs Committee on the Re-Identification Offence Bill noted that:[24]

- This type of prohibition has the potential to be a privacy-enhancing tool by providing a deterrent against the intentional re-identification of certain datasets.
- The introduction of criminal offences and civil penalties in relation to re-identification alone were unlikely to eliminate the risks associated with the publication of datasets.
- To meet the policy objective of the Re-Identification Offence Bill, it is also necessary to increase the accountability on entities that failed initially to appropriately anonymise personal information.

2.60 We suggest that these issues are considered if the proposal to re-introduce the Re-identification Offence Bill is adopted.

2.61 This re-identification prohibition must also be subject to clear and appropriate exceptions to ensure that the Bill does not inadvertently capture entities and researchers re-identifying information for appropriate purposes. Similar to the previous version of the Re-identification Offence Bill, we suggest that exceptions for purposes including research involving cryptology, information security and data analysis are appropriate. There may be other appropriate circumstances, such as where an entity conducts internal testing of the effectiveness of security safeguards that have been put in place to protect the information.

2.62 Consideration should also be given to the changed environment since the Re-identification Offence Bill was last introduced, including the interaction of this framework with other data sharing schemes, such as the Data Availability and Transparency Bill 2020 (DAT Bill).

2.63 Finally, we note that the Re-identification Offence Bill may not be necessary if the additional requirements around anonymised information discussed above and our recommendations about additional organisational accountability in Part 20 of this submission are adopted. We consider that these recommended amendments to the Privacy Act may meet the policy objectives of the Re-identification Offence Bill.

Recommendation 6 – Implement proposal 2.5 to replace the term 'de-identified' with 'anonymised' in the Privacy Act.

Recommendation 7 – 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 8 – 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.

[24] OAIC, *Privacy Amendment (Re-identification Offence) Bill 2016 — submission to the Senate Legal and Constitutional Affairs Legislation Committee*, OAIC website, December 2016, accessed 4 November 2021

Recommendation 9 – Introduce a prohibition on APP entities taking steps to re-identify information that they collected in an anonymised state that is subject to clear and appropriate exceptions including research involving cryptology, information security and data analysis and in order to conduct testing of the effectiveness of security safeguards that have been put in place to protect the information.

Recommendation 10 – 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.

Part 3: Flexibility of the APPs

3.1 Amend the Act to allow the IC to make an APP code on the direction or approval of the Attorney-General:

- where it is in the public interest to do so without first having to seek an industry code developer, and

- where there is unlikely to be an appropriate industry representative to develop the code.

3.2 Amend the Act to allow the IC to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.

Principles-based approach to the APPs

3.1 The principles, risk-based approach of the APPs is the foundation of Australia's privacy protection framework. As noted in our submission to the Issues Paper, we consider that this framework continues to be the most effective regulatory model for the protection of personal information in Australia.[25] We note that other submitters also generally expressed support for retaining the existing principles-based framework.[26]

3.2 The Discussion Paper proposes that some APPs should be amended to include greater legislative guidance as to their application in certain circumstances. We understand that these proposals are intended to clarify the matters that are relevant to determining what 'reasonable steps' are for the purposes of some APPs by elevating factors from the OAIC's APP guidelines into the law.[27]

3.3 For example, the Discussion Paper proposes to amend:

- APP 11.1 to state that 'reasonable steps' includes technical and organisational measures (proposal 19.1)
- APP 11 to include a list of factors that influence what reasonable steps may be required (proposal 19.2)
- APP 8 to clarify what circumstances are relevant to determining what reasonable steps are for the purpose of APP 8.1 (proposal 22.6).

3.4 We consider that the proposals to introduce greater prescription in relation to APPs 8 and 11 may result in inconsistency with the other APPs that are also centred around the 'reasonable steps' test. Introducing greater prescription in relation to certain APPs may result in a fragmented approach to the broader APP framework that is inconsistent with principles of

[25] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, p 38.

[26] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 8 November 2021, p 36.

[27] The APP guidelines set out the Commissioner's interpretation of the APPs including the matters that may be considered when the OAIC exercises its functions and powers under the Privacy Act. The APP Guidelines are available on the OAIC's website at: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines.

reducing complexity and improving clarity by, *inter alia*, ensuring that the same concepts are expressed consistently within the same legislation.[28]

3.5 As recommended in our submission to the Issues Paper, we consider that the aims of these specific proposals can be more broadly achieved by elevating the status of the OAIC's guidance, 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.[29] The OAIC is well placed to consult with regulated entities and other stakeholders when developing or updating guidance material to ensure it is informed by practical considerations that entities are able to comply with. While the guidance would not be binding, the requirement to have regard to the guidance would provide regulated entities with further certainty and clarity around the matters they should consider to meet their compliance obligations under the APPs.

3.6 This approach is consistent with a similar provision under the *Freedom of Information Act 1982* (Cth) (FOI Act), which requires agencies to have regard to guidelines issued by the Commissioner when performing a function or exercising a power under the Act.[30]

3.7 Further, the interpretation of the law, particularly in relation to the matters that are relevant to determining what constitutes 'reasonable steps' under the APPs, may be more appropriately decided by the courts rather than the legislature in the context of principles-based legislation and an increasingly innovative, data-driven economy, where the range of data uses is unable to be accurately predicted and reflected in the law. The changes to the existing privacy regulatory model proposed in the Discussion Paper will likely result in an increased number of privacy determinations and consideration of privacy matters by the courts (see Part 24 (Enforcement) and Part 25 (A direct right of action) of this submission). Judicial decisions around the application of the APPs can be quickly reflected in the OAIC's guidance and serve to provide further clarity as to the application of the law in practice.

3.8 Accordingly, we consider that elevating the status of guidelines issued by the Commissioner will maintain the consistency of the existing principles-based privacy framework and support an efficient and flexible response to changing case law and precedent. The proposed enhancements to the Commissioner's existing APP code-making powers discussed below can also be used to introduce greater particularisation or specificity to the law, where appropriate.

Recommendation 11 – Include a new provision that would require APP entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

[28] Office of the Queensland Parliamentary Counsel (OQPC), *Principles of good legislation: OQPC guide to FLPs*, OQPC, June 2013, accessed 8 November 2021, p 18; AGD, *Clearer Commonwealth Laws: causes of complex legislation and strategies to address these*, AGD, June 2014, accessed 8 November 2021.

[29] See recommendation 16 from OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021.

[30] *Freedom of Information Act 1982* (Cth) s 93A.

Legislative flexibility to adapt the APPs

3.9 While we consider the principles-based approach to the APPs should be retained, we acknowledge that there may be areas that require further certainty of specificity in the law, or that merit specific privacy protections. In these circumstances, the existing APP code-making powers in the Privacy Act provide an effective mechanism to prescribe specific requirements or treatments in relation to certain classes of entities, information or acts and practice where appropriate.

3.10 However, under the existing framework, the Commissioner's powers to develop and register an APP code 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.[31]

3.11 In certain circumstances, it may be challenging to identify a code developer that is generally representative of the entities that are intended to be captured. It may also be difficult to identify a code developer with adequate resources and expertise to develop an APP code that is intended to capture a wide range of entities of various sizes with different personal information handling practices.

3.12 Additionally, a situation may arise where an APP code needs to be developed as a matter of urgency. In these circumstances, it would be beneficial for the Commissioner to have the ability to expeditiously issue a temporary APP code where there is a clear public interest in doing so. An example of a scenario where a temporary APP code may be beneficial is in relation to the new or changed information-handling practices that have arisen because of the response to the COVID-19 pandemic, such as the rollout of Quick Response (QR) codes and the collection of contact-tracing information by entities.

3.13 Recommendation 14 in our submission to the Issues Paper was designed to provide the Commissioner with greater flexibility and discretion to develop APP codes, which would ensure that further specificity and particularisation can be given to the APPs where required and emerging privacy risks can be quickly and efficiently addressed.

3.14 To that end, we support proposal 3.1 to amend the Privacy Act to allow the Commissioner to make an APP code on the direction or approval of the Attorney-General in either of the following two scenarios::

- where it is in the public interest to do so without first having to seek an industry code developer, or
- where there is unlikely to be an appropriate industry representative to develop the code.

3.15 For the avoidance of doubt, we recommend that the Commissioner is able to develop an APP code on the direction or approval of the Attorney-General in circumstances where it is in the public interest to do so without first have to seeking an industry code developer *or* in circumstances where there is unlikely to be an appropriate industry representative to develop the code.

[31] *Privacy Act 1988* (Cth) s 26G.

3.16 Enabling 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) would help to address the challenges associated with identifying a representative code developer that has the necessary capacity to develop a code in circumstances where an APP code is intended to apply to a wide range of entities and personal-information handling activities, and the length of time that this process can take.[32]

3.17 Industry and any other persons likely to be affected must still play a key role in the development of any APP code made by the Commissioner through the mandatory consultation requirements in the code-making framework. For instance, under the existing s 26G(3) of the Privacy Act, before registering an APP code, the Commissioner must:

- make a draft of the code publicly available
- invite the public to make submissions to the Commissioner about the draft within a specified period (which must run for at least 28 days)
- give consideration to any submissions made within the specified period.

3.18 Section 17 of the *Legislation Act 2003* also requires rule-makers to consult before making legislative instruments.

3.19 We also support proposal 3.2 to enable the Commissioner to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.

3.20 A temporary APP code issued quickly in response to changing circumstances would assist affected entities by providing greater clarity and certainty around their privacy obligations and provide confidence to the community that their personal information will be handled appropriately.

3.21 We recommend that the proposed amendments also provide that the consultation requirements in relation to APP codes do not apply to temporary APP codes. This is consistent with the approach taken for temporary public interest determinations under the Privacy Act and temporary codes of practice under New Zealand's *Privacy Act 2020*.[33]

Recommendation 12 – Adopt proposal 3.1 to amend the Act to allow the Commissioner to make an APP code on the direction or approval of the Attorney-General in either of the following two scenarios:

- where it is in the public interest to do so without first having to seek an industry code developer, or
- where there is unlikely to be an appropriate industry representative to develop the code.

[32] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, p 40.

[33] *Privacy Act 2020* (NZ) s 34.

Recommendation 13 – Adopt proposal 3.2 to amend the Act to allow the Commissioner to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.

Recommendation 14 – Ensure that the proposed amendments to enable the Commissioner to issue a temporary APP code stipulate that the consultation requirements in relation to APP codes do not apply.

Emergency declarations

3.3 Amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:

- entities, or classes of entity

- classes of personal information, and

- acts and practices, or types of acts and practices.

3.4 Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

What additional safeguards should be put in place to allow organisations to disclose personal information to states and territories under an Emergency Declaration?

3.22 Special privacy provisions in Part VIA of the Privacy Act take effect if the Prime Minister or the Attorney-General declares an emergency or disaster that affects Australian citizens or permanent residents, either in Australia or overseas.

3.23 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.

3.24 We support proposal 3.3 to allow Emergency Declarations to be more targeted by prescribing their application in relation to entities, or classes of entities, classes of personal information, and acts and practices, or types of acts and practices.

3.25 We also support proposal 3.4 to amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

3.26 We note Commonwealth agencies are already able to disclose personal information to state and territory authorities when an Emergency Declaration is in force. Further, any disclosure

would need to be for a permitted purpose that directly relates to the Commonwealth's response to an emergency or disaster in respect of which an emergency declaration is in force.[34]

3.27 Finally, we reiterate our comments from our submission to the Issues Paper that the Emergency Declaration provisions override the ordinary purposes for which personal information may be collected, used or disclosed under the APPs. In these circumstances, the OAIC considers that it is appropriate that Part VIA is only relied on in limited circumstances. We note 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.[35]

Recommendation 15 – Adopt proposal 3.3 to amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:

- entities, or classes of entity
- classes of personal information, and
- acts and practices, or types of acts and practices.

Recommendation 16 – Adopt proposal 3.4 to amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

[34] *Privacy Act 1988* (Cth) s 80H.

[35] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, p 56.

Part 4: Small Business Exemption

Are there further high privacy risk acts and practices that should be prescribed as exceptions to the small business exemption?

What regulatory impact would this have on small businesses who engage in these acts and practices?

What support for small business would assist with adopting the privacy standards in the Act and realising the benefits of improved privacy practices?

How can small businesses be encouraged to adopt best practice information collection and handling?

To what extent do small businesses that trade in personal information currently rely on the consent provisions?

Would Proposal 9.1 to require consent to be voluntary, informed, current, specific and unambiguous address concerns about the privacy risks associated with the consent provisions of the small business exemption?

Would Proposal 23.2 to introduce a voluntary domestic privacy certification scheme be useful to small businesses that wish to differentiate themselves based on their privacy practices?

4.1 The Australian Government's Digital Economy Strategy aims to make all businesses digital businesses by 2030.[36] Already, 84% of Australian small businesses have online services.[37] This represents a significant proportion of the 2.4 million small businesses currently operating in Australia.[38]

4.2 Online businesses typically handle personal information in the course of providing their services. The shift to digital environments and ubiquitous data collection creates opportunities for more innovative products and services. However, it also creates privacy risks. These risks arise from the amount and sensitivity of personal information that an organisation collects and the number of individuals whose information is collected, rather than being linked to the turnover of a business.

4.3 Data breaches involving personal information can also occur to businesses of any size. Almost two-thirds of businesses reported it is very likely or likely that their organisation would be the

[36] Department of Prime Minister and Cabinet, *Digital Economy Strategy 2030*, Department of Prime Minister and Cabinet, Australian Government, 2021, accessed 24 November 2021.

[37] See AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 8 November 2021, p 41 citing Cynch Security, Deakin University, RMIT, AustCyber Projects Fund, *Big cyber security questions for small business: the state of cyber fitness in Australian small businesses*, Cynch Security, Deakin University, RMIT, AustCyber Projects Fund, January 2021, accessed 24 November 2021, p 4.

[38] This accounts for 95.26% of the 2,402,254 businesses trading in Australia. Based on Australian Bureau of Statistics (ABS), 8165.0 Counts of Australian Businesses, including Entries and Exits, Jun 2017 to Jun 2021, prepared for the OAIC in December 2021. This figure does not take account of small businesses that have opted in to the Privacy Act under s 6EA (697 businesses, as at 6 December 2021) or that are treated as 'organisations' regardless of their turnover, by virtue of ss 6D(4)-(9).

target of a cyber-attack or threat in the next 12 months.[39] In 2021, 56% of cyber security incidents targeted small businesses with less than 1,000 employees.[40] Despite this, implementation of the Essential Eight Mitigation Strategies to reduce cyber security risk is mixed amongst small businesses.[41]

4.4 Although there is a mechanism in the Privacy Act for small businesses to opt-in to coverage under the Act, only 697 small businesses have done so.[42] This suggests that legislative changes are needed to address the privacy risks faced by businesses. Additional opt-in schemes, such as a voluntary domestic privacy certification scheme, may assist in raising privacy standards amongst small businesses that recognise the value of this as a market differentiator. However, the OAIC does not consider this is sufficient to raise the standard of personal information handling across the economy in line with the risks currently posed.

Removing the small business exemption

4.5 The OAIC supports the removal of the small business exemption. The exemption was introduced over 20 years ago in recognition of the potentially unreasonable compliance costs for small businesses that may pose little or no risk to the privacy of individuals.[43] The small business exemption does not apply to specific business types that were considered at the time to pose higher privacy risks.

4.6 The OAIC considers that the small business exemption is no longer appropriate given the increased privacy risks posed by small businesses in the online environment and the regulatory uncertainty created by the application of the exemption. We recommend that the small business exemption is removed, subject to an appropriate transition period to aid with awareness of, and preparation for compliance with, the Privacy Act.

4.7 We acknowledge the concerns of small business representatives about the removal of the small business exemption, including increased compliance costs, particularly in the context of economic recovery following the COVID-19 pandemic, and the imposition of an unjustified regulatory burden on small businesses that do not pose a privacy risk. Representatives also noted that small businesses rely on systems provided to them by larger entities and should not be penalised where these systems fail.

4.8 Although extension of the Privacy Act to small businesses will create additional obligations and some compliance costs, the principles-based nature of the APPs enables businesses to take a risk-based approach to compliance. This will ensure that the compliance burden is proportionate to the risk posed by the particular personal information handling practices of the business. Small businesses will be able to take account of the safeguards placed on personal

---

[39] Varonis, *Australian cybersecurity risk report: understanding Australian business and their approach and attitudes towards cybersecurity*, Varonis, 2021, accessed 24 November 2021, p 12.

[40] G Bassett, D Hylender, P Langlois, A Pinto and S Widup, *2021 Data Breach Investigations Report*, Verizon, 2021, accessed 5 November 2021, pp 89–90.

[41] Australian Signals Directorate (ASD), *Cyber Security and Australian Small Business: Results from the Australian Cyber Security Centre Small Business Survey*, Australian Cyber Security Centre (ACSC), ASD, Australian Government, November 2020, accessed 1 November 2021, pp 15–16.

[42] As at 6 December 2021. Small businesses are able to opt-in to the Privacy Act under s 6EA.

[43] Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), pp 5–6.

information by their service providers when considering the reasonable steps required to comply with relevant APPs. Some submitters noted that a number of small businesses are already required to comply with the GDPR and have been able to meet these regulatory obligations 'without significant financial or resource impost.'[44] These businesses will be well placed to comply with the Australian Privacy Act if the small business exemption is removed.

4.9 As recognised in submission to the Issues Paper, compliance with the Privacy Act can increase the competitiveness of small businesses seeking to engage with larger organisations. Compliance with the APPs may remove the need for larger organisations to impose additional contractual controls and audit requirements, thereby removing complexity and improving the position of small businesses in the marketplace.[45]

4.10 Compliance with the Privacy Act can also benefit small businesses through increased consumer trust. The OAIC's 2020 ACAPS results found that 71% of respondents considered that small businesses should be covered by the Privacy Act. Almost 60% of Australian consumers say they would stop spending money with a brand if they fell victim to a phishing attack involving that brand.[46]

4.11 Finally, removing the small business exemption would bring Australia in line with comparable international privacy regimes. The small business exemption has proved to be one of the major issues for Australia in seeking adequacy under the GDPR.[47] An adequacy decision would require the European Commission (EU Commission) to decide that Australia ensures an adequate level of protection to personal data. Adequacy would allow entities subject to the GDPR to transfer personal data to entities in Australia without any specific authorisation or further steps. The adequacy of Australia's privacy regime was considered by the EU in 2001, but the Article 29 Data Protection Working Party found that further safeguards were needed.[48] One of their key concerns was the small business exemption, as any data transfers to Australian businesses could be to a small business operator that is not subject to the Privacy Act.[49] This is particularly important as transferring data to Australia on a basis other than adequacy faces additional hurdles under the GDPR that may discourage information flows.[50] New Zealand now has a

[44] A Johnston, *Submission in response to the Privacy Act Review – Issues Paper, October 2020*, Salinger Privacy, 20 November 2020, accessed 5 November 2021, p 11; Dr J Siganto, *Response to Review of the Privacy Act — Issues Paper*, Privacy108, 29 November 2020, accessed 5 November 2021, pp 4–5.

[45] Australian Medical Association (AMA), *Privacy Act Review: AMA submission to the Attorney General's Department – the Review of the Privacy Act 1988, a response to the Issues Paper*, AMA, December 2020, accessed 24 November 2021, p 4.

[46] Mimecast, *Brand Trust: one cyberattack is enough to lose consumer trust and custom*, Mimecast, 12 October 2021, accessed 25 November 2021 , p 14

[47] GDPR art 45.

[48] Article 29 Data Protection Working Party, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, Article 29 Data Protection Working Party , 26 January 2001, accessed 24 November 2021, p 3.

[49] Article 29 Data Protection Working Party, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, Article 29 Data Protection Working Party , 26 January 2001, accessed 24 November 2021, p 3.

[50] See *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* [2021] OJ L 199/31 [18]–[22].

similar 'adequacy' provision in its Privacy Act, and although no decisions about comparable safeguards have been made to date, the small business exemption may raise similar concerns.[51]

4.12 The OAIC is well placed to support small businesses to comply with the Privacy Act, including through providing template documents, advisory services and increased proactive outreach to the small business community to address gaps in privacy compliance.

4.13 Additional support from the OAIC would complement existing government support for small business cyber security capabilities. The Australian Cyber Security Centre (ACSC) provides a range of resources for small and medium businesses, including a 24-hour hotline for cyber security advice and an online cyber security assessment tool.[52] The Australian Government is considering other supports, such as a voluntary health check to support small businesses to uplift their cyber security practices,[53] and the Digital Economy Strategy includes funding to uplift the cyber security maturity of small and medium enterprises.[54]

Alternatives to removing the exemption

4.14 The Discussion Paper considers a range of alternative approaches to modifying the small business exemption, with the aim of addressing privacy risks and increasing privacy protections in a targeted way. As set out above, we consider the small business exemption should be removed in its entirety. However, if it is only modified, it is important that the revised exemption addresses privacy risks across the information lifecycle and that the scope of the exemption is clear through unambiguous, objective criteria. This will ensure that individuals, small businesses and the OAIC can easily identify which businesses are captured by the Act.

4.15 If additional types of businesses that engage in high privacy risk acts and practices are prescribed as exceptions to the small business exemption, current OAIC guidance could assist in determining what acts or practices are high risk.[55] For example, small businesses that hold personal information of a large number of individuals or hold sensitive information pose higher privacy risks.

4.16 Considering risk by reference to the number of individuals affected is a standard that is also used in other domestic regulatory regimes. Under the *Security of Critical Infrastructure Act 2018* (Cth), the responsible entity for a critical infrastructure asset has reporting obligations in relation to certain data sets containing the personal information of at least 20,000 people. This

---

[51] *Privacy Act 2020* (NZ) ss 22 (Information Privacy Principle 12), 213.

[52] ACSC, *Small & medium businesses*, cyber.gov.au, n.d., accessed 25 November 2021; the Hon M Price MP and the Hon A Hastie MP, *A hotline to help Australian businesses* [media release], Department of Home Affairs and Department of Defence, Australian government, 25 November 2021, accessed 26 November 2021.

[53] See Department of Home Affairs, *Strengthening Australia's cyber security regulations and incentives– Discussion Paper*, Cyber, Digital and Technology Policy Division, Department of Home Affairs, Australian Government, 13 July 2021, accessed 24 November 2021, pp 47–51.

[54] Department of Prime Minister and Cabinet, *Digital Economy Strategy 2030*, Department of Prime Minister and Cabinet, Australian Government, 2021, accessed 24 November 2021, p 29; iTWire, 'Federal Government funding new Western Sydney Uni Cybersecurity Aid Centre', *iTWire*, 11 May 2021, accessed 24 November 2021.

[55] See OAIC, *When do agencies need to conduct a privacy impact assessment*, OAIC website, 14 September 2020, accessed 5 November 2021; OAIC, 'Chapter 6: Civil penalties', *Guide to privacy regulatory action*, OAIC website, June 2020, accessed 5 November 2021, [6.29]; OAIC, *Guidelines on data matching in Australian Government administration*, OAIC website, 18 June 2014, accessed 6 December 2021, [1.1(a)].

data set attracts reporting obligations because it bears 'the highest level of risk in relation to acts, sabotage, espionage or coercion'.[56] Given the threshold of personal information of at least 20,000 reflects the highest level of risk, the OAIC considers a lower number of individuals or records of personal information should be considered to capture all small businesses posing a high risk.

4.17 We also note that Chapter 11 of the Discussion Paper sets out high risk practices to be considered as restricted or prohibited practices. These could also be considered high risk acts or practices for the purposes of the small business exemption.

Recommendation 17 – 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 18 – If the small business exemption is not removed, further exceptions to the small business exemption should address privacy risks across the information lifecycle and be clear in scope.

Recommendation 19 – If additional types of businesses that engage in high privacy risk acts and practices are prescribed as exceptions to the small business exemption, these should include small businesses that:

- hold personal information of a large number of individuals
- hold any sensitive information, regardless of the number of records
- engage in restricted or prohibited practices.

Removing the consent exception in section 6D

4.18 The Discussion Paper asks whether proposal 9.1 to require consent to be voluntary, informed, current, specific and unambiguous addresses concerns raised by submitters to the Issues Paper about the privacy risks associated with the consent provisions of the small business exemption. These provisions allow small business that trade in personal information to be exempt from the Privacy Act where they obtain the consent of the individual to collect or disclose the information.[57]

4.19 We remain concerned about these consent provisions, despite proposal 9.1, and recommend these provisions are removed.

4.20 The exception to the small business exemption for businesses that trade in personal information was introduced in recognition of the fact that these activities pose a high risk to

[56] Explanatory Statement, *Security of Critical Infrastructure Rules 2018* (Cth), [27].

[57] *Privacy Act 1988* (Cth) ss 6D(7)–(8).

privacy. Businesses that trade in personal information are likely to have large personal information holdings as this forms a part of their core business. The kinds of personal information they hold can range from basic identification information such as name through to sensitive information such as racial or ethnic origin.

4.21 Despite these broad personal information holdings, the effect of giving consent under these provisions is to exempt the small business from all the obligations in the Privacy Act. We consider that this mechanism unfairly places responsibility on the individual to understand the broad implications of their consent and to give up the protections of the Privacy Act in relation to their personal information. Given these broad implications of giving consent, we also consider it would be difficult for a small business to demonstrate they obtained valid consent.

Recommendation 20 – If the small business exemption is not removed, remove the consent provisions in ss 6D(7)(a) and 6D(8)(a)(i).

Part 5: Employee records

To what extent are employers collecting personal information about employees beyond what is reasonably necessary for their functions or activities?

Are employers using or disclosing personal information about employees in ways that do not meet community expectations?

How might the employee records exemption be modified to address the impact of the Full Bench of the Fair Work Commission's decision in *Lee*?

How might the employee records exemption be modified to better protect those records while retaining the flexibility employers need to administer the employment relationship?

To what extent would the fair and reasonable test for the collection, use and disclosure of personal information proposed in Chapter 10 be suitable for the employment context?

To what extent would the current exceptions in APPs 12 and 13 address concerns about the need for employers to conduct investigations and manage employee performance if the exemption were modified?

What would be the benefits and costs associated with requiring employers to take reasonable steps to prevent employees' personal information from misuse, interference or loss?

What challenges or barriers would there be to requiring employers to comply with the NDB scheme in relation to eligible data breaches involving all employee records?

What would be the benefits and limitations of providing enhanced protections for employees' privacy in workplace relations laws?

5.1 Employers hold a range of information about their employees, including health information, which generally receives additional protections under the Privacy Act. However, the Privacy Act does not apply to the private sector where an organisation acts 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.[58]

5.2 The employee records exemption was introduced with the intention that private sector employees' privacy would be regulated by workplace relations laws.[59] However, as recognised in the Discussion Paper, workplace relations laws offer limited privacy protections.

5.3 The COVID-19 pandemic has increased the importance of this issue as employers are collecting additional information about employees in response to changing circumstances. For example, many employers are collecting COVID-19 related information such as vaccination status or

[58] *Privacy Act 1988* (Cth) s 7B(3).

[59] Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [100].

travel history. Increased working from home may lead to the collection of data through workplace surveillance tools.[60]

5.4 We recommend that the employee records exemption is removed to ensure that employees' personal information is adequately protected and to give employees recourse if their information is mishandled.

5.5 We consider that the Privacy Act is a more appropriate regulatory framework to address privacy risks than workplace relations laws. The primary concern of workplace relations laws in setting record keeping obligations is to ensure that employees receive the correct wages and entitlements. This is a different policy focus and objective to the Privacy Act.

5.6 Applying the Privacy Act to private sector employee records will ensure that there is consistency of privacy protection and regulation across the economy, and that employees' personal information is protected across the information lifecycle. These protections would complement and recognise existing requirements in workplace relations law, including through 'required or authorised by law' exceptions to some APPs.

Employee records and notifiable data breaches

5.7 In some cases, the employee records exemption will mean that a private sector employer will not need to notify individuals or the Information Commissioner of an eligible data breach under the Notifiable Data Breaches (NDB) scheme in the Privacy Act. However, private sector employees are still required to notify in some instances, including data breaches involving tax file number (TFN) information or where there is unauthorised access to an employee record by a third party.

5.8 Removing the employee records exemption would provide stronger privacy protections to employees for all data breaches. According to a recent survey, most businesses believe the most likely target for a cyber-attack is sensitive personal data, such as employee information.[61] If employers were required to notify employees under the NDB scheme, affected employees could take action to protect themselves against any potential harms.

5.9 Compliance with the NDB scheme in relation to all personal information is unlikely to create a large compliance burden for employers as they already need to have processes and procedures in place to respond to eligible data breaches where the employee records exemption does not apply. In contrast, the limited application of the employee records exemption is likely to create an increased compliance burden for employers as they have to determine whether the Privacy Act does or does not apply to their particular personal information handling activity.

Application of the Privacy Act if the exemption is removed

5.10 The Discussion Paper notes concerns from submitters to the Issues Paper about the impact that removal of the employee records exemption would have on the ability of employers to manage

[60] See C Taylor, 'Australian privacy laws struggle to protect modern workers', *The Canberra Times*, 11 November 2021, accessed 12 November 2021.

[61] Varonis, *Australian cybersecurity risk report: understanding Australian business and their approach and attitudes towards cybersecurity*, p 10.

their workplaces. These concerns include the implications for workplace performance records and investigations and requirements for consent to collect sensitive information.

5.11 The principles-based nature of the APPs allows employers to take a risk-based approach to compliance. This is supported by exceptions to the APPs that permit the collection of sensitive information and use and disclosure of personal information without consent. For example, an APP entity is permitted to collect sensitive information and use or disclose personal information for a secondary purpose to take appropriate action in response to unlawful activity or serious misconduct.[62] These exceptions will help to facilitate particular aspects of the employment relationship.

5.12 Some submitters raised concerns about compliance with APPs 12 and 13 in the context of an employment relationship. As noted in our submission to the Issues Paper, if the employee records exemption is removed, the Review could consider the exceptions in APP 12 to ensure that they remain appropriate and fit for purpose in an employment context. For example, the Review could consider the need for additional exceptions where an employment reference was given in confidence, or where access would have a substantial adverse effect on the organisation's management or assessment of personnel.

5.13 We do not consider that further exceptions are required to APP 13, as APP entities are already permitted to refuse to make a correction if satisfied that the personal information they hold is accurate, up-to-date, complete, relevant and not misleading having regard to the purposes for which it is held.[63]

5.14 We consider employee records should also be protected through a requirement for collection, use and disclosure of personal information to be fair and reasonable (proposal 10.1). This would place additional checks and balances on employers' handling of personal information in a context where individuals are likely to have limited control over information handling practices. It would also supplement consent as the fair and reasonable requirement would apply even where the APP entity obtains consent. As discussed further in Part 10 of this submission, a fair and reasonable requirement is an important way to raise the standard of information handling and hold entities to account. In the employment context this could address concerns about workplace surveillance that exceeds what is fair and reasonable.

Recommendation 21 – Remove the employee records exemption and consider whether it is appropriate to add additional exceptions to specific APPs to address the particular business needs of employers.

[62] See *Privacy Act 1988* (Cth) s16A(1), sch 1 APPs 3.4, 6.2.

[63] See *Privacy Act 1988* (Cth) sch 1 APP 13.3; OAIC, 'Chapter 13: APP 13 — Correction of personal information', *Australian Privacy Principles guidelines*, OAIC website, 22 July 2019, accessed 15 November 2021, pp 211–212.

Part 6: Political Exemption

What would be the impact, if any, on freedom of political communication and the operation of the electoral and political process in Australia if political parties were brought within the scope of the exemption that currently applies to political representatives and the affiliates of political representatives and political parties?

What would be the benefits and costs of applying some specific APPs to political parties and their affiliates? For example, could political parties and their affiliates be required to have a privacy policy under APP 1 (including information on how individuals can make a complaint about a breach of any applicable APPs), or comply with security obligations under APP 11?

6.1 The objective of the political exemption is to encourage freedom of political communication and enhance the operation of the electoral and political process in Australia.[64] It was introduced to preserve political communication, on the basis that effective representation requires parliamentarians to be able to readily collect, use and disclose information concerning the electorate, its constituents, and the issues relevant to the community.[65]

6.2 We recognise the importance of this objective. However, it is well-recognised by the High Court that some limitations on political communication are justified where those impacts are compatible with and proportionate to the freedom of political communication.[66]

6.3 Since the introduction of the political exemption, the use of technology and voters' personal information in political systems around the world has evolved significantly. As submissions to the Issues Paper note, the current unlimited exemptions for political parties and political acts or practices may now be unintentionally resulting in negative public perceptions of our political system. Changes to the volume and granularity of personal information collected, together with rising incidents of data breaches, create diverse and complex risks to personal and sensitive information in the current political landscape, and demonstrates the need for political parties, acts and practices to be regulated under the Privacy Act.

6.4 This can be achieved in a way that is consistent with freedom of political communication. Recent academic analysis has concluded that the current requirements of the Privacy Act are not incompatible with this freedom.[67] As the Discussion Paper highlights, there is little evidence that data protection laws operating in other democratic countries have had any considerable

[64] *Privacy Amendment (Private Sector) Bill 2000*, Second Reading Speech, 12 April 2000, 15752.

[65] House of Representatives Standing Committee on Legal and Constitutional Affairs, Parliament of Australia, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* 54 [5.14]; 57 [5.26]; 61 [5.44].

[66] *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520; *Levy v Victoria* (1997) 189 CLR 579; *Coleman v Power* (2004) 220 CLR 1; *Monis v The Queen* (2013) 249 CLR 92; *McCloy v New South Wales* (2015) 257 CLR 178.

[67] See M Paterson and N Witzleb, 'Voter Privacy in an era of big data: Time to abolish the political exemption in the Australian Privacy Act', in M Paterson, N Witzleb and J Richardson (eds), *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-targeting*, Routledge, UK, 2020 for an academic legal analysis on why removing the political exemption is highly unlikely to conflict with the freedom of political communication.

impact on political parties' ability to perform their basic democratic roles, including political communication.[68]

6.5 If the political exemption is removed, the principles-based nature of the Privacy Act would achieve proportionate outcomes for the interests of political parties and the privacy rights of Australians. We consider that Privacy Act protections can co-exist with the freedom of political communication and can benefit the political process by promoting transparency and accountability and increased trust and confidence in the political system.

6.6 The OAIC supports the removal of the political parties exemption, in both its broad application to political parties and more limited application to political acts or practices.

The need for privacy protections in the political system

6.7 The OAIC has opposed the political 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. There is a risk that the effect of the exemption on political transparency may damage Australia's system of representative democracy, as well as the public's trust in Australia's privacy protections.

6.8 The community also expects that the Privacy Act should apply to political parties. The OAIC's 2020 ACAPS results show that 62% of the Australian public incorrectly believe that political parties are covered by the Privacy Act,[69] and 74% of respondents stated that political parties should be subject to the Act.[70] A separate study conducted in September 2021 by Resolve Strategic found that 80% of respondents consider that political parties should comply with the Privacy Act.[71]

6.9 An example of the misalignment of public expectations and privacy regulation of political parties is in relation to unsolicited political messaging practices.[72] In August 2021, within 5 days of an unsolicited mass-text message campaign, the Australian Communications and Media Authority (ACMA) had received over 4,000 complaints.[73] In comparison, the ACMA received a

[68] For example, UK political parties are subject to the *Data Protection Act 2018* (UK) and are prohibited from processing personal information unless they have a 'lawful basis' such as 'an activity that supports or promotes democratic engagement'. This allows them to engage in political communication while ensuring adequate privacy protections.

[69] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 59.

[70] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 60.

[71] Resolve Strategic, *Political Campaigning Exemptions*, survey report to the Sydney Morning Herald, p 2, as reported on by D Crowe, 'Voters want to ban politicians from spamming them with texts and calls', *The Sydney Morning Herald,* 26 September 2021, access 20 November 2021.

[72] A recent study by Resolve Strategic has shown that 78% of Australians believe political parties should not send out automated text messages, while 80% believe parties should not call people with "robocalls" that play recorded voice messages. However, we note that these results may be more relevant to the *Spam Act 2003* and the *Do Not Call Register Act 2006* and that some of these concerns may be adequately addressed by amendments to those Acts; Resolve Strategic, *Political Campaigning Exemptions*, p 2.

[73] Shalailah Medhora, 'How is this legal? People are really annoyed by that Craig Kelly SMS', *Triple J Hack*, 2 September 2021, accessed 29 November 2021.

total of 11,178 complaints about spam for the entire 2020-21 reporting year.[74] The number of complaints about this campaign indicates that there is strong community concern about these practices.

6.10 Another issue is the use of voters' personal information for profiling and micro-targeted communications during election cycles. Micro-targeted messaging is a modern tool that may enhance political communication in our digital world. However, it also has potential to be harmful if misused to manipulate voter behaviours or to engage in political redlining, where sensitive information like religious beliefs or ethnicity are used by political parties to avoid communication of certain policies to select demographics.

6.11 There has also been a growing threat of cyber-attacks against political parties in recent years.[75] The amount of personal information stored by political parties make them an attractive target for malicious actors. This emphasises the need for political parties to be subject to appropriate security requirements and to notify individuals when their data has been compromised.

Building privacy into the political process

6.12 As a principles-based framework, the Privacy Act allows entities to pursue their functions and activities within a privacy protective framework. Rather than acting as a prohibition on activities, the Privacy Act will enable political parties and their affiliates (including members of parliament, subcontractors, and volunteers) to continue to perform their unique and essential functions in a more transparent and secure and privacy protective manner.[76]

6.13 Political parties will still be able to undertake many of their current activities under the Privacy Act, for example, collecting personal information about their electorates from the Australian Electoral Commission, their constituents, and other sources, and using that information to communicate with voters within the framework of the Act. Some privacy obligations, like the obligation to ensure that personal information is accurate, up-to-date, and complete, may improve political parties' access to reliable information that will assist them to properly understand the needs of their electorate.

6.14 The principles-based nature of the Privacy Act would be further enhanced to provide proportionate outcomes for both voters and political parties if other proposals in the Discussion Paper and recommendations in this submission are adopted. For example, the proposed requirement for fair and reasonable collection, use and disclosure would provide a

---

[74] ACMA received 49,779 unsolicited communications complaints for the 2020-21 reporting year, consisting of 38,601 telemarketing and 11,178 spam complaints; ACMA, *Annual Report 2020-21*, ACMA, 20 October 2021, accessed 29 November 2021, p 55.

[75] The Federal and NSW Parliament were subjects of cyber attacks in 2019 and 2020 respectively; see M Grattan, 'State actor makes cyber attack on Australian political parties', *The Conversation*, 18 February 2019, accessed 29 November 2021; A Galloway and D Crowe, 'NSW government was target of major cyber attack operation linked to China', *The Sydney Morning Herald*, 19 June 2020, accessed 29 November 2021.

[76] This includes through requirements for privacy policies and notices. We note that several political parties already publish privacy policies that state that they seek to comply with the Privacy Act or follow privacy best practice. See The Australian Greens, *Privacy Policy*, The Australian Greens website, n.d., accessed 29 November 2021; The Australian Labor Party, *Privacy and Legals*, The Australian Labor Party website, n.d., accessed 29 November 2021; The Liberal Party of Australia, *Privacy*, The Liberal Party of Australia website, n.d., accessed 29 November 2021; The National Party of Australia, *Privacy Policy and Disclaimer*, The National Party of Australia, n.d., accessed 29 November 2021.

threshold to guide instances when freedom of political communication would justify unsolicited communication, or to delineate between proportionate and disproportionate micro-targeted communications. Factors such as whether it is an active election period and the content of the communication may be relevant to whether a particular use of voters' personal information is fair and reasonable.

6.15 To the extent that there are concerns about the effect of an enhanced Privacy Act on political communication, further consideration could be given to how the Act will apply to political parties.

6.16 One method may involve the unique functions of political parties, as compared to agencies and organisations, being reflected in the form of exceptions that authorise specific practices in certain circumstances (for example, during an official election period). However, any exceptions for political parties should be limited only to those directly necessary to enable political communication. This would not require, for example, completely exempting political parties, acts or practices from particular APPs. The APPs are structured to reflect privacy obligations across the information lifecycle, as entities collect, hold, use, disclose, and destroy or de-identify personal information. Accordingly, a holistic approach to compliance with the APPs is required to give full effect to the privacy protective framework set out in the Act.

6.17 Alternatively, if considered necessary for abundant clarity, an option would be to remove the political exemption and include a provision that states that the Privacy Act does not apply to the extent that it would infringe on the constitutional doctrine of implied freedom of political communication. The provision could be modelled on similar provisions in the *Spam Act 2003* (Cth) (Spam Act) and the *Telecommunications Act 1997* (Cth).[77] This would be consistent with community expectations and would contribute to the improvement of public trust and confidence in the Australian political system.

Recommendation 22 – Remove the political parties exemption by:

- amending the definition of 'organisation' under the Privacy Act to include a 'registered political party', and
- repealing section 7C of the Privacy Act which exempts political acts and practices for political representatives and affiliates of political parties.

Recommendation 23 – If considered necessary for abundant clarity, include a provision in the Privacy Act that provides that the Act does not apply to the extent that it would infringe on the constitutional doctrine of implied freedom of political communication.

[77] *Spam Act 2003* (Cth) s 44; *Telecommunications Act 1997* (Cth) s 138; Neither provision has been an active subject of any legal proceedings.

Part 7: Journalism exemption

What further evidence is available, such as case studies and any quantitative evidence, to indicate that acts or practices engaged in by media organisations in the course of journalism are presently posing a risk to individuals' privacy?

What impact would introducing a public interest requirement into the journalism exemption have on the free flow of information to the public through the media?

What might be the positive or adverse consequences of applying security obligations under APP 11 to media organisations in the course of journalism?

How could the self-regulation model for media organisations under the journalism exemption be improved?

7.1 The journalism exemption was introduced into the Privacy Act in recognition of the public interest in allowing a free flow of information to the public through the media. The exemption also recognises the importance of protecting personal information through the requirement to commit to published privacy standards. Any changes to the journalism exemption should preserve these policy aims to achieve the best outcome for the community.

A public interest requirement

7.2 The OAIC supports in principle the suggested approach of introducing a public interest test into the journalism exemption. This would ensure that media organisations would only benefit from the exemption where their journalism is in the public interest, in line with the rationale behind the creation of the exemption.

7.3 Introducing a public interest requirement would better align the journalism exemption in Australia with that in the UK *Data Protection Act 2018* (Data Protection Act), which includes a limited exemption for processing personal data with a view to the publication of journalistic material where the publication would be in the public interest.[78]

7.4 Although this change would narrow the scope of the exemption available to media organisations, any disruption to journalism can be limited by leveraging existing understandings of when publication is in the public interest. Many of the privacy standards that media organisations have publicly committed to uphold include public interest considerations.[79] The ACMA has also published privacy guidelines for broadcasters that provide helpful comment on what is in the public interest.[80] Using the public interest standard from

[78] *Data Protection Act 2018* (UK) Schedule 2, Part 5, paragraph 26.

[79] See Australian Press Council, *Statement of General Principles*, Australian Press Council, August 2014, accessed 16 November 2021; Australian Press Council, *Statement of Privacy Principles*, Australian Press Council, December 2015, accessed 16 November 2021; Media, Entertainment & Arts Alliance (MEAA), *Journalist Code of Ethics*, MEAA website, February 1999, accessed 16 November 2021; Commercial Television Industry Code of Practice 2015; SBS Codes of Practice 2014 (revised in July 2019); Commercial Radio Code of Practice 2017; ABC Code of Practice 2019.

[80] ACMA, *Privacy guidelines for broadcasters*, ACMA, September 2016, accessed 16 November 2021, pp 6-7.

these sources will promote consistent protection of public interest journalism and limit the regulatory burden on media organisations.

7.5 It is important that any changes to the journalism exemption continue to facilitate the free flow of information to the public. For example, careful consideration would need to be given as to how this change would interact with proposal 25.1 to create a direct right of action.

7.6 It will also be important to consider any overlap of complaint handling under the Privacy Act and other privacy standards that bind media organisations if the scope of the exemption is revised. For example, the Review should consider the impact of the ACMA finding a media organisation has not breached the privacy provisions of a code because it has acted in the public interest.[81]

Recommendation 24 – Amend the journalism exemption to confine it to journalism that is, on balance, in the public interest, as recognised in existing journalism privacy standards.

Media organisations and APP 11

7.7 Whether or not the scope of the exemption is amended, the OAIC supports the suggestion in the Discussion Paper that all media organisations should be required to comply with the security requirements under APP 11. We consider that it is appropriate for APP 11 to apply to all media organisations, as these obligations would not interfere with the free flow of information to the public. In the context of media organisations, they can encourage good security practices that protect the confidentiality of journalistic sources.

7.8 Security obligations are already reflected in some privacy standards, such as the Australian Press Council's Statement of Privacy Principles, which require constituent bodies to take reasonable steps to ensure personal information is protected from misuse, loss or unauthorised access.[82]

7.9 Applying APP 11.1 to media organisations would also require them to notify individuals of an eligible data breach under the NDB scheme. We acknowledge that this may compromise an investigation or reporting in some cases. To address this, we recommend introducing a similar approach to the UK, such that a media organisation does not need to notify the individual of an eligible data breach where they meet the criteria of the journalism exemption and reasonably believe that notification to the individual would be incompatible with journalism.[83] The media organisation would still need to notify the OAIC of the eligible data breach, regardless of whether they are required to notify the individual.

[81] The ACMA has complaint handling functions in relation to media organisations subject to a code of practice under the Broadcasting Services Act and national broadcasters. See *Broadcasting Services Act 1992* (Cth) ss 149, 151, 170.

[82] Australian Press Council, *Statement of Privacy Principles*, Australian Press Council, December 2015, accessed 16 November 2021, p 1.

[83] *Data Protection Act 2018* (UK) Schedule 2, Part 5, paragraph 26(9)(c)(i).

7.10 APP 11.2 should also apply to media organisations. The principles-based nature of APP 11.2 can accommodate the various purposes for which a media organisation will need to retain personal information. For example, the use of news articles as historical records means that media organisations may justify retention for an extended period of time. This could be explained in OAIC guidance.

7.11 Requiring media organisations to comply with APP 11 is unlikely to add a further compliance burden as they already comply with the Privacy Act in regard to personal information handling that does not occur in the course of journalism. This means that they will already have processes and procedures in place to comply with APP 11 and the NDB scheme.

Recommendation 25 – Amend the journalism exemption to require media organisations to comply with the security requirements under APP 11, with appropriate exceptions to data breach notification obligations.

Part 8: Notice of collection of personal information

8.1 Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.

8.2 APP 5 notices would be limited to the following matters:

- the identity and contact details of the entity collecting the personal information
- the types of personal information collected
- the purpose(s) for which the entity is collecting and may use or disclose the personal information
- the types of third parties to whom the entity may disclose the personal information
- if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection
- the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and
- the location of the entity's privacy policy which sets out further information.

8.3 Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.

8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, at or before the time of collection, or if that is not practicable as soon as possible after collection, unless:

- the individual has already been aware of the APP 5 matters; or
- notification would be *impossible* or would involve *disproportionate effort*.

Is Proposal 8.4 likely to result in any practical difference when compared with the current requirement on entities to take such steps (if any) as are reasonable in the circumstances to notify individuals?

Is Proposal 8.4 sufficiently flexible to permit APP entities to provide no notice where it would be harmful or where an entity collects, uses or discloses personal information on behalf of another entity? If not, how might the requirement be framed so as to increase individuals' awareness of personal information handling while not subjecting individuals to notice fatigue?

8.1 Privacy policies and APP 5 notices are important transparency mechanisms in the Privacy Act. Transparency obligations are 'intended to ensure that individuals have knowledge of, and

choice and control over, how information about them is handled by APP entities.'[84] They play a critical role in privacy self-management and organisational accountability.

8.2 APP 5 notices and privacy policies provide information to the individual to enable them to make choices about what services or products they wish to engage with based on an APP entity's personal information handling practices.

8.3 In addition to supporting privacy self-management, privacy policies and notices are important for organisational accountability. The process of drafting or updating a privacy policy or notice requires APP entities to have strong understanding of the personal information they are collecting and why. This provides an opportunity for the entity to consider the approach they take to meeting the obligations of the APPs and the risks associated with their personal information handling activities.

8.4 As set out in our submission to the Issues Paper, as data handling becomes more complex it can require more detail to explain, increasing the length of the notice.[85] This makes it harder for some individuals to understand the uses of their information and exercise meaningful choice. Equally, individuals engage with an increasing number of APP entities, which can lead to information overload through the sheer volume of material individuals are asked to read.

8.5 Even if individuals are able to engage with and understand this material, the changing nature of the information economy challenges the notion of meaningful choice. Increasingly, schooling, work and socialising are taking place in an online environment. When there are no feasible alternatives to engaging with online services in completing these everyday activities, individuals are required to accept the information handling terms on offer.

8.6 In addition, collections of personal information increasingly impact a broader set of people than the specific individual who is given an APP 5 notice. For example, internet of things devices collect information from all individuals in a given space, not just the information relating to the individual who installed the device and had the opportunity to engage with an APP 5 notice.

8.7 Given these challenges, the measures to promote greater transparency discussed in this Part should sit alongside measures to reduce the information burden on individuals and to raise the standard of information handling across the economy. This will enable individuals to have greater confidence that they will be treated fairly, no matter what they choose. Our submission provides a framework to achieve this:

- Part 10 discusses proposals to ensure fair and reasonable collection, use and disclosure of personal information.
- Part 11 identifies practices that require additional regulation as restricted or prohibited practices.
- Part 20 details organisational accountability mechanisms to ensure that APP entities consider and mitigate the impacts of their information handling practices up front.

---

[84] Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) [109].

[85] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, pp 70-71.

8.8 Adopted together, these measures create strong protections for personal information and minimise the cost of rectification, by building in responsible practices upfront. These measures also enable individuals to have confidence that their information will be handled appropriately, a responsibility that cannot be abrogated by entities through notice and consent.

Notice requirements

8.9 We support proposal 8.1 to include an express requirement for APP 5 notices to be clear, current and understandable.

8.10 This proposal recognises that privacy self-management relies on entities making information about their personal information handling practices accessible and understandable. APP 5 notices need to communicate information handling practices clearly and simply, but also comprehensively and with enough specificity to be meaningful.

8.11 There is currently a disconnect between this aim and current practice. The OAIC's 2020 ACAPS results found that only 20% of Australians both read and are confident they understand privacy policies, which are used by some entities to provide the information of an APP 5 notice.[86]

8.12 The Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry (DPI) Final Report identified numerous practices that make it difficult for individuals to understand how their personal information is being used, such as the length and complexity of documentation, the use of ambiguous language in how personal information is used and complex interlinking documents.[87] This reflects a trend of merging APP 5 notices with privacy policies as a single document or incorporating them as part of broader terms and conditions to be 'agreed to'.[88]

8.13 This evidence base suggests a legislative response is required to ensure that APP 5 notices are more effective privacy self-management tools for individuals.

---

[86]Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p 67. Also see K Kemp, *The absence of competition in the privacy terms of online marketplaces — Submission in response to the ACCC General Online Retail Marketplaces Issues Paper*, Katherine Kemp, 16 August 2021, accessed 3 September 2021; Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021), which suggest that APP 5 notice information is sometimes included in privacy policies or with other information.

[87] See ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, July 2019, accessed 17 November 2021, pp 401–428. Research from Deloitte makes similar findings – the 2018 Privacy Index stated that 'often terms and conditions are complex, heavily reliant on legal language and must be agreed to, before signing up for a product or service'. It also found that 40% of organisations provided insufficient information for consumers to understand how their personal information would be used. See Deloitte, *The symbiotic relationship: Getting the balance right - Deloitte Australia Privacy Index 2018*, Deloitte, 2018, accessed 20 July 2021, pp 8, 16.

[88] See P Leonard, *Notice, Consent and Accountability: addressing the balance between privacy self-management and organisational accountability*, report to OAIC, June 2020, accessed 4 November 2021, pp 17–18; K Kemp, *The Absence of Competition in the Privacy Terms of Online Marketplaces — Submission in Response to the ACCC General Online Retail Marketplaces Issues Paper*, Katherine Kemp, 16 August 2021, accessed 3 September 2021. We note that the practice of incorporating APP 5.2 matters into documents that are publicly available online is not, without more, sufficient to satisfy APP 5. In a recent determination, the Information Commissioner stated 'publishing a privacy policy on a website does not amount to compliance with APP 5' as it is not reasonable to assume that customers will have searched for and read the privacy policy prior to providing their information. See Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) [120]–[121].

8.14 The requirements in proposal 8.1 support privacy self-management by assisting the individual to understand how their personal information is collected, used and disclosed and ensuring they are provided with up-to-date information. They promote user-friendly structuring and plain language while retaining the principles-based approach of the Privacy Act. APP entities will need to consider the appropriate length of their APP 5 notice in order to comply with the requirements for notices to be clear and understandable. The requirement for the APP 5 notice to be current creates a legal obligation for APP entities to update their documentation when their practices change, such as information being used for a new purpose.

8.15 As set out in our submission to the Issues Paper, these notice requirements could be supported through the use of APP codes for particular sectors or personal information-handling practices, or Commissioner-issued guidelines.[89]

Recommendation 26 – Adopt proposal 8.1 for APP 5 notices to be clear, current and understandable.

Matters to be included in APP 5 notices

8.16 The OAIC supports the need to evaluate the matters currently set out in APP 5.2 to ensure that they remain relevant and appropriate for inclusion in APP 5 notices. The Discussion Paper sets out suggested matters in proposal 8.2.

8.17 There are also other proposals in this Discussion Paper that would impact the content of an APP 5 notice, for example:

- proposal 16.2 requires use or disclosure of personal information to influence an individual's behaviour or decisions to be notified as the primary purpose
- option 2 of proposal 11.1 could result in restricted practices being included in an APP 5 notice.

8.18 As recognised in the Discussion Paper, APP 5 notices provide specific information relevant to a particular collection of personal information. Unlike privacy policies, they are not intended to be about how an organisation handles personal information more generally.

8.19 In evaluating what matters should be included in APP 5 notices, the OAIC considers that the primary aim of the notice should be to facilitate privacy self-management. This requires an APP entity to provide individuals with sufficient information for them to make a genuine choice about whether they wish to engage with the entity and equip them with the information they need to understand and access their rights.

[89] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 9 November 2021, pp 73–74.

8.20 To exercise choice, individuals need easy access to the information that is likely to influence their decision to provide their personal information for the collection at hand. This includes understanding:

- the purpose for the collection
- any purposes the information will be used or disclosed for that the individual is likely to find concerning
- what rights they have in relation to the information, including the rights to object and erasure, and where they can find more information on those rights.

8.21 We consider that each of the matters included in proposal 8.2 will further an individual's understanding of these issues.

The OAIC's 2020 ACAPS results provide some insight into the data practices the majority of Australians find concerning, and which are therefore more likely to impact their choice to engage with a service:

70% of Australians are uncomfortable with government agencies and businesses sharing their personal information with businesses in Australia

82% of Australians consider an organisation revealing their information to other organisations to be a misuse of personal information

74% of Australians consider an organisation sending consumers' data to an overseas processing centre to be a misuse of personal information.[90]

Other matters that should be included in APP 5 notices

8.22 In addition to the matters outlined in proposal 8.2, we recommend that the following matters should be included in the APP 5 notice:

- where the individual may not be aware that the APP entity has collected the personal information, that the entity has collected personal information and the circumstances of that collection
- if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised
- whether the APP entity is likely to disclose the personal information to overseas recipients
- the right to withdraw consent where consent has been required for the personal information handling

[90] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, pp 28, 37, 40.

- any purposes the information will be collected, used or disclosed for that the individual is likely to find concerning, including where it will be collected, used or disclosed for a restricted practice, as proposed in option 2 of proposal 11.1.

8.23 Each of these categories of information is necessary to enable privacy self-management, either because it helps the individual to exercise choice or it facilitates access to their rights. For example, notification of whether collection is required or authorised by law means that (where possible) the individual can avoid engaging with a service if they do not want this information collected.

8.24 While we note that this increases the matters to be notified under APP 5.2, this will also involve an element of proportionality as APP 5 only requires APP entities to take reasonable steps to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances.[91] It will be important to retain this flexibility as to what must be notified, as it allows APP entities to limit notice to what is needed in the circumstances. For example, OAIC guidance clarifies that an APP 5 notice does not need to include 'internal purposes that form part of normal business practices, such as auditing, business planning, billing or de-identifying personal information'.[92]

Recommendation 27 – Adopt proposal 8.2, which should be expanded to include the following matters for inclusion in an APP 5 notice:

- if the individual may not be aware that the APP entity has collected the personal information, the fact that the entity so collects, or has collected, the information and the circumstances of that collection
- if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection)
- whether the APP entity is likely to disclose the personal information to overseas recipients
- the right to withdraw consent where consent has been required for the personal information handling
- any purposes the information will be collected, used or disclosed for that the individual is likely to find concerning, including where it will be collected, used or disclosed for a restricted practice.

[91] See for example Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) [110].

[92] OAIC, 'Chapter 5: APP 5 — Notification of the collection of personal information', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 November 2021, [5.16].

Standardised notices

8.25 We support proposal 8.3 for standardised layouts, wording and icons to be considered in the development of APP codes such as the proposed Online Privacy code (OP code).[93] This aligns with recommendation 33 of our submission to the Issues Paper.

8.26 When used properly, standardised layouts, wording and icons can assist individuals to choose the option that best meets their privacy preferences. Consumer research shows that individuals find it difficult to properly compare entities' practices where different entities provide different amounts of information.[94] Standardisation makes it easier for individuals to compare between different services. In addition, it could provide an opportunity for individuals to automatically apply their privacy preferences across services through development of machine-readable icons.[95]

8.27 However, it is important that these mechanisms are not used to obscure data practices by omitting important details of an APP entity's data handling. Oversimplifying information through icons or stock phrases could mislead individuals about how their personal information is handled. Any standardisation should be industry-led and coupled with consumer experience and comprehension testing to ensure the standardised formats meet their objective of assisting individuals.[96] Further research could be conducted into how standardisation mechanisms have been received in jurisdictions that already contemplate the use of standardisation, such as the EU.

Recommendation 28 – Adopt proposal 8.3 for standardised privacy notices to be considered in the development of APP codes, such as the OP code, including standardised layouts, wording and icons, with consumer comprehension testing required to ensure the effectiveness of the standardised notices.

When notice is required

8.28 APP 5.1 currently requires an entity to take such steps (if any) as are reasonable in the circumstances to notify the individuals of such matters in APP 5.2 as are reasonable in the circumstances, or otherwise ensure that the individual is aware of any such matters. This creates a flexible requirement that can adapt to meet the breadth of circumstances in which

[93] Exposure Draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) s 26KC(2)(e)

[94] E Costa and D Halpern, *The behavioural science of online harm and manipulation, and what to do about it*, The Behavioural Insights Team, 15 April 2019, accessed 3 August 2021, pp 35–36.

[95] Several projects have developed in the EU to create machine-readable icons based on the principles in the GDPR. See for example A Rossi and M Palmirani, *DaPIS: the Data Protection Icon Set*, the Legal Design network website, 2021, accessed 1 December 2021.

[96] Some research in this area has been completed by the Behavioural Insights Team – see the Behavioural Insights Team, *Best practice guide — Improving consumer understanding of contractual terms and privacy policies: evidence-based actions for businesses*, the Behavioural Insights Team, 18 July 2019, accessed 26 October 2021.

information may be collected, without the need for specific exceptions to the notification requirement.

8.29 The Discussion Paper explains that proposal 8.4 is designed to be more prescriptive about when notice is required in order to reduce APP entities' discretion to decide whether to provide notice and to increase notification where information is collected indirectly.[97]

8.30 The OAIC supports these aims, however we are concerned that proposal 8.4 will have the effect of requiring notice to be provided in circumstances where it may not be needed, or where it may in fact be harmful.

8.31 The OAIC's APP guidelines outline a limited number of scenarios in which not providing notice under APP 5 may be reasonable under the current law. These include 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 without a notice
- notification may jeopardise the purpose of collection or the integrity of the personal information
- notification may pose a serious threat to life or safety
- notification would be inconsistent with other legal obligations
- notification would be impracticable, including where the time and cost, outweighs the privacy benefit of notification, such as notifying the individual where they have been listed as an emergency contact by someone.[98]

8.32 These scenarios reflect important public interest justifications for not providing notice, including public health and safety. The suggested wording in proposal 8.4 may not allow for an APP entity to not provide notice in these circumstances. For example, health service providers may be required to notify family members if an individual provides them with information about their family history of disease.

8.33 The Review may also wish to consider whether the benefits of increased notification that is likely to result from the implementation of proposal 8.4 may be outweighed by the potential for notification fatigue, which has a detrimental impact on privacy self-management.

8.34 As an alternative approach, we recommend retaining the current wording of APP 5.1 and adopting other proposals in the Discussion Paper and recommendations in this submission to achieve the intended outcomes of this proposal. For example, concerns about the current notice requirements being too flexible could be addressed by our recommendation in Part 3 of this submission for APP entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act.

8.35 If proposal 8.4 is adopted, we recommend including additional exceptions to encompass appropriate circumstances in which notice may not need to be provided. These should be

---

[97] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 8 November 2021, pp 72–73.

[98] OAIC, 'Chapter 5: APP 5 — Notification of the collection of personal information', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 November 2021, [5.7].

developed in consultation with government and industry and at a minimum should recognise the scenarios set out in the APP guidelines.

Recommendation 29 – Retain the current wording of APP 5.1 or introduce additional exceptions to proposal 8.4 to limit notice for recurring collections or where there is a legitimate public interest reason not to provide notice.

Part 9: Consent

9.1 Consent to be defined in the *Privacy Act 1988* (Cth) as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

9.2 Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.

14.1 An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

Are there additional circumstances where entities should be required to seek consent?

Should entities be required to refresh or renew an individual's consent on a periodic basis, where such consent is obtained for the collection, use or disclosure of sensitive information?

Does the proposed requirement for valid consent have any particular implications for different sectors, such as healthcare?

9.1 Under the Privacy Act, APP entities are required to seek consent for the collection, use or disclosure of personal information in a limited set of higher privacy risk circumstances. This includes where an APP entity collects 'sensitive information' or uses or discloses personal information for a purpose other than the primary purpose for which it was collected. Consent is not required for routine personal information handling or where such handling would be reasonably expected. For example, the Act permits collection of personal information where it is reasonably necessary for, or, for agencies, directly related to, the entity's functions or activities.[99]

9.2 This recognises the importance of consent as a privacy self-management tool in high privacy risk situations. The limitations of this mechanism mean that consent should not be relied upon for routine personal information handling.[100]

9.3 The OAIC supports the proposals in the Discussion Paper to strengthen consent. These changes will be enhanced by other proposals in the Discussion Paper and recommendations in this submission, which will have the effect of raising the general standard of personal information handling and the systems that entities have in place to manage consent. In particular, proposals and recommendations:

[99] *Privacy Act 1988* (Cth) sch 1 APP 3.1.

[100] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, pp 71-72.

- that will ensure a fair choice for the individual through fair and reasonable collection, use and disclosure of personal information (discussed in Part 10 of this submission)
- to introduce additional obligations on entities that wish to engage in activities with increased privacy risks (discussed in Part 11 of this submission)
- to increase organisational accountability requirements, which will ensure that entities have the right systems and processes in place to seek valid consent and then handle personal information in accordance with that consent (discussed in Part 20 of this submission).

Defining consent

9.4 The OAIC supports proposal 9.1 to define consent in the Privacy Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action. This proposal aligns with recommendation 34 of our submission to the Issues Paper to 'amend the definition of 'consent' to require a clear affirmative act that is freely given, specific, current, unambiguous and informed'.

9.5 Setting high standards for consent is important to address the limitations of this mechanism and ensure that individuals can genuinely exercise choice in high-risk privacy situations.

9.6 Defining consent aligns with the approach taken in other domestic and international data protection regimes, which specify requirements for consent.[101] The proposed requirements also align with the requirements for consent that must be included in the proposed OP code.[102] The OAIC supports this alignment as a way of reducing the compliance burden on entities. The elements of consent that are proposed reflect the principles-based approach of the Privacy Act and are unlikely to change over time.

9.7 This definition could be supplemented by Commissioner-issued guidance, which will give further clarity to APP entities about the meaning of these terms, while ensuring that this more specific guidance can adapt over time as needed.

Current

9.8 The Discussion Paper asks whether entities should be required to refresh or renew an individual's consent on a periodic basis where such consent is obtained for the collection, use or disclosure of sensitive information.

9.9 The OAIC considers that the period that has elapsed since consent was originally obtained is an element of assessing the currency of the consent. As noted in the section about current and specific consent in the APP guidelines, 'consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely.'[103] This is also reflected in the UK

[101] See, for example, *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r 4.9; GDPR art 4(11).

[102] Exposure Draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) s 26KC(2)(e).

[103] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 November 2021, [B.49].

ICO's guidance, which indicates that the length of time that consent will last depends on the context, including the scope of the original consent and the individual's expectations.[104]

9.10 This context dependent approach to the duration of valid consent is reflected in recent legislative initiatives that include specific duration requirements. For example, under the CDR, the maximum amount of time for an enduring consent is 12 months.[105] The proposed OP code will also include requirements around periodic renewal of consent.[106]

9.11 We consider that specifying a requirement for periodic renewal of consent in the Act is unnecessary given the requirement for consent to be current. We support the use of APP codes or legislation to set specific time periods for the renewal of consent, where required.

Unambiguous indication through clear action

9.12 The current definition of consent makes clear that consent can be express or implied. Express consent is given explicitly, either orally or in writing.[107] Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.[108]

9.13 The ability for entities to rely on implied consent is important in a number of contexts. For example, where a medical practitioner collects a specimen to send to a pathology laboratory for testing, it can be implied from the conduct of the individual that they consent to the laboratory collecting their health information, without the need for the laboratory to seek further express consent from the individual.

9.14 The OAIC considers that the requirement for an unambiguous indication through clear action would ensure that consent can still be implied by entities in appropriate circumstances. In contrast, consent that is given through the use of preselected settings or opt-outs will not be sufficient to meet this requirement as it is ambiguous as to whether the individual did in fact consent or simply did not engage with an opt-out mechanism. We welcome the elevation of our guidance on this issue into law.

Recommendation 30 – Adopt proposal 9.1 for consent to be defined in the Privacy Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

---

[104] UK ICO, 'Consent', *Guide to the UK General Data Protection Regulation*, UK ICO website, 1 January 2021, accessed 6 December 2021.

[105] *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) r 4.14(1)(d).

[106] Exposure Draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) s 26KC(2)(e)(ii).

[107] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 November 2021, [B.36].

[108] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 November 2021, [B.37].

Withdrawing consent

9.15 Proposal 14.1 of the Discussion Paper discusses the withdrawal of consent in the context of the proposed right to object. Entities would be required to take reasonable steps to stop collecting, using or disclosing the individual's personal information where consent is withdrawn or the individual objects, and to inform the individual of the consequences of the withdrawal or objection.

9.16 As noted in the Discussion Paper, consent is currently only required for a limited range of collections, uses and disclosures of personal information. Consent is generally needed for the collection of sensitive information under APP 3.3, unless an exception applies. Consent also functions as an exception permitting APP entities to use or disclose personal information for a secondary purpose under APP 6.1(a). Finally, consent may be relied on to authorise the use or disclosure of personal or sensitive information for the purposes of direct marketing in certain circumstances (APP 7), or as a basis for cross-border disclosures of personal information (APP 8). Consent is not the sole basis for handling personal information in these APPs, and in many cases, the general principle or one of the other exceptions would apply to permit an APP entity's proposed handling of personal information.

9.17 The circumstances in which an individual will be able to withdraw their consent will therefore also be limited to the above situations where consent has been required under the APPs. We support the ability of individuals to withdraw consent in these circumstances. This is an important element of the currency of consent and is reflected in the OAIC's APP guidelines.[109] The right to object would apply to other personal information handling, where it has not been necessary for an APP entity to seek consent because the collection, use or disclosure has been permitted by the main principle or other exceptions.

9.18 We therefore consider that the withdrawal of consent is more appropriately dealt with in relation to the Review's proposed changes to consent requirements, rather than in relation to the right to object.

9.19 Under the existing law, once an individual has withdrawn consent, an APP entity cannot rely on the consent for any future use or disclosure of the individual's personal information, unless another exception to APPs 3 or 6 applies.[110] An APP entity should make the individual aware of the implications of withdrawing consent, such as no longer being able to access a service.[111]

9.20 We support the proposed requirement for an entity to take reasonable steps to stop collecting, using or disclosing the individual's personal information on receiving notice of an objection (see Part 14 of this submission). However, we do not consider that the 'reasonable steps' requirement is an appropriate standard where an individual has withdrawn their consent. We recommend that this should be an absolute right and not be subject to a reasonable steps test.

---

[109]OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 November 2021, [B.51].

[110] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 November 2021, [B.51].

[111] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 November 2021, [B.51].

9.21 If an individual withdraws their consent, another existing exception in APPs 3 and 6 may apply to enable the APP entity to continue to collect, use or disclose the individual's personal information, for example, if the collection, use or disclosure is required or authorised by law. These exceptions align with several of the circumstances the Discussion Paper lists as instances where the reasonable steps test would allow continued collection, use or disclosure. We therefore do not consider it necessary for a reasonable steps threshold to be applied to the withdrawal of consent.

9.22 This is consistent with approaches to consent in other areas of domestic law and data protection law overseas, including the GDPR and Singapore's Personal Data Protection Act.[112] Withdrawing consent is well-recognised in other Australian contexts, such as in healthcare and torts law for access to private property.[113]

9.23 We recommend that the OAIC's guidance on the ability to withdraw consent through an easy and accessible process should be elevated into the law. When an individual wishes to withdraw their consent, they should be made aware of the implications of withdrawing consent. As recommended in Part 8 of this submission, if consent was required for the personal information handling, APP entities should be required to notify the individual of the ability to withdraw their consent.

9.24 This highlights the need for APP entities to be specific about the purposes for which they are collecting personal information under the Act, in order to support compliance with the relevant principles for collection, use or disclosure. Our recommendation in Part 20 of this submission that APP entities should be required to specifically record the purposes for which they are collecting, using or disclosure personal information will assist entities to identify whether they should be seeking consent or whether other exceptions would apply to their proposed personal information handling.

Recommendation 31 – Elevate OAIC guidance on withdrawing consent into the Privacy Act.

Standardising consent

9.25 As acknowledged in the Discussion Paper, it may be impractical to develop standardised forms of consent across all sectors, due to the wide range of contexts in which the Privacy Act applies. We consider that sector-specific standardisation is more appropriate to assist individuals in their comprehension and decision-making in relation to consent, with cross sector alignment to the extent practicable.

[112] GDPR art 7(3); *Personal Data Protection Act 2012* (Singapore) s 16.

[113] In the healthcare context, guidance on informed consent makes it clear that individuals can withdraw consent prior to treatment and that treatment or procedures without consent are unlawful unless otherwise permitted by law. See Australian Commission on Safety and Quality in Health Care, *Fact sheet for clinicians: Informed consent in health care*, Australian Commission on Safety and Quality in Health Care, September 2020, accessed 31 October 2021, p 1. In torts law consent is a defence to trespass to land but can be revoked – see *Cowell v Rosehill Racecourse Co Ltd* (1937) 56 CLR 605.

9.26 The Consumer Data Standards in the CDR are a good example of contextual standardisation. The Inquiry into Future Directions for the CDR considered the value of standardisation within the CDR. The inquiry recognised that developing standardised consents for uses of CDR data can assist consumers by promoting accessible language.[114] However, the inquiry also recognised the risk that standardisation might limit the ability to innovate through new uses of CDR data.[115] As such it is important for entities developing standardised consent processes to engage with industry, interest groups, wider government and to conduct consumer experience testing.[116]

9.27 We agree with proposal 9.2 that APP codes could be used to set out standardised consent processes on a sector-specific basis. For example, where appropriate, the proposed OP code could require standardised layouts, wording, icons or consent taxonomies.[117] As set out in Part 8 of this submission, any standardisation should be industry-led and involve consumer experience testing.

Recommendation 32 – Adopt proposal 9.2 for standardised consent to be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies, with cross sector alignment to the extent practicable, supported by consumer comprehension testing.

[114] The Treasury, *Inquiry into Future Directions for the Consumer Data Right – Final Report*, The Treasury, 23 December 2020, accessed 6 December 2021, pp 127-129.

[115] The Treasury, *Inquiry into Future Directions for the Consumer Data Right – Final Report*, The Treasury, 23 December 2020, accessed 6 December 2021, pp 127-129.

[116] The Treasury, *Inquiry into Future Directions for the Consumer Data Right – Final Report*, The Treasury, 23 December 2020, accessed 6 December 2021, pp 127-129.

[117] See Exposure Draft Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) s 26KC(2)(d).

Part 10: Additional protections for collection, use and disclosure

10.1 A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

10.2 Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances;

- The sensitivity and amount of personal information being collected, used or disclosed;

- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information;

- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity;

- Whether the individual's loss of privacy is proportionate to the benefits;

- The transparency of the collection, use or disclosure of the personal information; and

- If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.

Does the proposed fair and reasonable test strike the right balance between the interests of individuals, APP entities and the public interest?

Does the proposed formulation of the fair and reasonable test strike the right balance between flexibility and certainty?

What impacts (if any) would the fair and reasonable test have on the business operations of entities?

What factors would likely to be more challenging for entities to comply with?

Should entities be required to satisfy each factor of the fair and reasonable test, or should the factors be interpretative considerations in determining whether something is, in its entirety, fair and reasonable?

10.1 In the past, transparency and privacy self-management requirements in the Privacy Act have been sufficient to enable individuals to understand what is happening with their data and take steps to protect themselves from harm when needed. These tools enabled people to easily understand what was happening with their personal information and who it might be disclosed to. With this knowledge, individuals could take steps to protect themselves by exercising control over the handling of their personal information.

10.2 The dramatic increase in the amount of personal information collected, used and disclosed in the digital economy has impacted on the effectiveness of these privacy protective tools. Individuals are constantly receiving information about how their data is being handled, as personal information becomes more important to the operation of modern products and services. Personal information is being increasingly shared between third parties and the information handling activities of APP entities are growing in complexity.

10.3 Transparency and individual choice and control are still essential components of the Privacy Act. However, these mechanisms are limited in their ability to restrain harmful activities. It is unrealistic to expect individuals to consider and understand every collection notice and privacy policy, and to take steps to protect themselves from privacy harms. The burden of understanding and consenting to complicated practices should not fall on individuals alone.

10.4 These issues can be addressed by raising the general standard of personal information handling across the economy. This includes making APP entities more accountable for their information handling practices by requiring them to proactively ensure their activities are appropriate. Introducing more checks and balances will help to build a more trustworthy digital economy and increase the confidence of the Australian community about how their personal information is handled. The community expects more from entities than is currently required by the Privacy Act.

10.5 Proposal 10.1 will help to achieve these important policy objectives by creating a proactive obligation on APP entities to act fairly and reasonably. This will set a baseline standard of information handling that is flexible and able to adapt as circumstances and technology changes. It will also place sensible obligations on entities in the digital economy where personal information is being increasingly bought, sold or transferred between entities that may not have a direct relationship with the individual data subject, or used in increasingly complicated ways that may not be expected by individuals.

10.6 The APPs do not currently require APP entities to ask whether their activities are fair and reasonable or how they will impact individuals. Proposal 10.1 will address this important gap by requiring entities to take more proactive steps upfront to actively consider the foreseeable risks to individuals and take reasonable steps to mitigate these potential impacts. These steps could include providing increased transparency, designing systems differently or providing customers with greater choice and control.

10.7 If proposal 10.1 is adopted, it will be critical to also ensure that entities are required to have appropriate organisational accountability mechanisms in place. This will enable them to effectively assess whether their activities are fair and reasonable. Part 20 of this submission sets out recommendations on how to enhance the existing organisational accountability requirements and support the proposed fair and reasonable reforms.

10.8 The fair and reasonable test will help to create a fairer digital environment that will benefit individuals, APP entities and the wider public interest. These reforms will place individuals at the centre of the privacy framework, which will act as key line of defence to protect the community from privacy harms. Entities that are trying to do the right thing will be able to innovate with confidence and know that they are not competitively disadvantaged when taking a privacy-protective approach to handling the personal information that they hold.

Recommendation 33 – Adopt proposal 10.1 to amend APP 3 and APP 6 to require that the collection, use or disclosure of personal information must be fair and reasonable in the circumstances.

Fairness and reasonableness factors

10.9 An important component of proposal 10.1 is that it is flexible and principles-based, in keeping with the existing APP framework. This fairness and reasonableness test will be able to adapt as circumstances and technology changes, while applying proportionately to the privacy risks posed by an APP entity's activities.

10.10 The terms 'fairness' and 'reasonableness' are widely understood legal concepts. Proposal 10.2 to introduce non-exhaustive, principles-based factors will ensure that these terms are interpreted by APP entities, the OAIC and the courts from a uniquely privacy law perspective. In this data protection context, fairness and reasonableness requires more than mere transparency or the avoidance of covert or deceptive practices.[118] In most circumstances, merely informing an individual about how their information will be handled will not make those activities fair and reasonable.

10.11 These factors will address the risk of an overly narrow, procedural interpretation of proposal 10.1 by ensuring it captures key concepts in privacy law, such as ensuring that the handling of personal information of individuals does not lead to unfair or unjustified impacts. Including factors in the legislation will help to guide entities towards logical and predictable outcomes and promote confidence in how fairness and reasonableness is to be assessed. As highlighted in the Discussion Paper, guidance and determinations from the Commissioner, as well as court judgments will, over time, further shape the interpretation of these terms and the application of this test.

10.12 In our view, these factors should act as interpretative considerations that will guide a holistic assessment of whether the conduct, in its entirety, is fair and reasonable. We do not think that these factors should be viewed as legal tests or thresholds that must be met in every circumstance but rather as relevant to a contextual assessment that requires entities to weigh up a range of considerations. Additionally, some factors such as considering the best interests of the child will not be relevant in every circumstance.

10.13 We have set out more specific observations on the factors outlined in proposal 10.2 below.

[118] Under the current test at APP 3.5, whether a means of collecting information is fair will depend on the circumstances but includes collections that do not involve intimidation or deception and are not unreasonably intrusive. For more information, see OAIC, Chapter 3: APP 3 – Collection of solicited personal information *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 30 November 2021, [3.62-3.63] for more information.

Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstance

10.14 The APPs do not require entities to consider whether information handling is within the reasonable expectations of an individual, except when using or disclosing personal information for a secondary purpose under APP 6.2. In our view, this proposed factor will ensure that the reasonable expectations of individuals play a greater role in the current operation of the APPs by requiring APP entities to consider this as part of a holistic assessment of whether an act or practice is fair and reasonable.

10.15 As highlighted by the Discussion Paper, there may be certain circumstances where this factor will be a key element in ensuring that the collection, use or disclosure is fair or reasonable. This factor will likely be important where:

- sensitive or other higher risk information is being handled
- the primary purpose for which the information is being used, while reasonably necessary for the APP entity's functions or activities, is unusual or unlikely to be anticipated by a reasonably informed individual
- the entity handling the personal information does not have a direct relationship with the individual (for example because they collected the information from a third party).

10.16 APP entities will be able to use existing transparency mechanisms to help to ensure their activities are fair and reasonable by taking additional steps to clearly draw information handling practices to individuals' attention where these may not otherwise be within their reasonable expectations.

10.17 The intersection between this factor and APP 6.2 is considered in more detail below.

The sensitivity and amount of personal information being collected, used or disclosed

10.18 The sensitivity and amount of information being collected, used or disclosed are important factors when assessing the potential impacts of information handling on individuals. As noted in the Discussion Paper, certain types of information, including sensitive information or information relating to an individual's vulnerabilities, should be treated with a higher degree of care.

10.19 We suggest that this factor should be broadened to refer to the 'kinds' as well as the sensitivity and amount of personal information being handled. This will promote consistency with the NDB scheme, which refers separately to the 'sensitivity' and 'kinds' of personal information as relevant factors when determining whether serious harm is likely to occur as a result of a data breach.[119] The explanatory memorandum for the introduction of the NDB scheme states that

[119] Privacy Act, s 26WG(c) & (d).

while these considerations may be similar and can be considered together at times, there will be cases where the 'kinds' and 'sensitivity' of information may give rise to different issues.[120]

10.20 Accordingly, we recommend that this factor clarify that APP entities must consider the kinds, sensitivity and amount of personal information being collected, used or disclosed.

The foreseeable risks of unjustified adverse impacts or harms

10.21 We support this factor, which will focus APP entities' attention on the foreseeable risks of unjustified adverse impacts or harms to individuals or classes of individuals that may occur because of an APP entity's information handling activities. The types of unjustified adverse impacts or harms can be further clarified through judgments, OAIC guidance and determinations.

10.22 The combined effect of the focus on adverse impacts or harms in the fair and reasonable test and our recommendations about organisational accountability in Part 20 of this submission will ensure that the onus will be on APP entities to proactively consider and assess the risks stemming from their information handling activities and take appropriate and reasonable steps to mitigate these possible outcomes. This will have clear positive impacts for the Australian community.

Whether the information handling is reasonably necessary to achieve the functions or activities of the entity

10.23 Reasonable necessity is an important limitation on the collection of personal information under APP 3. This requires that entities only collect personal information that is reasonably necessary for their functions and activities. This concept of reasonable necessity, however, does not apply to the use or disclosure of personal information under APP 6.

10.24 We support this factor, which will require entities to consider whether the personal information that is used or disclosed pursuant to APP 6 is actually reasonably necessary for this purpose. Importantly, an APP entity will also have to determine whether it can minimise the amount of personal information collected, used or disclosed, or even whether it can undertake its functions or activities without using any personal information.

10.25 The intersection between this factor and APP 3 is considered in more detail below.

Whether the individual's loss of privacy is proportionate to the benefits

10.26 Proportionality is an important concept in privacy law stemming from the ICCPR, which underpins the Privacy Act.[121] A recent determination by the Commissioner has highlighted the importance of proportionality in properly applying the collection limitation principle in APP 3.[122]

---

[120] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, p 76 - 77.

[121] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285, [69]-[70] (Bell J).

[122] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021)* [2021] AICmr 50 (29 September 2021).

10.27 Proportionality, along with reasonableness and necessity, are key concepts when determining whether limitations on non-absolute human rights are justifiable.[123] These are principles that the OAIC regularly cites when providing advice on proposed legislation or initiatives, to ensure that any collections, uses or disclosures are reasonable, necessary and proportionate to achieve a legitimate policy aim.[124]

10.28 Proportionality is also a key element in comparable overseas jurisdictions. For example, the concepts of necessity and proportionality are relevant principles for processing under Article 5 of the GDPR, as well as when applying the legitimate interest test under Article 6.[125] Similarly, several cases in Canada have considered proportionality when assessing whether a reasonable person would consider that the purpose for a collection, use or disclosure is appropriate in the circumstances.[126]

10.29 We support this factor, which will formalise this important principle in Australian privacy law.

10.30 The Discussion Paper also refers to three considerations for entities when applying this factor:

- whether the collection, use or disclosure intrudes to an unreasonable extent upon the personal affairs of the affected individual
- whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and
- any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.

10.31 We agree that these are important considerations in assessing proportionality as part of the fair and reasonable test. We recommend that the explanatory memorandum for this amendment highlight that these issues will be relevant for APP entities considering this factor.

The UK ICO's recent opinion on the use of live facial recognition technology in public spaces provides an example of how a flexible fairness requirement can apply to a modern technology. In this opinion, the UK ICO considered issues such as proportionality, necessity and adverse impacts flowing from this processing, but was also able to consider the specific issues presented by this technology such as technical effectiveness, statistical accuracy and the risk of bias and discrimination.[127]

---

[123] Parliament Joint Committee on Human Rights, *Guide to Human Rights*, Australian Government, 2015, accessed 25 October 2021

[124] See for example OAIC *Data Sharing and Release legislative reforms discussion paper — submission to Prime Minister and Cabinet*, OAIC, 17 October 2019, accessed 25 October 2021

[125] See European Data Protection Board *Guidelines 08/2020 on the targeting of social media users*, EDPB, 2020, accessed on 25 October 2021 and UK ICO, Legitimate interests, *Guide to the General Data Protection Regulation (GDPR)*, ico.org.uk, March 2021, accessed 25 October 2021

[126] See discussion in Privacy Commissioner of Canada *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*, Office of the Privacy Commissioner of Canada, May 2018, accessed 25 October 2021

[127] UK ICO, *Information Commissioner's Opinion: The use of live facial recognition technology in public places*, ICO website, 18 June 2021, accessed 11 November 2021, p 37

The transparency of the collection, use or disclosure of the personal information

10.32 We do not recommend that the transparency of the information handling is included as a standalone factor for the fair and reasonable test. While transparency is an essential element under the Privacy Act, we suggest that these fairness and reasonableness factors should focus on the substantive impacts of APP entities' activities and whether they are proportional, rather than procedural issues. As stated above, simply being transparent will not make an act or practice fair and reasonable, and we are concerned that this would send the wrong signal about the scope of proposal 10.1.

10.33 Additionally, the transparency of personal information handling will be adequately captured through the proposed factor about whether the information handling activities are in the reasonable expectations of an individual. This is because appropriate transparency mechanisms may help to ground this reasonable expectation. Equally, deficiencies in an APP entity's transparency practices – whether it is because these notices are overly broad and unspecific, too legalistic, misleading or simply too long – may tend to suggest that information handling activities are not fair and reasonable.

Best interests of the child

10.34 We support this factor, which will ensure that APP entities give specific consideration to the impacts of their information handling activities on children. The exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Online Privacy Bill) also proposes to give limited effect to this proposal through a similar fair and reasonable requirement that requires primary consideration be given to the best interests of the child.[128] This is considered in more detail in Part 13 of this submission.

Additional factors – lawfulness and collective privacy

10.35 We suggest that the Review considers including two additional factors to clarify the scope and application of the fair and reasonable test.

10.36 The first additional factor is whether the collection, use or disclosure of personal information is lawful. We have suggested below that the existing requirement at APP 3.5 that personal information is only collected by fair and lawful means is repealed. Including lawfulness as a factor will ensure that this aspect of APP 3.5 is covered by the fair and reasonable test. It will also make clear that the unlawful collection, use or disclosure of personal information will not be allowed under the Privacy Act. Alternatively, a similar rule could be introduced through the prohibited purposes regime.[129]

10.37 The Discussion Paper also states that recognising the public interest in privacy in the objects of the Privacy Act would highlight that privacy is a collective concern and require APP entities to

[128] Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, s 26KC(6)(e)-(f).

[129] This approach has been taken in the no-go zone regime by the Office of the Privacy Commission of Canada. See Privacy Commissioner of Canada *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*, Office of the Privacy Commissioner of Canada, May 2018, accessed 25 October 2021.

consider if their collections, uses or disclosures of personal information will attract societal harms as part of the fair and reasonable test. This may be captured to some extent in other proposed factors, particularly around avoiding unjustified adverse impacts and ensuring any loss of privacy is proportionate. However, we recommend the inclusion of an additional factor to explicitly clarify the application of the fair and reasonable test to societal harms and the potential impacts on privacy as a collective concern.

10.38 It is important in the digital age that APP entities, regulators and the courts take a more holistic view of privacy breaches beyond the impact on specific individuals. For example, Part 11 of this submission discusses the potentially negative impacts that online personalisation and targeting can have on individuals. Profiling individuals and continually targeting them with harmful or inappropriate content on a large scale can also have cumulative effects that are negative for groups or for society as a whole. This may include the collective impacts of targeting individuals with political content, which may impact their participation in democratic processes, or some news and media content, which may spread misinformation and disinformation. Introducing this factor will ensure that the fair and reasonable test can capture collective and societal harms. It will also require entities to consider these possible impacts of their activities when reviewing their practices under APP 1.

Recommendation 34 – Adopt proposal 10.2 to introduce legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances.

Recommendation 35 – Include the following legislated factors:

- Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances
- The kinds, sensitivity and amount of personal information being collected, used or disclosed
- Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information
- Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity
- Whether the individual's loss of privacy is proportionate to the benefits
- If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child
- Whether the collection, use or disclosure of personal information is lawful
- Whether the collection, use or disclosure of personal information will have a foreseeable impact on the public interest in privacy.

Recommendation 36 – Include the following issues in the explanatory memorandum to this amendment as relevant when considering the factor about ensuring the individual's loss of privacy is proportionate to the benefits:

- whether the collection, use or disclosure intrudes to an unreasonable extent upon the personal affairs of the affected individual
- whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits
- any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual.

Interaction of proposal 10.1 with existing APP 3 and APP 6 requirements

Should the fair and lawful collection requirement in APP 3.5 be subsumed by an overarching fair and reasonable requirement, or should a fair and reasonable requirement apply only to purposes for use and disclosure in APP 6?

How should an overarching fair and reasonable test interact with the exceptions in APP 3.4, APP 6.2 (a) and 6.2(b)-(f)?

10.39 Introducing a fair and reasonable test will have a clear positive impact on privacy protections in Australia. The test will enhance the existing framework and serve as a central consideration in the application of the existing APPs. We recommend that proposal 10.1 is applied in an overarching way as a positive obligation to all collections, uses and disclosure, ensuring that the information handling activities of APP entities are inherently fair and reasonable. This will qualify the way the APPs operate and ensure that they deliver proportionate outcomes.

10.40 It is also essential that this proposal is implemented in a way that is cohesive with the existing APP framework and does not create undue complexity for entities as they make information handling decisions. Introducing this proposal as an overarching test rather as a replacement for the APPs will reduce the impact on entities by not requiring them to learn to navigate an entirely new framework.

10.41 We have set out below our comments on the specific questions in the Discussion Paper around how we envisage proposal 10.1 will interact with the existing APPs.

Interaction of proposal 10.1 with APPs 3.1, 3.2 and 6.2(a)

10.42 APPs 3.1, 3.2 and 6.2(a) and the factors proposed at 10.2 draw on similar privacy concepts such as reasonable necessity and reasonable expectations. However, we do not consider that the fair and reasonableness test should act as a substitute for these existing requirements to handle personal information under the APPs.

10.43 As highlighted above, we consider that the factors at proposal 10.2 should be interpreted as a guide for the holistic assessment of whether conduct is fair and reasonable in the circumstances. Notably, these factors will not act as requirements or standalone tests in isolation. In contrast, APPs 3.1, 3.2 and 6.2(a) impose specific requirements before an APP entity can collect personal information or use or disclose it for a secondary purpose. Replacing these APPs with the fair and reasonable test would likely mean that the factors would have to be elevated to standalone threshold assessments.

10.44 For example, APPs 3.1 and 3.2 provide the threshold requirements for the collection of personal information. These requirements serve as a data minimisation principle by limiting the personal information that an entity may collect to only that which is reasonably necessary for, and for agencies, directly related to, one or more of its functions or activities. This specific data minimisation principle is an important requirement of the Privacy Act, and there is a risk that the more flexible fair and reasonable requirement may not act as a complete substitute for these provisions.

10.45 Similarly, APP 6.2(a) provides an important exception to the primary purpose requirements under APP 6 by allowing APP entities to use or disclose personal information for a secondary purpose where it is within the reasonable expectations of the individual data subject and is related (or directly related for sensitive information) to the primary purpose. These requirements define the relationship or connection that secondary purposes for use and disclosure must have with the primary purpose for collection before this exception can be enlivened. We do not consider that any one factor at proposal 10.2 should be interpreted as a strict requirement in this same way. There would therefore not be this requisite connection between primary and secondary purposes under the Act if APP 6.2(a) was subsumed into the fairness and reasonableness test.

10.46 Additionally, the exceptions at APP 6 each allow for a particular type of secondary purpose. This clarifies and limits the types of secondary uses and disclosures that are allowed under the APPs. Providing this clarity on the secondary purposes that will or will not be allowed helps individuals to understand how their information may be used while allowing entities to operate with confidence. These benefits would be lost if APP 6.2(a) is subsumed into the fair and reasonable test.

10.47 Rather, the role of the fair and reasonable test should be to complement the existing principles and help to increase the standard of information handling under the Privacy Act more generally by ensuring that the impact of information handling on individuals is considered and mitigated up front. Once an entity has undertaken that process, they would apply the exceptions in APP 6 for secondary uses and disclosures related to specific transactions in context.

10.48 For example, although entities will be required to act fairly and reasonably when handling personal information for a primary purpose, no individual factor at proposal 10.2 will be definitive or act as a standalone requirements for processing in all circumstances. On the other hand, where handling information for a secondary purpose, the fair and reasonable test will apply and APP 6.2(a) will impose an additional standard by requiring that the purpose is within the reasonable expectations of the individual and is relevant or directly relevant to the primary purpose. This is similar to our recommendation below about how fair and reasonable intersects with existing consent requirements, which will serve as an additional protection over proposal 10.1.

10.49 In this way, proposal 10.1 would operate like the processing principles of the GDPR. Under this regime, controllers must process personal data pursuant to one of the several lawful bases for processing such as by consent or the legitimate interests tests.[130] All processing under the GDPR, however, must be pursuant to the data processing principles, including requirements to process personal data lawfully, fairly and transparently.

10.50 Accordingly, we do not recommend subsuming the existing APP 3.1, 3.2 or 6.2(a) requirements with the proposed fair and reasonable test and consider they should be applied alongside each other.

Interaction of proposal 10.1 with APP 3.5

10.51 We recommend that APP 3.5 is subsumed with an overarching fairness and reasonableness test which will enable an assessment of both the purpose and means of collection. We do not support the suggestion that the fair and reasonable test only apply to uses and disclosures of personal information but not collections.

10.52 The collection of personal information is an important part of the information handling lifecycle. The processes put in place by APP entities to ensure appropriate collection of personal information is one of the first lines of defence to ensure that individuals' privacy rights are protected.

10.53 As outlined in our submission to the Issue Paper, our regulatory experience suggests that the requirement in APP 3.5 for collection of personal information by fair and lawful means does not go far enough, as it primarily applies to the means of collection and may not extend to prevent other inappropriate practices.

10.54 Replacing APP 3.5 with the proposed fair and reasonable test will help to close this gap by extending the existing protection more clearly beyond the means of collection.

10.55 Additionally, if the fair and reasonable test was only applied to uses and disclosures, this would mean that there would be similar but slightly different tests in APPs 3 and 6, which will create regulatory uncertainty. As stated above, applying proposal 10.1 to collection, use and disclosure would bring the Privacy Act into line with the GDPR.

Interaction of proposal 10.1 with consent mechanisms in APPs 3.3 and 6.1(a)

10.56 Consent is an important part of privacy self-management. However, as highlighted by the OAIC and other submitters to the Issues Paper, there are limits to the level of protection that consent provides to individuals in the digital age. Individuals may not always be well placed to assess the risks and benefits of allowing their personal information to be shared or may simply feel resigned to consent because of an actual or perceived reliance on a service.

10.57 Given these concerns, it is essential that an APP entity cannot seek to 'consent out' of its fair and reasonable requirements. This would run counter to one of the policy objectives for proposal 10.1 by placing a high burden on individuals rather than putting the onus on entities to establish appropriate organisational accountability mechanisms to ensure their processes

[130] GDPR, Article 6.

are fair and reasonable. It would also position individual consent as overriding the important factors contained in proposal 10.2 and be inconsistent with equivalent protections in Europe, the UK and Canada. For example, while consent is one basis for processing under the GDPR, all information handling must still be undertaken in accordance with the lawful, fairness and transparency principle.[131]

10.58 Accordingly, we recommend that the fair and reasonableness test apply in addition to where an individual has consented to the specific information handling under APPs 3.3 and 6.1(a). We expect that the valid consent of an impacted individual to an information handling practice will be relevant when assessing whether an activity is fair and reasonable. Seeking consent from individuals, may be one way of seeking to reduce the privacy intrusion and demonstrating compliance with this test.

10.59 Proposal 10.1 will also have an important role to play in uplifting consent processes. For example, this will help to ensure that where consent is sought from an individual, the choices being offered will be fair and reasonable options. These benefits will not be achieved if consent takes precedence over fairness and reasonableness requirements.

Interaction of proposal 10.1 with APPs 3.4 and 6.2(b)-(e)

10.60 In our view, the fair and reasonable test could be applied alongside APP 3.4 and APP 6.2(b)-(e). This would enhance the application of these exceptions by encouraging entities to act proportionately by considering the extent of the information that is required and the way it will be handled. For example, while the permitted general situations at s 16A of the Privacy Act would allow collection, use and disclosure in defined circumstances, proposal 10.1 would ensure that the specific activities undertaken by an APP entity pursuant to this exception are conducted fairly and reasonably. This could include ensuring that an entity cannot covertly collect personal information pursuant to a permitted general situation, except in appropriate circumstances.

Recommendation 37 – Adopt proposal 10.1 alongside the existing APP 3.1, 3.2 or 6.2(a) requirements.

Recommendation 38 – Subsume APP 3.5 within the overarching fair and reasonable requirement of proposal 10.1.

Recommendation 39 – Ensure that proposal 10.1 applies to collections, uses and disclosures of personal information.

Recommendation 40 – Clarify that the fair and reasonableness test applies in addition to where an individual has consented to the specific information handling under APPs 3.3 and 6.1(a).

[131] GDPR, Article 5 and 6.

Requirements on third party collections

10.3 Include an additional requirement in APP 3.6 to the effect that that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

10.61 We support proposal 10.3, which adopts recommendation 17 from our submission to the Issues Paper and will provide an important protection for individuals where personal information is collected from a third party. We agree that Commissioner-issued guidelines could assist with practical application of this requirement by providing examples of reasonable steps that could be taken. The OAIC is well placed to work with stakeholders to develop such guidance.

Recommendation 41 – Adopt proposal 10.3 to include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Defining primary and secondary purpose

10.4 Define a 'primary purpose' as the purpose for the original collection, as notified to the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.

10.62 Purpose specification is an essential principle that underpins privacy laws globally. The purpose specification principle, together with the use limitation principle, requires that individuals be notified of the purposes for which their personal information was collected and limits the uses of information to those purposes unless an exception applies.[132] These principles promote data minimisation by ensuring that information is only collected and held where there is a valid purpose for its use.

10.63 The purpose specification and use limitation principles are mostly given effect through APP 6 in the Privacy Act. This restricts the use of personal information to the primary purpose of collection, except where a valid exception applies. These exceptions notably include additional obligations when using information for a secondary purpose, including consent requirements

[132] Organisation for Economic Co-Operation and Development, *The OECD Privacy Framework*, OECD, 2013, accessed 24 November 2021, p 14-15.

or requiring that the purpose is within the reasonable expectations of an individual.[133] However, the ACCC's DPI Final Report highlighted some limitations in this framework, and noted that certain digital platforms were setting out vague or overly broad primary purposes in their privacy policies.[134] Submitters to the Issues Paper also considered that the concepts should be defined or further clarified.

10.64 We support the need for clarity and certainty in this area. However, we are concerned that defining these terms in the Privacy Act will have unintended negative consequences and create uncertainty in the application of the APPs. We are also concerned that encouraging APP entities to classify a greater range of uses and disclosures as primary purposes may exacerbate the limitations in this framework identified in the DPI Final Report.

10.65 We consider that the objective of proposal 10.4 can be more effectively achieved by adopting other proposals from the Discussion Paper and recommendations in this submission, as discussed further below. Taken together these proposals will also serve to provide a more targeted response to concerns about APP entities describing overly broad or unspecific primary purposes.

10.66 The two elements of proposal 10.4 are considered separately below.

Definition of primary purpose

10.67 The potential primary purposes for which an APP entity can use and disclose personal information are broad, varied and emerging. So too are the potential privacy risks that may attach to these purposes. As the Discussion Paper highlights, OAIC guidance states that the scope of a purpose should be determined on a case-by-case basis and, in the case of ambiguity, should be construed narrowly.[135]

10.68 The definition of primary purpose in proposal 10.4 is intended to provide additional certainty and encourage APP entities to classify a greater range of uses and disclosures as primary purposes. However, we are concerned about the potential unintended consequences of the definition linking the primary purpose to what is notified to the individual.

10.69 The OAIC's APP guidelines establish that assessing the primary purpose for collection is an objective test informed by the circumstances surrounding the collection.[136] This contextual assessment is an important part of the primary purpose test by ensuring that it is flexible and able to mould to an APP entity's circumstances. At the same time, the objective nature of the test places crucial limits on the abilities of entities to subjectively define the primary purpose of collection.

10.70 Practically speaking, when the Commissioner makes a determination, they are required to come to an objective view on what the primary purpose for collection actually was in the

---

[133] Privacy Act, APP 6.1 and 6.2.

[134] ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, July 2019, accessed on 24 November 2021, p 438.

[135] OAIC, 'Chapter B – Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed on 3 December 2021.

[136] OAIC, 'Chapter B – Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 December 2021, [B.99]. See also 'WZ' and CEO of Services Australia (Privacy) [2021] AICmr 12 (13 April 2021) at [148].

circumstances. In these circumstances, the Commissioner is not bound by the subjective views of the relevant APP entity. Linking the primary purpose to the purpose notified to the individual will detract from the objective nature of this assessment and give entities greater control over the primary purpose recognised under the APPs. It is also not clear how this definition will apply where notice is not necessary under APP 5 or where the Commissioner determines that the primary purpose(s) included in an information collection statement are invalid.

10.71 We also have concerns about linking the primary purpose to transparency requirements, which may not have the effect of promoting purpose specification and use limitation. APP entities will still be able to define their own primary purposes under this proposed definition, so will not be prevented from including overly broad or unspecific primary purposes in their notices. The link with notices will also place the onus on individuals to understand these notices and protect themselves from privacy harms.

10.72 The Discussion Paper notes that this proposal will encourage APP entities to classify a greater range of uses and disclosures as primary purposes. However, this may not be a privacy-enhancing outcome, given the protections available for individuals through the additional requirements on uses and disclosures that fall outside a primary purpose, for secondary purposes.

10.73 Further, this proposal may incentivise an overly legalistic approach to defining primary purposes in an APP 5 notice. APP 5 notices are intended to provide an individual with relevant information to help them understand the nature of the proposed handling of their personal information. This will necessarily entail a clear and understandable statement of the APP entity's primary purpose for collection. It is reasonable and expected that an entity's description of its primary purpose for the regulator or for the courts would be a more legalistic statement than that which is contained in an APP 5 notice for individuals.

10.74 Linking the purposes notified in an information collection statement to the authorisation to use and disclose personal information under APP 6 will likely incentivise APP entities to approach their notifications from this more legalistic standpoint. This is because entities may want to ensure they are able to undertake their activities in compliance with APP 6, rather than seeking to provide clear and understandable information to individuals.

10.75 Similarly, encouraging entities to classify a greater range of uses and disclosures as primary purposes will likely increase the length of notices to include an extensive list of activities and/or cause entities to define their primary purposes very broadly and ambiguously to encompass a wide range of different activities.

10.76 We consider that the most effective way to address these concerns and clarify the application of the primary purpose concept is by adopting our recommendation in Part 3 of this submission to elevate the status of the OAIC's guidance generally by requiring entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act. Our guidance could provide further clarity on the meaning of primary purpose, taking into account any relevant court judgments and Commissioner determinations, while also retaining the objective test.

10.77 The amendments to APP 3 to require that purposes be specific, as recommended in Part 20 of this submission, will also help to provide clarity and address the issue of overly broad or vague primary purposes. We recommend amending APP 3 to expressly require entities to determine,

at or before the time of collection, each of the known specific purposes for which the information is to be collected, used or disclosed and to record those purposes.[137] If an entity sought to use or disclose personal information for a new purpose, it would need to record that new purpose before undertaking the use or disclosure. While this recommendation will not replace the current objective test around primary and secondary purposes, it will encourage entities to take a privacy by design approach by requiring that they have a clear and specific purpose in mind for the subsequent handling of the information. This will also be a relevant consideration for the Commissioner in making an objective assessment of the primary and secondary purposes associated with an information collection.

10.78 Several other proposals in the Discussion Paper will also help to ensure that APP entities do not rely on overly broad primary purposes to try to justify expansive information handling activities. This includes proposal 10.1 to introducing the fair and reasonable test, and the additional enforcement powers proposed in the Discussion Paper and recommended in Part 24 of this submission, which will allow the Commissioner to effectively pursue regulatory action.

Definition of secondary purpose

10.79 An important exception to APP 6 allows the use or disclosure of personal information for a secondary purpose where an individual would reasonably expect this use or disclosure and the secondary purpose is related to the primary purpose (or directly related for sensitive information).

10.80 The proposed definition, which will limit secondary purposes to those directly related or reasonably necessary to support the primary purpose, is intended to limit overly broad secondary purposes. However, we are concerned that it will also have the unintended consequence of preventing the use or disclosure of personal information for widely accepted secondary purposes. Common examples of this may be the use of personal information for the purposes of an APP entity undertaking its accounting or improving its internal processes. These uses may often not be directly related or reasonably necessary to support a primary purpose but still be essential to the entity's functioning and reasonably expected by the community.

10.81 As stated above, we consider that other proposals in this Discussion Paper and recommendations in this submission will address the issues of concern in relation to secondary purposes and assist the Commissioner to take regulatory action in relation to overly broad secondary purposes.

Recommendation 42 – Consider alternative solutions for meeting the objectives of proposal 10.4, including adopting:

- the OAIC's recommendation to include a new provision that would require APP entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities under the Privacy Act

[137] Article 5(b) of the GDPR includes a purpose limitation principle requiring that personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- the OAIC's recommendation to amend APP 3 to expressly require entities to determine, at or before the time of collection, each of the known specific purposes for which the information is to be collected, used or disclosed and to record those purposes
- proposal 10.1
- the additional enforcement powers proposed in the Discussion Paper and recommended in Part 24 of this submission.

Part 11: Restricted and prohibited practices

11.1 Option 1

APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:

- Direct marketing, including online targeted advertising on a large scale*
- The collection, use or disclosure of sensitive information on a large scale
- The collection, use or disclosure of children's personal information on a large scale
- The collection, use or disclosure of location data on a large scale
- The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software
- The sale of personal information on a large scale
- The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale
- The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or
- Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.

*'Large scale' test sourced from GDPR Article 35. Commissioner-issued guidance could provide further clarification on what is likely to constitute a 'large scale' for each type of personal information handling.

Option 2

In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice.

Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices (see 'Right to Object'), or by ensuring that explicit notice for restricted practices is mandatory.

11.1 In the digital economy, we recognise that there is value in the Privacy Act taking a more proactive, outcome focused regulatory approach for certain higher risk activities. This will provide clearer protections for individuals while giving the regulated community additional certainty and confidence in what is required of them. It will also complement the existing flexible, principles-based APPs by signalling that there will be higher expectations when engaging in higher risk activities.

11.2 We support the introduction of a restricted and prohibited practices regime, which will allow for this ex-ante regulatory approach to privacy regulation in Australia. Our observations on how

the restricted and prohibited practices framework could operate in the Privacy Act are set out below.

Restricted practices

11.3 We support a restricted practice regime modelled on option 1 of proposal 11.1, which will provide additional protections for individuals while giving APP entities a clearer idea of the steps that are required before undertaking these proscribed activities. This regime will also intersect with and enhance the existing APPs and proposal 10.1 of the Discussion Paper to introduce a fair and reasonable test.

11.4 Option 1 proposes two flexible steps for APP entities that will help them to determine whether their activities for a restricted practice are fair and reasonable. APP entities must first take reasonable steps to identify privacy risks with the act or practice. We consider that conducting a thorough Privacy Impact Assessment (PIA) when planning to undertake a restricted practice, and periodically after that, may be an effective way to satisfy this requirement.

11.5 Having clear risk-based organisational accountability structures in place under APP 1 will also be essential to lay the foundation to assess the risks associated with these restricted practices. OAIC guidance will be able to help entities to identify what specific considerations may be necessary for each restricted practice when developing their internal systems and structures and undertaking a PIA.

11.6 Crucially, the second step will then require APP entities to implement measures to mitigate the risks identified. The necessary steps required to mitigate the risk will depend on the specific circumstances, but entities will be able to draw on core privacy concepts and existing APP requirements to help to identify steps that may mitigate these risks, such as collecting less personal information, only using de-identified information, providing enhanced notices or requiring consent. While the precise steps needed to mitigate the risks will change depending on the circumstances, the Commissioner would be well placed to work with stakeholders to develop practical guidance on what steps may be appropriate for each restricted practice. Our recommendation in Part 3 of this submission to elevate the status of the OAIC's guidance generally by requiring entities to have regard to any guidelines issued by the Commissioner when carrying out their functions and activities will also supplement the restricted practices framework.

11.7 Where an entity is able to identify the privacy risks associated with a restricted practice and mitigate them to a reasonable extent, this activity will be fair and reasonable. Simply identifying the privacy risks but failing to then successfully mitigate them would mean that the restricted practice would not be fair and reasonable in the circumstances. This framework will help entities to identify situations where they are unable to appropriately mitigate the privacy risks in relation to the proposed act or practice and would therefore not be able to undertake that activity.

11.8 The explanatory memorandum to this amendment should make clear that PIAs and other risk mitigation measures may be required in both the restricted practices framework and to demonstrate compliance with APP 1 more broadly.

11.9 To provide an additional layer of organisational accountability and wholly achieve the policy objective behind the restricted practices regime, we recommend that this framework should be supplemented by two additional measures.

11.10 APP entities undertaking a restricted practice should be required to conduct a periodic independent audit to ensure that they have identified the privacy risks associated with these activities and taken appropriate steps to mitigate those risks. This will provide an additional level of assurance and ensure that the risks stemming from the restricted practices are being appropriately addressed. Periodic internal and external review will help to account for changes to the practice or environment and ensure ongoing alignment with guidance from the OAIC. As suggested by the Discussion Paper, and building on our recommendation in Part 20 of this submission, evidence of the reasonable steps taken to identify privacy risks associated with a restricted practice, along with any independent audit reports, should be made available to the Commissioner on request.

11.11 The restricted practices framework should also be supplemented with a code-making power that will allow for the creation of enforceable requirements where there is evidence that industry is not following the OAIC's guidance and taking appropriate steps to mitigate privacy risks from restricted practices. Consultation with relevant stakeholders will ensure that any code is appropriately tailored and proportionate. This code-making power could be modelled on proposal 3.1 which allows the Commissioner to make an APP code on the direction of the Attorney-General.

11.12 As set out below, for some of the proposed restricted practices it is already apparent that there are instances where OAIC guidance may not be sufficient to mitigate the risk. The Review provides an opportunity to adopt regulations that set out specific requirements for these activities.

Acts or practices subject to the restricted practices regime

11.13 The restricted practices suggested in option 1 of proposal 11.1 cover a broad and diverse set of activities that are becoming increasingly common in the digital economy. These provide a starting point for a discussion around the acts and practices of most concern to the Australian community, where additional compliance requirements or a prohibition may be warranted.

11.14 We have set out observations on the proposed restricted practices, including suggested amendments to clarify their application and ensure that they are appropriately targeted. We have also recommended building on the restricted practice requirements and suggest that in relation to acts or practices where the privacy risks cannot be sufficiently mitigated, that these activities should be expressly prohibited. We consider that the use of facial and other similar technologies recognition in certain contexts, as well as data scraping of personal information from online platforms, should be identified as prohibited practices.

Direct marketing, including online targeted advertising on a large scale

11.15 We support this restricted practice. As noted in Part 16 of this submission, significant privacy risks have emerged from the use of high volumes of data, often involving personal information, by advertising technology (adtech) services delivering targeted or personalised advertising online. The use of personal information for this purpose is also of concern to the Australian

community, with over half of Australians uncomfortable with targeted advertising by digital platforms and online businesses based on what they have said and done online.[138]

11.16 We suggest that this restricted practice should not be subject to the 'large scale' test where an APP entity collects, uses or discloses personal information for the purpose of online targeted advertising. The online adtech ecosystem is driven by the sharing of personal information between many different participants. This means that while an APP entity may only engage in targeted advertising on a small scale or share a smaller amount of personal information it holds with the wider adtech ecosystem, this information may nevertheless be shared very widely.

11.17 We also note that online targeted advertising may be captured by our proposed restricted practice focusing on online personalisation.

The collection, use or disclosure of sensitive information on a large scale

11.18 We support this restricted practice, which will formalise our current expectations that APP entities are held to a higher standard when holding large amounts of sensitive information.

The collection, use or disclosure of children's personal information on a large scale

11.19 Part 13 of this submission addresses the challenges and risks associated with handling the information of children who are particularly vulnerable online given limitations in their basic and digital literacy, their cognitive abilities and their capacity for mature decision-making.[139]

11.20 This submission makes several recommendations that will help to address the privacy risks associated with handling children's personal information. These privacy risks will also be a major area of focus in the proposed OP code, which will introduce additional protections for children's information, including enhanced notice and consent requirements and an obligation to handle children's information fairly and reasonably.

11.21 We support this restricted practice, which will provide additional protections for children's information when handled on a large scale. Any additional rights and obligations should be consistent with the protections in the OP code.

The collection, use or disclosure of location data on a large scale

11.22 We support this restricted practice, which will provide valuable protection for individuals for a category of personal information that is being increasingly collected and shared in the digital age.

11.23 Location 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

[138] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p. 29

[139] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p. 8

were uncomfortable with digital platforms/online businesses tracking their location through their mobile or web browser.[140]

11.24 There are several factors that may impact on the risks posed by the collection, use or disclosure of personal information. For example, the accuracy of the location information or way that the location information is used will often increase risks from this data.[141] There will also be higher risks where the location reveals categories of sensitive information, such as being present at places of worship or medical centres. Technical controls around the way location information is stored will also affect the risk, such as whether the identifier attached to the information is temporary and how often this identifier is rotated. Location information may also be very difficult to de-identify or may have a high re-identification risk.

11.25 Using this information in a seamless way can have benefits for individuals, such as the easy use of ride sharing or food delivery through mobile phone applications. At the same time, the inappropriate collection, use and disclosure of location information, can lead to potentially serious privacy abuses and harms.[142] The proposed restricted practices regime will provide flexibility for APP entities to consider the context in which they are handling location information and take appropriate steps, informed by the OAIC guidance, to mitigate these risks.

11.26 At the same time, we consider that an important privacy risk in the digital age has come through the increased collection of location information through mobile phones and the growth in the market for sharing this information between entities.[143] The Review provides an opportunity to create additional regulations to address this issue, for example, by creating stricter requirements on the sharing of location information for purposes that are not reasonably necessary for the provision of the service or product, subject to appropriate public interest exceptions. Given the higher risks of harm and re-identification risk, the Privacy Act could more closely regulate the use and disclosure of precise location information, whether or not an individual is identified or reasonably identifiable from that information.

The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software

11.27 We recommend that this proposed restricted practice is reframed to focus on the use of biometric information for the purposes of automated biometric identification or verification. This reflects the very real community concerns about the potential privacy risks stemming from

---

[140] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p. 79.

[141] For example, according to a report by the Norwegian Consumer Council, location data is now sufficiently varies and precise that it can permit a consumer to be tracked indoors to the specific floor of a building. See Forbruker Radet, *Out of Control: How consumers are exploited by the online advertising industry*, Forbruker Radet, 14 January 2020, accessed on 8 December 2021, p 96.

[142] See for example M Boorstein, M Iati and A Shin, *Top U.S. Catholic Church official resigns after cellphone data used to track him on Grindr and to gay bars*, Washington Post website, 21 July 2021, Accessed on 5 December 2021; E Bevin, *Man pleads guilty to talking and controlling ex-girlfriend's car with his computer*, ABC News, 7 November 2019, accessed on 6 December 2021; J Keegan, A Ng, *The Popular Family Safety App Life360 Is Selling Precise Location Data on Its Tens of Millions of Users*, The Markup website, 6 December 2021, accessed on 8 December 2021

[143] See for example J Keegan, A Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup website, 30 September 2021, accessed on 24 November 2021; J Valentino-De Vries, N Singer, M Keller and A Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, New York Times website, 10 December 2019, Accessed on 5 December 2021

the handling of this biometric information and biometric templates through the use of technology to automatically recognise human features. This includes facial recognition software but also systems that can recognise individuals through other traits such as gait, fingerprints or voice.

11.28 We have recommended that the Review consider a prohibited practice focused on the use of automated biometric verification and identification systems below.

The sale of personal information on a large scale

11.29 The free flow of personal information has become common in the digital economy. However, the OAIC's 2020 ACAPS results found that there was concern in the community about this practice, with 69% of parents being uncomfortable with the selling of personal information about a child to third parties and 77% of individuals suggesting they should have a right to object to certain data practices, including the selling of their personal information, while still being able to access and use the service.[144]

11.30 The Privacy Act already highlights this activity as having a higher privacy risk. Section 6D of the Privacy Act will capture any entities disclosing personal information about another individual to anyone else for a benefit, service or advantage even if their annual turnover is $3,000,000 or less. While trading in personal information will generally mean buying, selling or bartering personal information, this exception goes beyond the sale of personal information to capture any kind of benefit, service or advantage, whether financial or otherwise.[145] For example, a company exchanging their customer list in return for that of another entity would constitute a benefit, service or advantage for the purpose of this exception.[146]

11.31 We support this restricted practice, which will address this key risk in the digital economy and meet the expectations of the community. It will be important to appropriately frame this restricted practice to capture the full range of ways that personal information can be disclosed or otherwise made available to another party for a benefit (monetary or otherwise).

11.32 This restricted practice would be supported by our recommendation in Part 14 of this submission to introduce an absolute right to object to the sharing, disclosure or otherwise making available of an individual's personal information to third parties for a benefit (monetary or otherwise), and particularly where the personal information relates to a child.[147]

11.33 We suggest that the sale or other disclosure of personal information for a benefit should be a restricted practice, regardless of whether it is undertaken at a large scale. This would reflect the high degree of concern that individuals have around the sale of their personal information in any context.

---

[144] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p. 67 and 91

[145] See OAIC, *Trading in personal information*, OAIC website, n.d., accessed 11 November 2021; OAIC, *Small business*, OAIC website, n.d., accessed 11 November 2021

[146] OAIC, *Small business*, OAIC website, n.d., accessed 11 November 2021

[147] A similar right is provided under the privacy framework in California and would align with community expectations around the sharing and selling of their personal information. See *California Consumer Privacy Act of 2018*, 1.81.5 Cal Civil Code § 1798.135(a)(1).

The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale

11.34 The internet has become essential in the lives of individuals globally. It is where we go to work, to socialise, to buy new products, to consume news and to seek new opportunities, whether it is looking for a different job or a new home. A key component of the internet in the digital age has been the development of systems to personalise our experiences online and target the content we see on an individual basis. This system is driven by the collection and use of personal information that is used to predict people's preferences and behaviours.

11.35 In its Final Report on Online Targeting, the UK Centre for Digital Ethics and Innovation stated that:

> Online targeting systems' effectiveness lies in their ability to predict people's preferences and behaviours. They collect and analyse an unprecedented amount of personal data, tracking people as they spend time online and monitoring and learning from how they respond to content and how this compares to other people with similar characteristics. This enables them to predict how users will react when shown different items of content. Their predictions are used to decide what content to show people in order to optimise the system's desired outcome. People's responses to this content are then collected and fed back into the system in an iterative cycle.[148]

11.36 Online personalisation and targeting go beyond behavioural advertising and include providing individuals with more personalised content including social media posts, media articles or products. This can have benefits by serving individuals with more relevant content, whether this is ads for products they are interested in or information about their hobbies and interests. It can also be used to ensure that vulnerable people are not exposed to harmful content.

11.37 At the same time, these targeting systems have also made it possible to influence people's behaviours in more negative ways, exploit their vulnerabilities or amplify harmful conduct.[149] Of equal importance is what we are not shown online. Research from the Consumer Policy Research Centre and University of Melbourne observed that individuals had different experiences online, whether it is the products that we see or even the prices that we are charged, although the basis for these differences could not be determined.[150] These risks of discrimination online can be very serious, for example, where advertisements for different products or even jobs are shown or not shown to individuals on the basis of race, gender or religion.

11.38 We welcome the Discussion Paper's focus on the role that personal information can play in influencing our behaviour and decisions. The concept of influencing our behaviour or decisions, however, is very broad. We recommend that the focus be shifted to the collection, use or disclosure of personal information for the purposes of online personalisation and delivering targeted advertising. This will target the technology that allows APP entities to anticipate and

---

[148] Centre for Data Ethics and Innovation, *Online targeting: Final report and recommendations*, UK Government website, 4 February 2020, accessed 12 November 2021

[149] Centre for Data Ethics and Innovation, *Online targeting: Final report and recommendations*, UK Government website, 4 February 2020, accessed 12 November 2021

[150] DQUBE Solutions, Dr S Dreyfus, Associate Professor S Chang, Dr A Clausen and Professor J Paterson, *Drawing Back the Curtain: Consumer Choice in a Data Tracking World*, University of Melbourne, 2020, p. 27.

shape our preferences with increasing accuracy. This could include systems that select the content that individuals see on online platforms and the order that search results are presented where automated decisions draw on the profiling of individuals based on their personal information.[151] In our view, this restricted practice could apply regardless of whether these activities are undertaken at a large scale.

11.39 This restricted practice framework will require APP entities to deliberately assess the risks stemming from these activities and take steps to mitigate them, particularly any harms that may stem from online personalisation. The Review may wish to consider whether stronger limitations are appropriate where the benefits of online personalisation to APP entities are not proportionate to the potential risks to privacy and other rights.

11.40 We suggest below a prohibited practice around the profiling, online personalisation and behavioural advertising of children. Additional areas where the Review could consider further regulation relate to:

- The circumstances where sensitive information related to individuals can be used for online personalisation or targeted advertising. Sensitive information has additional protections under the Privacy Act because this data can be uniquely used as a basis for unjustified discrimination.[152] Introducing additional requirements around how sensitive information can be used in online personalisation systems would help address this risk. It would also meet community expectations around the use of sensitive information online, with 79% of Australians considering that an organisation inferring information about them (for example, sexual orientation, mental health, political views) based on what they do online to be misuse.[153]

- Requiring consent before an entity can combine personal information for the purposes of delivering targeted advertising. This requirement has recently been adopted for inclusion in Europe's proposed Digital Markets Act.[154]

11.41 Any additional requirements should be subject to appropriate exceptions to ensure that beneficial uses of online personalisation are not prevented.

The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects

11.42 We support this restricted practice in principle, which we consider in more detail in Part 17 of this submission.

---

[151] See for example Competition & Markets Authority *Online Search: Consumer and firm behaviour – A review of the existing literature*, UK Government website, 7 April 2017, accessed 12 November 2021, p. 3 which found that consumers focused mostly on results at the top of the search results & Department of Prime Minister and Cabinet, *Guidance Note: Harnessing the power of defaults*, DPM&C website, accessed 12 November 2021 p. 4 which found that the evidence overwhelmingly demonstrated that presenting an option as a default increases the chance it will be chosen.

[152] ALRC, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108),* ALRC, 12 August 2008, accessed 11 November 2021, 6.95

[153] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p. 36.

[154] See Compromise Amendment A to the Digital Markets Act, Article 6(aa)

Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual

11.43 We support this proposed restricted practice, which will provide flexibility for the restricted practice regime and allow it to capture other activities where entities should be required to assess and mitigate privacy risks to further protect individual privacy rights.

11.44 This restricted practice highlights the importance of our recommendations in Part 20 of this submission. This is because the Privacy Act will need to have an appropriate level of general organisational accountability obligations to help APP entities to assess whether their activities meet this restricted practice threshold.

Recommendation 43 – Adopt option 1 of proposal 11.1 to introduce a restricted practice regime that requires APP entities that engage in proscribed practices to take reasonable steps to identify privacy risks and implement measures to mitigate those risks.

Recommendation 44 – Introduce requirements for APP entities undertaking restricted practices to seek a periodic independent audit of the privacy risks identified in relation to the activity and measures implemented to mitigate those risks.

Recommendation 45 – Introduce the power for the Commissioner to create an APP code clarifying the steps required to mitigate risks for specific restricted practices, modelled on proposal 3.1 which allows the Commissioner to make an APP code on the direction of the Attorney-General.

Recommendation 46 – Adopt the following restricted practices:

- Direct marketing, including online targeted advertising
- The collection, use or disclosure of sensitive information on a large scale
- The collection, use or disclosure of children's personal information on a large scale
- The collection, use or disclosure of location data on a large scale
- The sale of personal information
- The collection, use or disclosure of personal information for the purposes of online personalisation and delivering targeted advertising
- The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects
- Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.

Prohibited practices

Should prohibited practices be legislated in the Act, or developed through Commissioner-issued guidelines interpreting what acts and practices do not satisfy the proposed fair and reasonable test, following appropriate public consultation?

11.45 The restricted practice regime outlined in the Discussion Paper and above provides a framework that will require APP entities to identify and appropriately mitigate privacy risks to ensure that their activities are fair and reasonable. In our regulatory experience, however, there will be some activities that will not be fair and reasonable because the privacy risks cannot be appropriately mitigated. For these activities, we think that a more proactive, outcome-based, ex-ante approach is required to address problematic activities before they cause harms in the community.

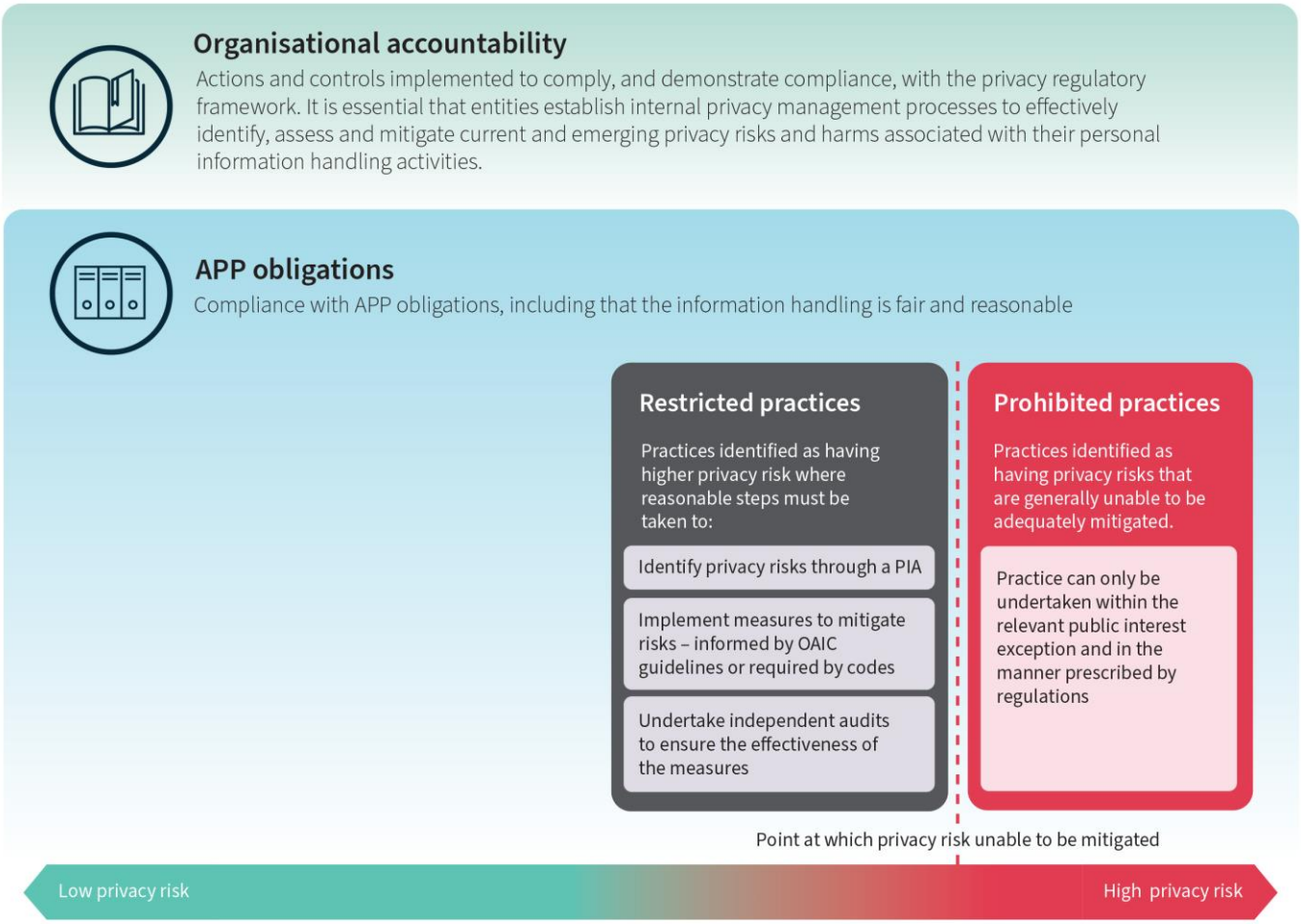
11.46 We recommend that clear prohibitions on certain practices are introduced into the Privacy Act. These prohibitions should be subject to limited and tailored exceptions in the public interest. The specific circumstances in which these activities are allowed, the entity or entities, or class of entity or entities that can undertake them, and any additional requirements or obligations that may apply could be prescribed by regulation.[155] The regulations could also set out clear rules on the way any personal information collected through these practices can be handled, for example, to ensure that it is not subsequently used or disclosed for any purposes not authorised by the regulation. As delegated legislation, regulations can be more easily amended to vary these exceptions where circumstances change, while providing the necessary regulatory certainty. A mechanism in the Privacy Act could also be introduced to allow Government to prescribe additional prohibitions in the regulations following appropriate consultation with the Commissioner and the community. This would provide additional flexibility to enable the framework to respond as needed into the future.

11.47 Additional requirements or prerequisites that must be satisfied when creating a regulation for a new prohibited practice could also be introduced into the Act, particularly requirements to consult with the Commissioner.[156]

11.48 In our view, this regime should be introduced in the legislative framework to ensure that these prohibitions and exceptions are clearly defined. While OAIC guidance is useful in helping entities to understand how the Commissioner will interpret the requirements under the Privacy Act, implementing this framework through guidance on the restricted practices and whether it is possible to mitigate the privacy risks of certain activities may not be effective. This is because this guidance is not enforceable and accordingly may not provide the regulated community with sufficient certainty about the legal requirements and activities that they cannot undertake.

[155] A similar approach is taken in APPs 9.1(b) and 9.3 and this may serve as a model.

[156] See for example the requirements under s 100 of the Privacy Act.



Acts or practices subject to the prohibited practices regime

11.49 There are several potential prohibited practices that we recommend are introduced into the Privacy Act, set out below. The views of submitters in response to this Discussion Paper will also be important in determining additional practices that should be included in this framework.

Profiling, online personalisation and behavioural advertising using children's personal information

11.50 In Part 13 of this submission, we set out the increased risks that apply to the handling of the personal information of children. Recent media reports have shown how the profiling of children online and the personalisation of their experiences in order to target them with behavioural advertising or other content can increase these risks and cause harms to children, particularly teenagers using online platforms.[157]

[157] G Wells, J Horwitz and D Seetharaman, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, The Wall Street Journal website, 14 September 2021, accessed on 8 December 2021; N Lomas, *Facebook accused of continuing to surveil teens for ad targeting*, Techcrunch website, 16 November 2021, accessed on 8 December 2021; A Dias, J McGregor and L Day, *The TikTok spiral*, ABC news website, 26 July 2021, accessed on 8 December 2021

11.51 The community is also concerned with these activities, with the OAIC's 2020 ACAPS results finding that parents were particularly uncomfortable with businesses targeting ads to children based on information they obtained by tracking a child online (65%) and businesses obtaining personal information about a child and selling it to third parties (69%).[158]

11.52 This is also an area of concern in other jurisdictions. Mostly recently, changes to the proposed Digital Markets Act in Europe have placed a prohibition on personal data of minors being processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.[159]

11.53 We recommend the introduction of a prohibited practice directed at profiling, online personalisation and behavioural advertising using children's personal information. This prohibited practice should be subject to appropriate exceptions to ensure that services that are beneficial for children and pose little privacy risk are not prohibited.

Inappropriate surveillance or monitoring of an individual through audio or video functionality of the individual's mobile phone or other personal devices

11.54 The Office of the Privacy Commissioner of Canada's no-go zone regime captures circumstances where an entity inappropriately surveils or monitors an individual through the audio or video functionality of an individual's mobile phone or other personal device.

11.55 In our view, the surveillance or monitoring of an individual through their own device will often be highly privacy-invasive and should be prohibited in Australia, except where there is a clear exception.[160]

11.56 We acknowledge that there may be some personal and home devices such as smart speakers may require entities to collect personal information for the purposes of developing and training the technology. The Review provides an opportunity to establish clear rules around the collection of personal information, including the recording of conversations for these purposes.[161]

The collection, use or disclosure of personal information that is unlawful

11.57 In Part 10 of this submission, we recommend that the lawfulness of information handling is a relevant factor when interpreting the fair and reasonable test. This would ensure that personal information handling that breaches Commonwealth, state or territory legislation, including anti-discrimination, surveillance or criminal laws, as well as common law requirements such as the duty of confidence, are prohibited under the Privacy Act.

---

[158] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p. 91

[159] Compromise Amendment A to the Digital Markets Act , Article 6(aa) and item 36(a).

[160] V Romo, *Spain's Top Soccer League Fined For Using App To Spy On Fans In Fight To Curb Piracy*, NPR website, 12 June 2019, accessed on 7 December 2021; Z Whittaker, *FTC bans spyware maker SpyFone, and orders it to notify hacked victims*, Techcrunch website, 2 September 2021, accessed on 7 December 2021;

[161] C Kirkham and J Dastin, *A look at Amazon's extreme data collection habits*, CRN website, 22 November 2021, accessed on 9 December 2021

11.58 An alternate approach is to define this as a specific prohibited practice. This approach has been taken in the no-go zone regime by the Office of the Privacy Commissioner of Canada.[162]

The use of automated biometric identification systems

11.59 Under the Privacy Act, biometric information is only sensitive information if it is 'collected for use in automated biometric verification and identification systems'. 'Biometric templates' are also sensitive information. In other circumstances, biometric information will only be personal information if it is about an identified or reasonably identifiable individual. This reflects the fact that biometric information may not carry significant privacy risks in isolation. For example, the drafting of the restricted practice relating to biometrics that is proposed in the Discussion Paper would likely capture companies that hold headshots or other photographs of individuals.

11.60 'Biometric information', 'biometric systems' and 'biometric templates' are not defined in the Privacy Act.[163] In a recent determination against Clearview AI Inc., the Commissioner set out the following definitions:

- 'Biometrics' encompass a variety of different technologies that use probabilistic matching to recognise a person based on their biometric characteristics. Biometric characteristics can be physiological features (for example, a person's fingerprint, iris, face or hand geometry), or behavioural attributes (such as a person's gait, signature, or keystroke pattern).[164] These characteristics cannot normally be changed and are persistent and unique to the individual.
- 'Biometric systems' scan, measure, analyse and recognise a particular and unique biometric (such as facial features), physical, biological and behavioural traits and characteristics to identify a person.
- A 'biometric template' is a digital or mathematical representation of an individual's biometric information that is created and stored when that information is 'enrolled' into a biometric system.[165] Machine learning algorithms then use the biometric template to match it with other biometric information, for verification, or to search and match against other templates within a database, for identification.[166]

---

[162] See Privacy Commissioner of Canada *Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)*, Office of the Privacy Commissioner of Canada, May 2018, accessed 25 October 2021.

[163] In Europe, the proposed Proposal for the Proposal for a Regulation laying down harmonised rules on artificial intelligence proposes a definition of 'biometric identification system' as an AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used.

[164] Office of the Victorian Information Commissioner, *Biometrics and Privacy*, OVIC website, July 2019, accessed 3 November 2021. See also, International Organization for Standardisation, (N/A) *Standard ISO/IEC 2382-37: 2017(en)*, ISO website, n.d., accessed 8 November 2021.

[165] International Organization for Standardisation, (N/A) *Standard ISO/IEC 2382-37: 2017(en)*, ISO website, n.d., accessed 8 November 2021

[166] *Commissioner-initiated investigation into Clearview AI Inc* (Privacy) 2021 AICmr 54, [122] - [123]; *Commissioner initiated investigation into 7- Eleven Stores Pty Ltd (Privacy)* [2021] AICmr 50, [47] - [49]

11.61 Genetic information is considered sensitive information under the Privacy Act and is therefore subject to increased protections, including additional consent requirements.[167] To the extent that genetic information is used in automated identification or verification systems, this will be captured in our proposed amendment to this restricted practice. Where genetic information is handled on a large scale, it will be addressed through the separate restricted practice above regarding sensitive information.

11.62 Biometric and genetic information carry unique privacy risks as they can often be used to uniquely identify individuals, are difficult or impossible to change and can be used to estimate or infer other sensitive or personal information such as age, sex, gender and ethnicity.

11.63 There are significant increased risks to privacy and other rights where this information is used for the purposes of automated identification systems. In some circumstances, automated biometric identification systems can collect large amounts of biometric information indiscriminately and without any direct involvement or even knowledge of individuals. This technology can also operate simply by an individual moving into a physical space, creating limitations on the effectiveness of traditional privacy self-management mechanisms such as notice and consent to provide individuals with control over their personal information.

11.64 The use of this technology also raises wider privacy concerns around the risks of surveillance and the use of this information to profile individuals, particularly given the potential for this technology to be inaccurate or biased.[168] There is also a high risk of this technology being abused if it is made more widely available, including facilitating stalking online.[169]

11.65 Given these significant privacy risks, we suggest that a prohibited practice focusing on the use of automated biometric identification systems is warranted.

Two-thirds (66%) of Australians are reluctant to provide biometric information to a business, organisation or government agency and a quarter (24%) are more reluctant to provide biometric information than any other type of information. This is higher than unwillingness to provide medical or health information (60% reluctant and 8% most reluctant) and location data (56% reluctant and 6% most reluctant).[170]

Domestic and global context

11.66 The appropriate regulation of this technology is an area of increasing focus in Australia and around the world.

11.67 The use of automated biometric identification and verification systems has been an important focus for the OAIC. The Commissioner has recently issued two significant determinations against Clearview AI Inc. and 7-Eleven Stores Pty Ltd, which concerned the use of facial

[167] This may be because it is health information about an individual or is genetic information about an individual that is not otherwise health information.

[168] See discussion of these issues in AHRC *Human Rights and Technology Final Report*, AHRC website, May 2021, p. 114-116

[169] See for example D Harwell, *This facial recognition website can turn anyone into a cop — or a stalker*, The Washington Post website, 14 May 2021, accessed 15 November 2021

[170] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p. 81.

recognition tools. The Clearview AI Inc. determination came after a joint investigation between the OAIC and the UK ICO. This built on a Resolution on Facial Recognition Technology presented by the OAIC and UK ICO at the Global Privacy Assembly's (GPA) Closed Session Conference in October 2020. The Commissioner has also engaged closely with Government in relation to the development of its identity-matching services.

11.68 In its recent Human Rights and Technology Final Report, the Australian Human Rights Commission (AHRC) recommended the introduction of specific legislation regulating the use of this technology that expressly protects human rights, applies to decisions that have a legal, or similarly significant effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement.[171]

11.69 The AHRC also recommended that, until this legislation is implemented, there should be a moratorium on Commonwealth, state and territory government uses of facial recognition and other biometric technology in decision making that has a legal, or similarly significant effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement.[172]

11.70 A similar law was recently proposed by the EU Commission in the Proposal for a Regulation laying down harmonised rules on artificial intelligence (Proposed Harmonised rules on AI),[173] which places a broad restriction on real-time biometric identification systems in publicly accessible spaces for law enforcement unless it is strictly necessary for the following purposes:

- the targeted search for specific potential victims of crime, including missing children
- the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack
- the detection, localisation, identification or prosecution of a perpetrator or suspect of specifically defined criminal offences which are punishable by a custodial sentence or a detention order for a maximum period of at least three years.[174]

11.71 In their response to the Proposed Harmonised rules on AI, the joint opinion of the European Data Protection Supervisor and European Data Protection Board (the EDPS and EDPB Joint Opinion) called for a general ban on the use of AI for the automated recognition of human features in publicly accessible spaces, including identifying faces, gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioural signals – in any context.[175]

---

[171] See for example AHRC, *Human Rights and Technology Final Report*, AHRC website, May 2021, Recommendation 19.

[172] See for example AHRC, *Human Rights and Technology Final Report*, AHRC website, May 2021, Recommendation 19 and 20.

[173] Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final. Additionally, in January 2021, the Council of Europe issued guidelines for legislators and decision-makers which highlighted the need for legislators and decision-makers to lay down specific rules for biometric processing by facial recognition technologies for law enforcement purposes and for public authorities (see pages 6-7).

[174] See Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts COM/2021/206 final, Article 5

[175] See European Data Protection Board and European Data Protection Supervisor, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*, EDPS website, 18 June 2021, accessed 11 November 2021

11.72 The UK ICO has also focused on the use of facial recognition technology. In 2019, the UK ICO issued a report on its investigation into how the police use facial recognition technology in public places.[176] This was followed by its opinion on the use of live facial recognition technology in public places more generally.[177] This set out key data protection requirements for the use of this technology, including that it must be lawful, fair, necessary and proportionate.

Co-sponsored by the OAIC and the UK ICO, the 42nd General Privacy Assembly reiterated the importance of:

1. The principles of data protection and privacy by design in facial recognition technology development and use

2. Necessity and proportionality principles, ensuring that facial recognition technology cannot be used where the purpose can reasonably be achieved by less intrusive means

3. Transparency and accountability about the use of personal data and its governance in facial recognition applications, and applicable rights for individuals, including in provision of the technology to and their use by law enforcement agencies

4. Requirements of fairness in processing personal data

5. An ethical approach to the use of biometric data

6. Legal frameworks that are fit for purpose in regulating evolving technologies such as facial recognition technology.[178]

Scope of a prohibited practice on the use of biometric information for the purposes of automated biometric identification or verification

11.73 The introduction of a prohibited practices framework provides an opportunity to closely consider the parameters around the use of this type of automated biometric identification or verification systems by APP entities under the Privacy Act.

11.74 It is essential that this regulation is appropriately adapted and tailored. An important element of these rules will be to consider the context in which this technology is deployed, and particularly where its use is for a purpose that is in the public interest. For example, there may be public policy considerations that justify the use of live facial recognition technology by government, including law enforcement, which will not be present for commercial uses of this technology.

11.75 The law should also focus on the types of automated biometric identification or verification systems that pose significant risks. We consider that the use of automated biometric

[176] UK ICO, *ICO investigation into how the police use facial recognition technology in public places*, ICO website, 31 October 2019, accessed 11 November 2021

[177] UK ICO, *Information Commissioner's Opinion: The use of live facial recognition technology in public places*, ICO website, 18 June 2021, accessed 11 November 2021

[178] General Privacy Assembly, *Adopted Resolution on Facial Recognition Technology*, GPA website, October 2020, accessed 11 November 2021

identification systems for one-to-many matching may often be quite privacy invasive.[179] On the other hand, a different approach may be appropriate for systems to undertake one-to-one matching that compares an individual's biometric information to existing information that an APP entity holds about that individual. This is generally less privacy-invasive, and is used to verify individuals for authentication purposes, such as to access a smart device.[180]

The OAIC's 2020 ACAPS results found that when it came to Government's use of biometrics, over half of those surveyed are comfortable with law enforcement using facial recognition and video surveillance to identify suspects (58% comfortable, 23% uncomfortable) or a government body using surveillance for public safety (56% comfortable, 22% uncomfortable).

Similarly, half of Australians are comfortable providing their biometric information to verify their identity to access government services (53% are comfortable, 25% uncomfortable), to do their day-to-day banking (49% are comfortable, 29% are uncomfortable) or to get on a flight (49% are comfortable, 24% are uncomfortable).

The majority of Australians are uncomfortable with the collection of their biometric information to shop in a retail store (52% uncomfortable, 25% comfortable), to get into a licensed pub, club, bar/hotel (43% uncomfortable, 31% comfortable) or to verify their identity to access services provided by a business or private organisation (40% uncomfortable, 33% comfortable).[181]

11.76 The approach to regulating this technology should also differ based on the context in which it is used. For example, in our view, the use of this one-to-many technology by private organisations for commercial purposes will rarely be reasonably necessary or proportionate to the significant risks that automated biometric identification systems pose to privacy and other human rights. Given these significant risks, we consider that there will be few situations where the public interest will justify the use of these systems by private organisations.

11.77 On the other hand, while the use of automated biometric identification or verification systems by government can also pose significant privacy risks, there may be important public policy considerations that counterbalance potential intrusions with privacy, particularly in a law enforcement or public safety context. We recognise that significant work has been undertaken by Government in relation to this technology including the National Facial Biometric Matching Capability and the National Drivers Licence Facial Recognition Solution.

11.78 We recommend that a prohibition on the commercial use of automated biometric systems used for one-to-many matching is introduced into the Privacy Act, subject to limited, public interest exceptions.

---

[179] Office of the Victorian Information Commissioner, *Submission in response to the Human Rights and Technology discussion paper*, AHRC website, 10 March 2020, accessed 8 November 2021, p. 6

[180] One-to-many matching involves comparing an unknown person's biometric information against a database to help identify an individual. This could be used to identify an individual in a crowd in real time. See Office of the Victorian Information Commissioner, *Biometrics and Privacy*, OVIC website, July 2019, accessed 8 November 2021

[181] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p. 79.

Scraping personal information from online platforms

11.79 Advancing online protections is a strategic priority for the OAIC.[182] Addressing the significant privacy issues around data scraping has been one way in which we have sought to achieve this aim. The OAIC and the UK ICO opened a joint investigation into the activities of Clearview AI Inc. and the Commissioner recently issued a determination finding that Clearview AI Inc. had interfered with the privacy of individuals, including because of its indiscriminate scraping of facial images from the internet for use in its facial recognition tools.[183]

11.80 The scraping of personal information poses significant privacy risks. It may be indiscriminate and impact a large amount of people who may not be given any notice that the activity has taken place or consented to the collection where required, such as the scraping of sensitive information. Additionally, while personal information scraped from websites will sometimes be publicly available, this information will often be shared or used for purposes that were not in the reasonable expectations of the individuals when they uploaded the information onto the internet. Recent media reports have identified alleged scraping incidents that potentially affected thousands of individuals.[184]

11.81 This can result in a range of privacy harms. Scraped information can be used for identity theft, posted online and be used for targeted social engineering or phishing attacks, the creation of facial recognition databases and unwanted direct marketing or spam. As individuals may not be aware that this scraping has taken place, they will not be well placed to take steps to protect themselves from these harms. Further, the Commissioner's determination in relation to Clearview AI Inc. stated:

> 176. More broadly, the indiscriminate scraping of facial images may adversely impact all Australians who perceive themselves to be under the respondent's surveillance, by impacting their personal freedoms.[185]

11.82 These privacy risks are significant, and we consider that a legislative approach is needed. The Review provides an opportunity to consider appropriate rules around personal information scraping from online platforms. As part of the restricted and prohibited practices regime, we recommend the introduction of rules including:

- A prohibition for the scraping of personal information from online platforms and other appropriate websites. The regulations could set out exceptions to this prohibition where there is an appropriate public interest, for example, where this is allowed under specific legislation, for journalism or research purposes or to allow search engines to index content online.
- A requirement that online platforms and other appropriate websites must proactively take reasonable steps to prevent the scraping of personal information. This recognises

---

[182] See our OAIC, *Corporate Plan 2021/2022*, OAIC website, August 2021, accessed 15 November 2021. This builds on our regulatory priorities in 2020/2021 which included a focus on online platforms and social media.

[183] *Commissioner-initiated investigation into Clearview AI Inc* (Privacy) 2021 AICmr 54, [46]

[184] C Duffy, *500 million LinkedIn users' data is for sale on a hackers site*, CNN Business website, 8 April 2021, accessed 17 November 2021

[185] *Commissioner-initiated investigation into Clearview AI Inc* (Privacy) 2021 AICmr 54, [176]

that it may not always be possible to identify the entity undertaking this type of personal information scraping, and that online platforms may have the ability to limit the capacity of the personal information on their platforms from being scraped.

Any other practice prescribed by regulation

11.83 We recommend introducing a mechanism that will allow Government to prescribe additional prohibitions in regulation following appropriate consultation with the Commissioner and the community. This would provide the flexibility to enable the framework to respond as needed into the future.

Recommendation 47 – Introduce prohibited practices into the Privacy Act, subject to appropriate public interest exceptions including in relation to:

- Profiling, online personalisation and behavioural advertising using children's personal information
- Inappropriate surveillance or monitoring of an individual through audio or video functionality of the individual's mobile phone or other personal devices
- The collection, use or disclosure of personal information that is unlawful
- The commercial use of automated biometric identification systems
- Personal information scraping from online platforms

Recommendation 48 – Introduce prohibited practices in relation to the scaping of personal information through a requirement that online platforms and other appropriate websites must proactively take reasonable steps to prevent it.

Recommendation 49 – Introduce the ability to prescribe additional prohibitions by regulation.

Part 12: Pro-privacy default settings

12.1 Introduce pro-privacy defaults on a sectoral or other specified basis.

Option 1 – Pro-privacy settings enabled by default

Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.

Option 2 – Require easily accessible privacy settings

Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.

Should pro-privacy default settings be enabled by default, or should requirements be limited to ensuring that privacy settings are clear and easy to access?

If pro-privacy default settings are enabled by default, which types of personal information handling practices should be disabled by default?

12.1 Privacy settings are a practical way for entities to offer individuals choice and control over how their personal information will be handled.[186] Default settings can be described as the pre-set function of a setting that applies unless changed by the user.[187]

12.2 The issue with default settings is that they may actively discourage users from making privacy protective choices. Default settings that are not privacy protective effectively encourage individuals to agree to certain personal information handling practices that may go beyond those that are necessary for the provision of a product or service.

12.3 Research indicates that some entities deliberately nudge individuals to choose less privacy-friendly options, for example, by requiring significantly more clicks to change privacy invasive default settings.[188] These are known as 'dark patterns.'[189]

12.4 According to research by the Behavioural Economics Team of the Department of Prime Minister and Cabinet, there is 'overwhelming' evidence that 'presenting one option as a default…

[186] UK ICO, '7. Default settings', *Age appropriate design: a code of practice for online services*, ico.org.uk, n.d., accessed 9 December 2021.

[187] ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, 26 July 2019, accessed 22 November 2021, p 429.

[188] Oyvind H. Kaldestad, *Report: Deceived by design*, Forbruker Rådet website, 27 June 2018, accessed 9 December 2021.

[189] Forbruker Rådet, *Every Step You Take: How deceptive design lets Google track users 24/7'*, Forbruker Rådet website, 27 November 2018, accessed 9 December 2021, p 12.

increases the chance it will be chosen'.[190] In other words, decision-makers are predisposed to accept the default when confronted by a choice with a default option.[191]

12.5 Default settings that are not privacy protective are also out of step with consumer expectations. The Deloitte 2020 Privacy Index found that 93% of individuals expect a service to provide them with an upfront option to opt-in to non-essential data handling practices, rather than requiring them to opt-out of these practices.[192] More broadly, the OAIC's 2020 ACAPS results found that 81% of Australians considered an organisation asking them for personal information that does not seem relevant to the purpose of the transaction to be a misuse.[193]

12.6 We consider that default settings that aim for data maximisation by encouraging individuals to make privacy choices against their own interests run counter to the policy intentions of the Privacy Act and increase the risk of harm to individuals.[194]

12.7 We support option 1 of proposal 12.1 to require pro-privacy settings to be enabled by default. We recommend that privacy settings should be set to privacy protective by default, except for the collection, use or disclosure of personal information that is reasonably necessary to provide the particular product or service.

12.8 This means that privacy settings will need to be set to 'off' by default to require individuals to expressly opt-in to collections, uses or disclosures of personal information that are not reasonably necessary to provide the particular product or service.

12.9 For example, a weather forecast app may use an individual's location data to provide local weather forecasts. However, if the app sought to use the individual's location data to serve localised targeted ads, this would likely be an additional use of the location data that is not reasonably necessary to provide the service. In these circumstances, use of location data for these secondary purposes that are not part of the core service should be set to 'off' by default.

12.10 What is 'reasonable' to enable the provision of the particular product or service would be a question of fact in each case. Consistent with existing OAIC guidance, what is 'reasonable' in the circumstances is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. It is the responsibility of the APP entity to be able to justify that its conduct was reasonable.[195]

12.11 The Commissioner could issue further guidance on the types of personal information handling practices that may not be reasonably necessary to provide a particular product or service and the matters entities should consider when implementing privacy protective default settings.

---

[190] Department of Prime Minister and Cabinet (PM&C), *Harnessing the Power of Defaults – Governance Note*, PM&C website, n.d., accessed 9 December 2021, p 4.

[191] ACCC, *Digital Platforms Inquiry – Final Report*, ACCC website, 26 July 2019, accessed 22 November 2021, p 469.

[192] Deloitte, *Opting-in to meaningful consent – Deloitte Australian Privacy Index 2020*, Deloitte website, 2020, accessed 9 December 2021, p 14.

[193] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 31.

[194] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, 11 December 2020, accessed 8 November 2021, p 78.

[195] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 9 December 2021.

The measures entities will need to implement will depend on their individual circumstances and the particular risks posed to individuals by their personal information handling activities.

12.12 By way of example, the UK's Age Appropriate Design Code requires settings to be 'high privacy' by default (unless the service can demonstrate a compelling reason for a different default setting, taking account the best interests of the child). The Code states that 'high privacy' default settings:

> ...means that children's personal data is only visible or accessible to other users of the service if the child amends their settings to allow this.
>
> This also means that unless the setting is changed, your own use of the children's personal data is limited to use that is essential to the provision of the service. Any optional uses of personal data, including any uses to personalise the service have to be individually selected and activated by the child.
>
> Similarly any settings which allow third parties to use personal data have to be activated by the child...
>
> You should also consider whether to put any further measures in place when a child attempts to change a setting. This depends on your assessment of the risks inherent in the processing covered by each setting and could include further age assurance measures.[196]

12.13 The enhanced accountability measures proposed in Part 20 of this submission will also help APP entities to assess, identify and select the circumstances in which they will need to implement privacy protective default settings.

12.14 Requiring pro-privacy settings to be enabled by default will 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.

12.15 It would also ensure a higher level of user engagement before APP entities can collect and use personal data for practices that are not reasonably necessary to provide the product or service.

12.16 While we are supportive of measures to provide individuals with an obvious and clear way to set all privacy controls to the most restrictive (option 2), this alone is not sufficient to protect privacy. Even if privacy settings are simplified, the opt out option would still require consumers to be proactive about protecting their privacy. This option still places a significant burden on individuals to understand complicated practices and take the time and effort to opt out.

12.17 For the reasons outlined above, we consider that the preferred approach is to require pro-privacy settings to be enabled by default – so that individuals must take steps to opt-in to certain information handling practices (option 1).

[196] UK ICO, '7. Default settings', *Age appropriate design: a code of practice for online services*, ico.org.uk, n.d., accessed 9 December 2021.

Recommendation 50 – Adopt option 1 of proposal 12.1 to amend the Privacy Act to require privacy settings to be set to privacy protective by default except for the collection, use or disclosure of personal information that is reasonably necessary to provide the particular product or service.

Part 13: Children and vulnerable individuals

13.1 Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The Review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so. The Review is also seeking feedback on the circumstances in which parent or guardian consent must be obtained:

Option 1 – Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16.

Option 2 – In situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.

The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction or erasure requests.

13.2 Require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child*.

Are there other contexts aside from children's use of social media services that pose privacy risks to children, which would warrant similar privacy protections to those proposed by the OP code?

Should consent of a parent or guardian be required for *all* collections of a child's personal information, or only for the existing situations where consent is required under the APPs?

Should the proposed assumed age of capacity of 16 years in the OP Bill apply to all APP entities?

Should APP entities also be permitted to assess capacity to consent on an individualised basis where appropriate, such as in the healthcare sector?

Should the proposed assumed age of capacity determine when children should be able to exercise privacy requests independently of their parents, including access, correction, objection or erasure requests?

Risks to privacy and potential harms for children

13.1 Many of the privacy risks and harms online have emerged due to the dramatic increase in the amount of data and personal information collected about individuals, and the subsequent use and disclosure of this information in ways users may not understand or expect.

13.2 A lack of transparency by online platforms around complex data practices presents significant challenges for individuals in making informed decisions about how their personal information is handled online.

13.3 Children frequently spend time online to connect with friends, learn and be entertained. Online environments give young people the chance to express themselves and build their identities. However, children require support online, just as they do offline. Online services are designed to appeal to young people, but may not always be safe, appropriate and privacy protective.[197]

13.4 In its DPI Final Report, the ACCC recognised that the risks associated with data collection and use could be particularly acute for children. The report also recognised that younger children, as a group of consumers, may lack the requisite technical, critical and social skills to engage with the internet in a safe and beneficial manner.[198]

13.5 The risks and harms that children face online arise primarily from the monetisation of their personal information, from the social impacts of sharing personal information on their reputation and life opportunities, and from online safety risks.[199]

13.6 The commercial practices that underpin websites are largely based on the monetisation of personal information via its use or on-sale for marketing. As noted in the Discussion Paper, entities may regularly share children's data for advertising purposes, or engage in harmful tracking, profiling of, or targeted marketing to children.[200]

13.7 Targeted marketing is designed to encourage the purchase of products and may pose financial risks if a child increases their spending by making impulse purchases or spends money on products that they cannot afford and would not otherwise have purchased.[201]

13.8 If the products advertised are unhealthy this may contribute to problems such as obesity, early alcohol consumption or smoking cigarettes or e-cigarettes. Further concerns about the influence of targeted marketing include modified psychological or mental health changes such as negative body image, sexualisation of children, entrenchment of gender stereotypes, stigmatisation of poverty and reduction in parents' authority and influence.[202]

13.9 Reputational harms may also result from a loss of control over personal information in the online context. Specifically, damaging information which may continue to exist online and be used for decision-making long after it is collected or has lost its currency.

13.10 The Australian Council on Children and the Media succinctly described the privacy risks and harms that children may face online as follows:

> In the short-term apps can gather children's data and use it to identify and locate them; can build children's profiles by tracking their likes and dislikes so as to keep them attached and sell them things; and can expose them to personal harm through cyberbullying and social grooming.

---

[197] OAIC, *Privacy tips for parents and carers*, OAIC website, n.d., accessed 17 November 2021.

[198] ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, 2019, accessed 17 November 2021, pp 447-448.

[199] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 29.

[200] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 17 November 2021, p 100.

[201] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 32.

[202] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 32.

In the long term, data collected over childhood and adolescence can be used against them in adulthood, for example when seeking placement in a desired course of study or selection for a "dream" job.[203]

Defining a 'child'

13.11 The Online Privacy Bill proposes to, amongst other measures, amend the Privacy Act to define a 'child' as an individual 'who has not reached 18 years of age.'[204] We note this would bring the Privacy Act into line with the *Online Safety Act 2021* (Online Safety Act) and the UK's Age Appropriate Design Code.

Determining when a child has capacity to consent

13.12 The Discussion Paper proposes to amend the Privacy Act to require consent to be provided by a parent or guardian where a child is under the age of 16 (proposal 13.1). Feedback is also sought on two options for the circumstances in which parent or guardian consent must be obtained (discussed further below).

13.13 The Privacy Act does not specify an age after which an individual can make their own privacy decisions. The OAIC's guidance provides that an entity will need to determine on a case-by-case basis whether an individual under the age of 18 has the capacity to consent.[205]

13.14 As a starting point, there is no consensus or consistency regarding the most appropriate age of consent in the privacy context or other legal frameworks. For example, in the health context, a child may take responsibility of their My Health Record (MHR) once they turn 14 years of age.

13.15 Approaches to the age of consent in overseas jurisdictions range from 13 to 18 years of age. It is relevant to note the challenges other jurisdictions have faced in attempting to prescribe a 'bright-line' age limit. For example, Article 8 of the GDPR currently requires parental consent to be obtained before processing the personal data of a child below the age of 16 years. However, this proposal was originally met with opposition from both industry and child rights experts. Industry argued that raising the age would increase the compliance burden on entities and would lead to the withdrawal of services from children. Child rights experts considered that the age limit was unrealistically high and would require children who have the capacity to make their own privacy decisions to seek their parents' consent.[206]

13.16 The EU addressed these various concerns by maintaining a default threshold age of 16 under GDPR, while allowing individual EU member states to derogate from this through domestic legislation and lower the age limit provided it was not lower than 13. This has resulted in a

---

[203] Australian Council on Children and the Media (ACCM), *Australian privacy law: is it protecting our children when online?*, ACCM website, n.d., accessed 17 November 2021.

[204] At the time of writing this submission, the Attorney-General's Department had published an exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 for public consultation. The exposure draft of the Bill is available on the Attorney-General's Department website at https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/.

[205] OAIC, *Australian Privacy Principles Guidelines*, OAIC, July 2019, accessed 22 November 2021, p 13.

[206] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 84.

fragmented approach to the privacy age of consent, which contradict the objective of the GDPR to create uniform data protection standards throughout the EU.[207]

13.17 Due to limitations associated with capacity outlined above, children do require support to make their own privacy decisions. Parental or guardian consent will still be a necessary and proportionate response to mitigate the risk of potential privacy-related harm that children may face in certain circumstances.

13.18 However, children also possess important participative rights, and it is important to adopt an approach that protects children's privacy rights against undue interference, yet also respects their increasing ability to make their own privacy choices independent of their parents.[208]

13.19 Adopting a 'bright-line' or 'one-size-fits-all' approach to the age of consent in the privacy context does not recognise that children's ability to make informed choices is developing throughout the teenage years. Children's cognitive, affective and decision-making skills develop at differing rates and reach the required level of maturity at different ages.[209] Consequently, it is important to acknowledge children's increasing ability to make their own privacy choices as they age.

13.20 The parental consent model is also based on the assumption that parents and guardians are better able to assess the consequences of providing consent than children. However, the parental consent model raises the same problems as the notice and consent model more generally. Adults may not be able to understand the terms and conditions they are agreeing to, and this issue applies equally to parents providing consent on behalf of their children.

13.21 Option 1 of proposal 13.1 would require parent or guardian consent for *any* collection, use or disclosure of personal information of a child under 16. Option 2 would require parent or guardian consent in situations where the Privacy Act currently requires consent (such as the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information).

13.22 APP entities are currently permitted to collect, use or disclose personal information without consent. 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.

13.23 In this way, the Privacy Act recognises that consent is not necessary or appropriate in all circumstances, which reflects the fact that many instances of personal information handling in the economy are reasonably expected by individuals.

---

[207] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 84.

[208] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 8.

[209] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 86.

13.24 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 environments. It may also become a 'tick-box' exercise which will detract the value of consent in higher-risk situations where it is of greater value.

13.25 Consequently, requiring parent or guardian consent in all circumstances relating to the handling of personal information of a child under 16 may be a disproportionate response to the particular harms that are seeking to be addressed. Further, for the reasons outlined above, we do not support option 2 to obtain parent or guardian consent in situations where the Act currently requires consent.

13.26 We consider that it is preferable to maintain the existing approach, which enables entities to assess whether an individual under the age of 18 has capacity to consent on a case-by-case or sector basis. Prescribing an economy-wide age of privacy consent may be challenging to align with the risk-based approach, which is fundamental to the APPs.A

13.27 As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. If they lack maturity, it may be appropriate for a parent or guardian to consent on their behalf.[210]

13.28 If it is not practical or reasonable for an entity to assess the capacity of individuals under the age of 18 on a case-by-case basis, the entity may presume that an individual aged 15 or over has capacity to consent, unless there is something to suggest otherwise. An individual aged under 15 is presumed not to have capacity to consent.[211]

13.29 The APP guidelines steer a middle ground between individualised assessment and practicability. This enables a flexible approach to assessing capacity that is applicable across various sectors and entities. This approach also supports children's developing ability to make informed privacy choices and is preferable from a children's rights perspective because it enhances their participation in matters affecting them.

13.30 However, we appreciate that entities need clarity around the age at which capacity to consent can be presumed. We will carefully consider submissions from other stakeholders to the Discussion Paper on this issue to determine whether 15 years remains appropriate or whether adjustments to our guidance are necessary.

13.31 Given the complexity of the issues involved and the range of interests affected, we consider that potentially legislating an age of consent could be done through the development of industry codes after extensive further consultation with experts, parents, children and the relevant industries. This approach would enable a privacy age of consent to be prescribed by industry or sector, taking into account the particular privacy risks and harms that may arise.

13.32 For example, under the proposed OP code, social media services will be required to comply with specific protections in relation to children, including a requirement to obtain parental or guardian consent before collecting, using or disclosing the personal information of a child

[210] OAIC, *Australian Privacy Principles Guidelines*, OAIC, July 2019, accessed 22 November 2021, p 13.

[211] OAIC, *Australian Privacy Principles Guidelines*, OAIC, July 2019, accessed 22 November 2021, p 13.

under 16. This reflects the particular risks social media services pose to children and also the challenges associated with establishing capacity on a case-by-case basis in the online sector.

Simplified privacy notices

13.33 Children are particularly vulnerable online given limitations in their basic and digital literacy, their cognitive abilities and their capacity for mature decision-making.[212] This vulnerability is particularly relevant in the privacy context due to the key role of notice and consent as the basis for current privacy protection.

13.34 To that end, we support proposal 13.2 to require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child*.

13.35 The Discussion Paper notes that visual or graphical communication could be used by an entity to ensure that its privacy notice is intelligible to children. We support measures that aim for more than mere disclosure of material facts. Privacy transparency should aim to educate, empower and enable privacy self-management accounting for a child's developing needs and capabilities.[213]

13.36 We also note that the Online Privacy Bill provides that the proposed OP code will deal with notification matters under APP 5, including by requiring all notices to be clear and understandable and how this applies in relation to children and other groups of people not capable of making their own privacy decisions.

Recommendation 51 – Adopt proposal 13.2 to require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child*.

Other protections for children

13.37 Children will also benefit from the enhanced privacy protections recommended throughout this submission.

13.38 As noted in Part 20 of this submission, reforms to privacy self-management mechanisms, such as notice and consent, should be complemented by appropriate organisational accountability obligations.

13.39 Further, we have recommended a broader change to the Privacy Act to require a new standard or benchmark of fair and reasonable handling of personal information when it is collected, used and disclosed. The proposed fair and reasonable test in Chapter 10 of the Discussion Paper

[212] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 8.

[213] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, p 102.

would permit the Commissioner to determine whether the collection, use or disclosure of a child's personal information was inappropriate in the circumstances.

13.40 The proposed fair and reasonable requirement would raise the standard of data handling in Australia so that individuals, including children, can have greater confidence that they will be treated fairly, no matter what they choose. Ideally, this would prevent notice and consent being used to legitimise handling of personal information in a manner that, objectively, is unfair or unreasonable.

13.41 We support the proposal that the fair and reasonable test would include a factor regarding 'whether a collection, use or disclosure of the personal information is in the best interests of the child.'

13.42 We also support proposal 11.1 to require APP entities to identify and mitigate privacy risks where they engage in a restricted practice. One of the restricted practices identified in the Discussion Paper that would trigger these requirements includes 'the collection, use or disclosure of children's personal information on a large scale.'

13.43 We have also recommended enhanced organisational accountability requirements in Part 20 of this submission, including that APP 1 is amended to expressly require APP entities to implement and be able to demonstrate the steps taken to implement a privacy by design approach.

13.44 We consider that an express requirement in APP 1 to implement a privacy by design approach, combined with the proposed requirement to handle personal information fairly and reasonably, will facilitate positive privacy outcomes by requiring APP entities to consider how their activities will impact individuals, including children, and to identify less privacy intrusive options for new projects, activities or initiatives.

13.45 Relatedly, there are also several online safety initiatives that are similarly designed to protect children online.

13.46 The Online Safety Act requires the eSafety Commissioner to develop industry codes that will cover similar entities to the proposed OP code, including social media services, and may deal with various matters including 'procedures directed towards the achievement of the objective of ensuring that online accounts are not provided to children without the consent of a parent or responsible adult.'[214]

13.47 Similarly, the Department of Infrastructure, Transport, Regional Development and Communications has recently consulted on a draft Online Safety (Basic Online Safety Expectations) Determination 2021, which sets out expectations around implementing age assurance mechanisms to prevent access to restricted content by children.[215]

---

[214] *Online Safety Act 2021* (Cth) s 138(3)(f).

[215] The public consultation on the draft Online Safety (Basic Online Safety Expectations) Determination 2021 opened on 8 August 2021 and closed on 12 November 2021. The draft Determination and other consultation information is available on the Department of Infrastructure, Transport, Regional Development and Communications website at https://www.infrastructure.gov.au/have-your-say/draft-online-safety-basic-online-safety-expectations-determination-2021-consultation.

13.48 Privacy and online safety have distinct but complementary roles to play to keep Australians safe online. They are both essential components in the ring of defence that is being built to address the risks faced by Australians in the online environment. Accordingly, it is important to ensure that enhanced privacy protections for children are interoperable with developments both domestically and internationally in the regulation of online safety.

Vulnerable individuals

13.49 The Discussion Paper considers whether additional or different privacy protections are required for individuals with vulnerabilities, including adults experiencing temporary or permanent incapacity for reasons such as disability, illness and injury.

13.50 Vulnerability can be defined as a heightened susceptibility to harm. Both individual characteristics and situational factors can influence an individual's susceptibility to harm. In this way, vulnerability can be dynamic and context specific, rather than a fixed trait associated with a particular group in all circumstances.[216]

13.51 Considering the above, vulnerability may be difficult to recognise and address, and may raise privacy issues of its own if entities were to request and collect additional personal information to assess vulnerability, beyond what is necessary to provide a service.

13.52 We acknowledge that individuals may be vulnerable in relation to their capacity to consent to certain privacy decisions. The OAIC's APP guidelines state that issues that could affect an individual's capacity to consent include:

- age
- physical or mental disability
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia, or
- limited understanding of English.[217]

13.53 As a starting point, an APP entity should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity to consent. If an individual does not have capacity to consent, even with support or the provision of additional resources such as an interpreter or alternative communication methods, and consent is required, an entity should consider who can act on the individual's behalf.[218]

13.54 The Privacy Act does not prevent an individual from nominating a third party to support them or to act on their behalf. Entities may implement their own procedures to enable an individual

---

[216] N Witzleb, M Paterson, J Wilson-Otto, G Tolkin-Rosen and M Marks, *Privacy risks and harms for children and other vulnerable groups in the online environment*, report to OAIC, Monash University and elevenM Consulting, 2020, pp 16, 139, 148.

[217] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 22 November 2021.

[218] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 22 November 2021.

to nominate a third-party to act on their behalf. For example, the OAIC provides a mechanism for individuals to nominate someone to represent them in a privacy complaint by completing a 'Privacy Complaint Authorised Representative Form' on our website.[219]

13.55 The Privacy Act also permits third parties with legal authority to act on behalf of individuals. Where a third party is legally appointed as a substitute decision maker, an APP entity should generally recognise this arrangement.

13.56 As highlighted in the Discussion Paper, the Australian Law Reform Commission (ALRC) considered it was unnecessary to explicitly recognise formal arrangements as the relevant laws that give effect to legal appointments determine the extent to which third parties can substitute decisions under the Act. Providing an additional hurdle to recognition would add unnecessary complexity to the existing patchwork of state and territory laws.[220]

13.57 Outside of the formal arrangements outlined above, the Privacy Act recognises relatives, friends and next-of-kin as 'responsible persons' in very limited circumstances. The onus is on the entity to assess an individual's capacity and ensure the third party meets the definition of responsible person.

13.58 In light of the above, we support the view expressed in the Discussion Paper that amendments to the Privacy Act to explicitly recognise third-party representative arrangements are unnecessary given the Act does not prevent third parties acting with consent or with legal authority as substituted decision-makers.

13.59 Relatedly, the Online Privacy Bill provides that the proposed OP code must include specific requirements and additional protections for individuals physically or legally incapable of giving consent.

[219] See https://www.oaic.gov.au/privacy/privacy-complaints/lodge-a-privacy-complaint-with-us

[220] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 109.

Part 14: Right to object and portability

The right to object

14.1 An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

14.1 We support proposal 14.1 to introduce a right to object to the collection, use or disclosure of personal information. This will require an entity, on receiving notice of an objection, to take reasonable steps to stop collecting, using or disclosing the individual's personal information and inform them of the consequences.

14.2 Although the rights are similar, we consider that the right to object is broader in application than a right to withdraw consent. The right to object allows individuals to object to personal information collection, use or disclosure in specific circumstances, subject to appropriate exceptions.

14.3 On the other hand, the circumstances in which an individual will be able to withdraw their consent will be limited to the situations where consent has been required under the APPs. Consent is currently only required for a limited range of collections, uses and disclosures of personal information. As set out in more detail in Part 9, we support formalising this existing right to withdraw consent in the Privacy Act.

The need for a right to object

14.4 The existing individual privacy rights under the Privacy Act help individuals to exercise control over their personal information. This is an important aspect of privacy self-management that helps to create trust and confidence in the personal information handling practices of APP entities. However, under the current framework, individuals have little control over how their personal information is used or disclosed after it is collected.

14.5 A right to object will provide individuals with greater ongoing control over their personal information following collection and enable them to make choices as risks and the privacy environment change over time. Proposal 14.1 gives effect to the community expectation that individuals should have a right to object to certain information handling practices.[221] Introducing this right would also help to bring Australian privacy law in line with the regulatory frameworks of other jurisdictions, including the UK and the EU.

[221] The OAIC's 2020 ACAPS results found that 77% of respondents considered that they should have a right to object to certain data practices while still being able to access and use the service; Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 67.

Anatomy of the right to object

The scope of the right to object

14.6 We recommend that the right to object applies to all purposes for which an APP entity collects, uses or discloses personal information, subject to the exceptions considered below. This could be modelled on the right to object proposed in s 26KJ(2)(h) of the Online Privacy Bill.

14.7 The right to object should apply to all personal information that an entity 'holds' within the meaning of the Privacy Act, including information held by third parties where the entity has a right or power to deal with that information.[222] This may mean, for example, that an APP entity will have to require third parties to stop handling personal information on its behalf if the handling is subject to a valid objection request in respect of personal information held by the entity.

14.8 While this broad right should be qualified by a reasonable steps test and exceptions (discussed below), we support the introduction of an absolute right to object to direct marketing, including profiling for the purposes of direct marketing. This is considered in more detail at Part 16 of this submission.

14.9 We also recommend that the Review consider extending this absolute right to object to the sharing, disclosure or otherwise making available of an individual's personal information to third parties for a benefit (monetary or otherwise), particularly where the personal information relates to a child. It is important that this absolute right extends to the various ways in which third parties are able to collect personal information from APP entities, whether it be through a purchase arrangement, real time bidding,[223] targeted advertising,[224] or other methods. A similar right is provided under the privacy framework in California,[225] and would align with community expectations around the sharing, disclosure and selling of their personal information.

The OAIC's 2020 ACAPS results found that 59% of Australians have experienced problems with the handling of their personal information. Most occurrences related to unwanted marketing communications, with 43% receiving unsolicited direct marketing without consent or that they were not able to unsubscribe from.[226] This was the most significant problem identified by those surveyed.

---

[222] Privacy Act, s 6 (definition of 'holds'); see also OAIC, *Chapter B – Key Concepts*, OAIC, n.d., accessed 17 November 2021, [B.79] – [B.82].

[223] 'Real time bidding' refers to the practice of organisations auctioning advertising space to advertisers on webpages in real time, as users land on it. This process involves advertisers (sometimes in the hundreds) being sent data such as the user's IP address, device ID, interests, demographics, and location, which are used by advertisers to determine their bidding price. Regardless of whether their bid is accepted, those advertisers have collected that data without paying for it, and may use it to identify an individual in the future.

[224] Advertisers are able to infer information about an individual through targeted advertising (e.g. an individual clicking on an ad for sports merchandise are likely to have an interest in sports). They are also able to embed their own links into a targeted advertisement that directs users to their own webpages, which may then contain cookies or other trackers that collect other user information that may be used to identify them in the future, such as IP addresses and device IDs.

[225] *California Consumer Privacy Act of 2018*, 1.81.5 Cal Civil Code § 1798.135(a)(1).

[226] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 21.

The 2020 ACAPS results also found that 69% of parents are uncomfortable with businesses selling their children's data to third parties.[227] Similarly, the Deloitte Australian Privacy Index 2018 found that 54% of consumers are likely to lose trust in organisations that use their personal information for cross selling, and 68% would likely lose trust for trading data, particularly without prior notice.[228] In the Deloitte Australian Privacy Index 2020, 83% of consumers said they are concerned by internet cookies that track their activity online and use this information for targeted marketing purposes or to sell their information to other companies.[229]

14.10 As noted in the Discussion Paper, an important aspect of the scope of the right to object is to allow an individual to object to certain types of data processing while permitting ongoing information handling for other purposes. This would ensure that individuals may be able to continue using some form of the product or service if they have only objected to a particular aspect of an entity's personal information handling activities.

14.11 The right to object would be supported by proposal 10.1 to apply a fair and reasonable test to assess the collection, use or disclosure of personal information, particularly where an APP entity considers entirely withdrawing their product or service from an individual. As noted in the Discussion Paper, this could involve consideration of the amount and sensitivity of the personal information collected and whether its use was reasonably necessary to achieve the functions and activities of the entity such that the individual could not be offered the service without it. This would be an appropriate safeguard for ensuring that Australians may still fairly access products or services whilst retaining some control over their personal information.

Reasonable steps to comply with an objection request

14.12 We recognise that when personal information is handled for purposes other than direct marketing, it would be impracticable for the right to object to give rise to an absolute obligation for an entity to stop handling the personal information in question. We consider that the requirement that an entity must 'take reasonable steps' to stop handling personal information enables entities to take a flexible, risk-based approach to giving effect to this right, while providing control to individuals over their own personal information.

14.13 The 'reasonable steps' test is common in the Privacy Act and is used throughout the APPs. Relevantly, a similar approach is taken under the existing APP 12 and 13 rights to access and correct personal information and the proposed right to object in the Online Privacy Bill, where entities are required to take steps (if any) as are reasonable in the circumstances.

14.14 What constitutes 'reasonable steps' to stop processing personal information for a specific purpose is an objective test that will vary based on the particular circumstances. Such a test will ordinarily involve consideration of factors such as the possible adverse consequences for the individual as a result of the ongoing collection, use or disclosure of their personal information

---

[227] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 91.

[228] Deloitte, *Deloitte Australian Privacy Index 2018 – The symbiotic relationship*, Deloitte, 2018, accessed 29 November 2021, p 17.

[229] Deloitte, *Deloitte Australian Privacy Index 2020 – Opting-in to meaningful consent*, Deloitte, 2020, accessed 29 November 2021, p 16.

for purpose(s) that is the subject of the objection request and the practicability, including the time and cost involved, in complying with the request.[230] The OAIC would develop guidance on this point and, where appropriate, 'reasonable steps' could also be legislatively defined for industry groups through an APP code.

Exceptions to the right to object

14.15 We recommend introducing clear exceptions to the right to object to help APP entities and individuals understand the scope of this right and to ensure that it does not undermine the effective operation of other aspects of the legal system or the rights of others. The OAIC supports the exceptions suggested in the Discussion Paper, namely, where further collection, use or disclosure is required:

- to complete a transaction or give effect to a contract
- to provide a service or product the individual has requested
- due to the application of an Australian law, court or tribunal order
- due to a permitted general or health situation
- to assist a law enforcement body undertake an enforcement-related activity.

14.16 It is important that the scope of the exception relating to the provision of a product or service is sufficiently narrow to ensure that only circumstances where personal information handling is actually required to provide the service are captured. This exception should not permit the ongoing use or disclosure of personal information if that information is only required to monetise the particular service or the APP entity's business model. The scope of this exception could be set out in the explanatory memorandum to the amendments.

14.17 The Review may wish to consider whether there should be an exception to the right to object where objection would inhibit the handling of personal information for archival, research or statistical purposes in the public interest. This would align with a similar exception proposed for the right to erasure (considered in Part 15 of this submission) and the right to object under the GDPR.[231] However, for the purposes of these exceptions, we suggest that a narrow interpretation of public interest should be adopted to prevent APP entities from rejecting objection requests on the basis of their own commercial research and statistical purposes.

14.18 It may also be appropriate to consider additional exceptions to the right to object based on the exceptions at APP 12.3, for example, where:

- the entity reasonably believes that ceasing to collect, use or disclose would pose a serious threat to the life, health or safety of any individual, or to public health or public safety

[230] These factors, among others, are considered when determining 'reasonable steps' to correct under APP 13; OAIC, 'Chapter 13: APP 13 – Correction of personal information', OAIC, *Australian Privacy Principles guidelines,* OAIC, 22 July 2019, accessed 29 November 2021, [13.47].

[231] GDPR art 21(6).

- ceasing to collect, use or disclose would have an unreasonable impact on the privacy of others
- the information relates to existing or anticipated legal proceedings between the entity and the individual
- ceasing to collect, use or disclose would be unlawful
- the request is frivolous or vexatious.

Recommendation 52 – Adopt proposal 14.1 to introduce a right to object, with the following recommended elements:

- an absolute right to object to direct marketing
- an absolute right to object to the sharing, disclosure or otherwise making available of an individual's personal information to third parties for a benefit (monetary or otherwise), and particularly where the personal information relates to a child
- a reasonable steps test to apply to the collection, use or disclosure of personal information for all other purposes
- appropriate exceptions to the general right to object.

Procedural and notification requirements

14.19 For the right to object to become a valuable privacy self-management tool, it is essential that individuals are provided with effective information to help them understand the specific collections, uses and disclosures they can object to, and the consequences for making this objection. In this context, appropriate procedural and notification requirements will be an important feature for individuals looking to use their new right.

Notification requirements

14.20 We support proposal 8.2 to require APP 5 notices to include information about individuals' right to object and how they may exercise it, which could build on the existing requirements under APP 5.2(h).[232] We also support proposal 8.2 to include notification about purposes for which the entity is collecting and may use or disclosure the information. This information will be necessary for individuals wishing to exercise this right.

14.21 We also recommend that similar information is required to be provided in an APP entity's privacy policy, which could build on the existing requirements under APP 1.3(d).

[232] A similar approach is taken under Article 21(4) of the GDPR.

Requirements when responding to an objection request

14.22 We recommend that requirements about how an entity deals with an objection notice are modelled on the requirements of APPs 12 and 13. Under these APPs, an agency must respond to an access or correction request within 30 days, and an organisation within a reasonable period.

14.23 The substance of a response to an objection request will depend on whether an entity accepts or refuses the request. The quality of the response would also be relevant when assessing whether an APP entity has satisfied their reasonable steps requirements.

14.24 Where an APP entity has accepted an individual's objection request, we agree with proposal 14.1 that the entity should be required to inform that individual of the consequences of their objection, namely what aspects of the product or service will be disrupted or ceased.

14.25 Where an objection notice is refused, we recommend that the response requirements build on those that are prescribed under APP 13 as well as the approach in the UK GDPR. At a minimum, there should be a requirement for the APP entity to:

- give the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so
- inform the individual about the mechanisms available to complain about the refusal.

14.26 However, as stated above, a challenge for individuals in effectively exercising this right will often be to understand the purposes that they can object to. Framing overly broad objection requests, rather than objecting to more targeted, specific purposes, may unnecessarily lock individuals out of accessing products or services or be more likely to trigger one of the exceptions to this right.

14.27 While an appropriately informative APP 5 notice may help individuals in this respect, we recommend that, where an objection notice is refused, APP entities should have obligations to assist individuals or to give some effect to their requests in a more limited way. This type of obligation exists under APP 12 and APP 13, which impose obligations on APP entities even where a request is refused.[233]

14.28 We recommend that this could be achieved through a requirement modelled on existing FOI requirements and could require APP entities to provide 'reasonable assistance' to individuals to reframe their request and provide them with a reasonable opportunity to revise a request, before the objection request is refused.[234] In practice, this may mean that where an entity receives an overly broad objection request, it can provide more detailed information on specific purposes that the individual can object to and the consequences of this. It could also require an entity to explain that it was unable to stop processing personal information for the requested purposes, but that it is able to stop for other purposes.

[233] Under APP 12, where an APP entity refuses to give access to the information, it must take steps as are reasonable to give access in a way that meets the needs of the individual and the entity. Similarly, where an individual refuses to correct information under APP 13, on request by the individual, an entity must take steps as are reasonable to associate a statement with the information that the individual believes it is inaccurate, out-of-date, incomplete, irrelevant or misleading.

[234] OAIC, *Part 3 – Processing and deciding on requests for access*, OAIC, 19 June 2020, accessed 29 November 2021, [3.20].

Recommendation 53 – Adopt proposal 8.2 to require APP entities to notify individuals about their right to object and the purpose(s) for which the entity is collecting and may use or disclose the personal information, and require similar information to be included in APP 1 privacy policies.

Recommendation 54 – Introduce the following procedural elements in relation to a right to object:

- APP entities must respond to objection requests within 30 days (for agencies) or within a reasonable period (for organisations)
- Responses to individuals following an objection request must include information about:
  - the consequences of the individual's objection
  - the entity's reasons for not taking action, if a request is not acted upon
  - the individual's complaint or appeal rights.
- Before an APP entity refuses an objection request, it must provide 'reasonable assistance' to individuals to reframe their request and provide them with a reasonable opportunity to revise a request.

Personal information portability

14.29 The OAIC agrees with Discussion Paper's conclusion that personal information portability rights should not be introduced into the Privacy Act, as this may duplicate aspects of the CDR and create unnecessary regulatory complexity.

Part 15: Right to erasure of personal information

15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions at 15.2, below:

- the personal information must be destroyed or de-identified under APP 11.2
- the personal information is sensitive information
- an individual has successfully objected to personal information handling through the right to object (see Part 14)
- the personal information has been collected, used or disclosed unlawfully
- the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and
- the personal information relates to a child and erasure is requested by a child, parent, or authorised guardian.

15.2 Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either all or some of the personal information held by an APP entity.

15.3 An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

In light of submitter feedback, should a 'right to erasure' be introduced into the Act?

Should an erasure request be only available on a limited number of grounds, as is the case under Article 17 of the GDPR?

What exceptions should apply to address the concerns raised in the government response to the ACCC's DPI report in relation to freedom of speech, challenges during law enforcement and national security investigations, and practical difficulties for industry?

How would entities determine whether one of the exemptions applies in practice?

Would the proposed public interest exception appropriately protect freedom of speech?

Should a right to erasure apply to personal information available online, including search results?

15.1 The OAIC supports the introduction of a right for individuals to request the erasure of their personal information in certain circumstances.

15.2 Under the current Privacy Act framework, individuals have little control over how their personal information is used or disclosed after it is collected.

15.3 As the Discussion Paper and other submissions have noted, a right for individuals to request the erasure of personal information held about them would even out the bargaining position between individuals and APP entities. It would also be consistent with community expectations, as both the OAIC's 2020 ACAPS results and the Deloitte Australian Privacy Index 2021 found overwhelming public support for a right to erasure.

The OAIC's 2020 ACAPS results found that 84% of respondents believe they should have the right to ask a business to delete their personal information.[235] Similarly, the Deloitte Australian Privacy Index 2021 results showed that 79% of individuals surveyed indicated that they would be 'likely' or 'very likely' to use a right to erasure.[236]

15.4 As the Discussion Paper also notes, a right to erasure would enable meaningful withdrawal of consent. Currently, even in the limited circumstances where consent may be withdrawn (that is, in situations where consent has been required under the APPs, as discussed in Part 9 of this submission), there is no right for individuals to request destruction of their personal information.

15.5 Introducing a right to erasure would be an important step in bringing the Australian privacy framework in line with other international jurisdictions, including the UK, the EU and parts of the US. A right to erasure in the Privacy Act would also ensure consistency with other domestic legislative frameworks, such as the CDR and MHR system, which allow individuals to request the deletion of their data in certain circumstances.[237]

15.6 Empowering individuals with a right to erasure is therefore an important development in furthering transparency, privacy self-management, harmonisation and public trust in the Australian privacy framework.

15.7 We recognise that 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. This section considers the potential elements of a right to erasure and makes recommendations to ensure that the right supports the protection of individuals' privacy and the interests of entities in carrying out their functions and activities.

Grounds for an erasure request

15.8 We support the grounds set out in proposal 15.1 upon which an individual may make an erasure request. As the Discussion Paper notes, these are closely modelled on the grounds that underpin the right to erasure in the GDPR.[238]

---

[235] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, p 67.

[236] Deloitte, *Deloitte Australian Privacy Index 2021*, Deloitte, 2021, accessed 29 November 2021, p 11.

[237] *Competition and Consumer Act 2010* (Cth)('CCA') s 56BAA, 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; *My Health Records Act 2012* (Cth) s 17(3), which requires the destruction of records containing health information in a My Health Record upon request by the individual.

[238] GDPR art 17(1).

15.9 We also support extending the right to erasure to de-indexing search engine results, to the extent that the construction of the index requires a collection of personal information.

15.10 We recommend that the right to erasure is qualified with a requirement for APP entities to take reasonable steps to comply with an erasure request.

Where an individual has successfully objected to personal information handling through the right to object

15.11 For Australians to receive the most benefit from the right to erasure, it should be a broad right that is available in relation to all kinds of personal information. This will enable individuals to exercise control over greater volumes of their own personal information and will ensure that the right to erasure is a key privacy self-management tool. As such, we suggest that it is particularly important for the right to erasure to be enlivened where an individual has successfully objected through the right to object, and that the right to object in proposal 14.1 is available for all purposes of collection, use, and disclosure.

Where personal information must be destroyed or de-identified under APP 11.2

15.12 This ground will most likely be enlivened in circumstances where individuals choose to close accounts with APP entities and cease accessing the product or service entirely. To that end, we agree with the Discussion Paper that including this ground has the potential to enhance the operation of APP 11.2 by allowing individuals to initiate a process that should already happen, but may not.

15.13 The OAIC would build on our existing guidance on the application of APP 11.2 to assist individuals to understand what information is required to be destroyed or de-identified and when.[239] We expect that the processes and procedures that APP entities have in place to meet their existing obligations under APP 11 would ease the burden of complying with a new right of erasure.

Application of a right to erasure to personal information in a generally available publication and search results

15.14 We support a right to erasure that includes de-indexing search results on search engines where the construction of a search index involves a collection of personal information. Such a right should not be absolute and would need to operate with exceptions and meaningful regulatory guidance to assist search engine operators in decision-making under this right.

15.15 This is consistent with recommendation 23 in our submission to the Issues Paper to extend the right to erasure to personal information that is no longer 'held' by an entity and to notify others

[239] OAIC, 'Part 11: APP 11 – Security of personal information', *Australian Privacy Principles Guidelines,* OAIC, 22 July 2019, accessed 29 November 2021.

of the erasure request where personal information has been made public. This would importantly include personal information held in a generally available publication.[240]

15.16 We recognise that the right to erase personal information from the public domain may be complex in practice. In the EU, this is known as the 'right to be forgotten' and applies where search engines receive de-indexing requests for indexed links that are 'inadequate, irrelevant or no longer relevant, or excessive'.[241] As the Discussion Paper notes, the right is not absolute, and execution involves the consideration of individuals' privacy rights, the freedom of expression, and the public interest in accessing information that may be relevant to public discourse.[242]

15.17 However, we consider that there is substantial public interest in introducing a right to erasure in Australia that includes de-indexing search engine results. The permanence of content on the internet is a significant challenge to the privacy of individuals. Content that may be embarrassing, harmful, inaccurate or irrelevant is easily accessible within fractions of a second after a search engine query involving an individual's name. The same is true for content that may be potentially defamatory, where in the absence of a right to de-index that material, individuals are required to engage in costly and laborious court action to achieve that result.

15.18 The ideal resolution to these problems may naturally be the complete removal of this content from the source that posted it. However, for a variety of reasons, this is not always possible (for example, where sources may be offshore, anonymous, or ignore takedown requests), and may not always be effective where other internet users replicate that content and spread it elsewhere online.

15.19 There is a strong case for a right to de-index in circumstances such as these, given the risk to individuals' privacy arises from the ability to find and access this content from a search engine query involving an individual's personal information, usually their name. Further, de-indexing is a relatively fast and cost-effective way for individuals to self-manage their personal information in these circumstances. Google's own research has found that over 92% of European de-indexing requests targeting personal or sensitive information result in a successful de-indexing,[243] and that the median time for processing a de-indexing request was 6 days.[244]

15.20 As an Australian right to de-index search results will simply be a function of the right to erasure, the same exceptions that will limit other erasure requests (discussed below) will also apply to a right to request the de-indexing of search engine results. Notably, the public interest exception will require search engine operators to assess whether the risk to an individual's privacy is proportionate to free expression and the public interest in accessing that information about an individual. This would not be significantly different to the current considerations of search

---

[240] A generally available publication is defined under s 6 of the Privacy Act to mean a magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public: (a) whether or not it is published in print, electronically or in any other form; and (b) whether or not it is available on the payment of a fee.

[241] *Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos* (Court of Justice of the European Union, Case C-131/12, 13 May 2014).

[242] Yann Padova, 'Is the right to be forgotten a universal, regional or 'global' right?', *International Data Privacy Law*, 2019, 9(1):15-29, p 16; *Google Spain SL v Agencia Espanola de Proteccion de Datos* ([81]).

[243] Theo Bertram et al., 'Five years of the right to be forgotten', *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 6 November 2019, accessed 29 November 2021, p 10.

[244] Theo Bertram et al., 'Five years of the right to be forgotten', *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 6 November 2019, accessed 29 November 2021, p 6.

engine operators when dealing with erasure requests under the GDPR.[245] The regulatory burden of this new right would therefore be eased given these existing systems and processes.

15.21 To further ease the regulatory burden, the OAIC would develop guidance on assessing public interest in subject matters such as those involving public officials, politicians, crimes and court matters, among others, as well as the role of free expression where news articles are the source of de-indexing requests. This could be based on the OAIC's existing guidance on the public interest test under the FOI Act.[246]

15.22 For these reasons, we recommend introducing a right to erasure that includes the de-indexing of search engine results, to the extent that the construction of a search index involves a collection of personal information.

Taking reasonable steps to comply with an erasure request

15.23 We note that an exception has been proposed for circumstances where erasure is technically impractical or would constitute an unreasonable burden. We consider that the same effect could be achieved through a reasonableness threshold drafted into the operative language of the right. This is consistent with the other rights for individuals in the APPs and our recommendation about the right to object in Part 14.

15.24 A reasonableness threshold is an appropriate way of addressing concerns raised in submissions to the Issues Paper about the technical impracticality of deleting some kinds of records. It is also consistent with the framing of the right to erasure in two other domestic legislative regimes, where reasonableness is an operative threshold:

- the CDR regime, which requires that data must be deleted 'to the extent reasonably practicable' upon request from a consumer[247]
- the COVIDSafe app regime, which requires the data store administrator to 'take all reasonable steps to delete the data from the National COVIDSafe Data Store as soon as practicable'.[248]

15.25 Reasonableness is also an operative threshold under several APPs, notably APPs 5, 10, 11, 12, and 13, all of which require APP entities to 'take such steps (if any) as are reasonable in the circumstances' to carry out their respective obligations under each APP.

15.26 Building on guidance on an equivalent right under the CDR and suggested factors in the Discussion Paper, the following factors could be included in OAIC guidance as being relevant to reasonable steps in relation to the right to erasure:

---

[245] GDPR art 17(3)(d); Theo Bertram et al., 'Five years of the right to be forgotten', *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 6 November 2019, accessed 29 November 2021, p 2.

[246] OAIC, 'Part 6 – Conditional exemptions', *Freedom of Information guidelines,* OAIC, 19 December 2016, accessed 29 November 2021, [6.19]-[6.22].

[247] CCA, s 56BAA; *Competition and Consumer (Consumer Data Right) Rules* 2020 rule 1.18.

[248] Privacy Act s 94L.

- the amount of personal information – more rigorous steps may be required as the quantity of information increases
- the possible adverse consequences for an individual if their personal information is not properly deleted – more rigorous steps may be required as the risk of adversity increases
- the practicality, including time and cost involved – although an APP entity would not be excused from deleting personal information by reason only that it would be inconvenient, time-consuming or impose some cost to do so[249]
- the technical capabilities of an APP entity
- a proportionality test that measures whether the burden or expense of erasure would be disproportionate to the risks to the consumer's privacy or community expectations in each case.

15.27 A 'reasonable steps' test would be supported by recommendations in Part 20 of this submission about enhanced organisational accountability requirements. For example, our recommendation to require APP entities to take a privacy by design approach would ensure that straightforward ways to delete or anonymise personal information are built into new technologies or applications to enable entities to more easily respond to erasure requests.

Exceptions to the right to erasure

15.28 We recognise that it is important for there to be exceptions to the right to erasure to address the impact of the right on issues such as the public interest, freedom of speech, challenges during law enforcement and national security investigations, and general practical difficulties for industry.

15.29 The Discussion Paper suggests possible exceptions to the right to erasure, a number of which are discussed below.

Where erasure would be technically impractical or constitute an unreasonable burden

15.30 As recommended above, we consider that the outcome that this exception is designed to achieve would be better addressed by introducing a reasonableness threshold into the operative language of the right. This would ensure consistency the APPs and other domestic rights to erasure, and align with our recommendation regarding the right to object in Part 14 of this submission.

Where erasure would hinder law enforcement

15.31 We support an exception to the right to erasure where erasure would hinder law enforcement, particularly where the subject data may reveal an individual's involvement in serious criminal

[249] OAIC, *CDR Privacy Safeguard Guidelines*, OAIC, 9 June 2021, accessed 29 November 2021, [12.106] – these elements inform the meaning of deleting data 'to the extent reasonably practicable'.

activity such as online child sexual abuse, human trafficking, illicit drug trafficking, money laundering, tax evasion, bribery and fraud.

15.32 We are cognisant of the challenges that a right to erasure creates in this context. For example, we note the challenges that a law enforcement exception may present in the absence of an approach from law enforcement at the time of an erasure request. However any exception for the rejection of erasure requests on the basis that a law enforcement agency may approach the APP entity at an unknown point in time in the future would be too broad. We support the proposal in the Discussion Paper to model such an exception on the existing APP 12.3(i), which should adequately address this concern.

15.33 We also support the proposal to model an exception to erasure on APP 12.3(b), where erasure would have an unreasonable impact on the personal information of another individual (for example, phone call records or multiplayer video game history and online chat logs). We consider that this would be a proportionate response to protect the community against serious criminal activity, potentially involving children. We agree with the Discussion Paper's suggestion that such an exception would operate more broadly than the law enforcement context, given the practical implications that would arise from erasing joint personal information at an individual's request.

Where erasure would be contrary to the public interest and freedom of expression

15.34 We support an exception to the right to erasure modelled on the public interest test under the FOI Act, which would consider whether 'erasure of the personal information in the circumstances would, on balance, be contrary to the public interest'. We recognise that there are likely to be legitimate circumstances in which information should be retained as relevant to the public interest, for example, where freedom of speech and freedom of the media are concerned. Introducing a right to erasure with a public interest exception would also align with the GDPR.[250]

15.35 The OAIC already provides extensive guidance on the operation of the public interest test within the FOI Act.[251] This includes non-exhaustive lists of public interest factors for and against disclosure.[252] Adapted guidance in the context of the right to erasure could include consideration of whether a particular erasure or retention of personal information would:

- promote the objects of the Act
- inform the public, or enable debate on a matter of public importance
- constitute an unreasonable limitation on the expression of a legitimate view or opinion

[250] GDPR art 17(3)(d).

[251] OAIC, Part 6 – Conditional exemptions, *Freedom of Information guidelines,* OAIC, 19 December 2016, accessed 29 November 2021.

[252] OAIC, Part 6 – Conditional exemptions, *Freedom of Information guidelines,* OAIC, 19 December 2016, accessed 29 November 2021, [6.17]—[6.22].

- inhibit the handling of personal information for archival, research or statistical purposes, journalistic purposes; or for academic, artistic or literary expression in the public interest.

15.36 As noted in Part 14 of this submission, to the extent that there is a public interest test applied to a research or statistical exception, that test should be narrowly constructed to prevent APP entities from rejecting erasure requests on the basis of their own commercial research and statistical purposes.

Other exceptions

15.37 We support the list of possible further exceptions included in the Discussion Paper. We recommend that these are modelled on relevant existing exceptions in APP 12, to the extent possible.

Recommendation 55 – Adopt proposal 15.1 and 15.2 to introduce a general right to erasure that includes a right to de-index search results and a requirement for APP entities to take reasonable steps to carry out an erasure request, subject to exceptions including:

- where erasure would hinder law enforcement
- where erasure would be contrary to the public interest and freedom of expression
- where personal information is required for a transaction or contract
- where the personal information sought to be erased is contained in a Commonwealth record
- where the entity is required to retain the information by or under an Australian law, or court/tribunal order
- where a request is 'frivolous or vexatious', consistent with APP 12
- where erasure would have an unreasonable impact on the personal information of another individual
- where erasure would pose a serious threat to the life, health or safety of any individual, or to public health and safety
- where personal information is required for the purposes of occupational medicine or for the management of health or social care systems or services
- where the information is required for archival, research or statistical purposes in the public interest
- where the information relates to existing or anticipated legal proceedings between the entity and the individual.

Procedural considerations

15.38 We recommend that the procedural considerations in relation to the right to erasure align as much as possible to those under APPs 12 and 13 and the right to object.

15.39 To this end, we support proposal 8.2 for APP 5 notices to include information about individuals' right to erasure and how they may exercise it, which could build on the existing requirements under APP 5.2(h). We also recommend that similar information is required to be provided in an APP entity's privacy policy, which could build on the existing requirements under APP 1.3(d). Adequately informing individuals of their right to erasure will be an important aspect of their ability to exercise their right.

15.40 We also support proposal 15.3 that APP entities must respond to erasure requests within a reasonable period. As we recommended in Part 14 of this submission in respect to the right to object, this could be based on APPs 12 and 13 where an agency is required to respond to access or correction requests within 30 days, and an organisation within a reasonable period.

15.41 We recommend that the same procedural framework is adopted as our recommended approach to the right to object in Part 14 of this submission:

- in the event of an acceptance of an erasure request, the entity should be required to inform that individual of the consequences of the erasure of their personal information
- in the event of a refusal of an erasure request, we support the requirement set out in proposal 15.3 for an APP entity to give the individual written notice that sets out the reasons for refusal and mechanisms available to complain.

15.42 To further align the procedural elements of the right to erasure with APPs 12 and 13, we recommend that where an erasure request is refused, APP entities should have obligations to assist individuals or to give some effect to their requests in a more limited way.[253]

15.43 We recommend that the obligations to erase 'a record' should include erasing any copy of the record, any previous version of the record and any back-up version of the record. This would align with the right to erasure under the MHR system. The right to erasure should also cover inferred personal information (unless it has been de-identified). As outlined in Part 2 of this submission, if inferred information is about an individual or reasonably identifiable individual, it will be personal information that has been collected for the purposes of the APPs. Ensuring that inferred information is captured in the right to erasure would align with the similar right in relation to derived data under the CDR.

15.44 We also reiterate recommendation 23 of our submission to the Issues Paper that the right to erasure should extend to personal information that is no longer 'held' by an entity, so that the entity would be required to notify others of the erasure request. This could be modelled on Article 19 of the GDPR, which requires third party notification unless this proves impossible or

[253] Under APP 12, where an APP entity refuses to give access to the information, it must take steps as are reasonable to give access in a way that meets the needs of the individual and the entity. Similarly, where an individual refuses to correct information under APP 13, on request by the individual, an entity must take steps as are reasonable to associate a statement with the information that the individual believes it is inaccurate, out-of-date, incomplete, irrelevant or misleading.

involves disproportionate effort. The right to deletion in section 1798.105 of the *California Privacy Rights Act 2020* also uses this wording.

15.45 Finally, we recommend that the right to erasure includes a requirement for APP entities to verify the identity of the requesting individual to ensure that the request is made by the individual concerned, or by another person who is authorised to make a request on their behalf, for example, as a legal guardian or authorised agent. This could be modelled on our existing APP 12 guidance.[254]

Recommendation 56 – Adopt proposal 8.2 to require APP entities to notify individuals about their right to erasure and require similar information to be included in APP 1 privacy policies.

Recommendation 57 – Adopt proposal 15.3 to require an APP entity to respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

Recommendation 58 – Provide that the right to erasure extends to erasure of:

- any copy of the record
- any previous version of the record
- any back-up version of the record
- any inferred personal information unless it has been de-identified
- personal information that is no longer 'held' by an entity, so that APP entities are required to notify others of the erasure request where personal information has been made public.

[254] OAIC, 'Chapter 12: APP 12 — Access to personal information', *Australian Privacy Principles guidelines,* OAIC, 22 July 2019, accessed 29 November 2021, [12.15]-[12.17].

Part 16: Direct marketing, targeted advertising and profiling

16.1 The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.

On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

16.2 The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected.

16.3 APP entities would be required to include the following additional information in their privacy policy:

- whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and

- whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.

16.4 Repeal APP 7 in light of existing protections in the Act and other proposals for reform.

Should express consent be required for any collection, use or disclosure of personal information for the purpose of direct marketing?

What are some of the practical challenges of implementing a global opt-out process, to enable individuals to opt out of all online tracking in one click?

What are the potential impacts of requiring that use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions be a primary purpose to be notified to the individual when their personal information is collected?

Is there any benefit in regulating direct marketing through a separate privacy principle or should APP 7 be removed in light of other proposals for reform?

Should the unqualified right to object to marketing extend to the collection and use of personal information where it is aggregated with the personal information of other users for marketing targeted at cohorts rather than individuals?

Do customer loyalty schemes offer more tangible benefits to consumers, and should they be regulated differently to other forms of direct marketing?

16.1 APP 7 applies to the use and disclosure of personal information for certain methods of direct marketing, as discussed further below. Direct marketing involves the use and/or disclosure of personal information to communicate directly with an individual to promote goods and services.[255]

16.2 The explanatory memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 notes that direct marketing is addressed separately in APP 7 because of the significant community interest about the use and disclosure of personal information for the purposes of direct marketing.[256]

16.3 However, privacy risks associated with direct marketing have changed significantly since 2012 when the APPs were introduced. Privacy risks have emerged because of the use of high volumes of data, often involving personal information, by adtech services that deliver targeted or personalised advertising on websites and apps.

16.4 These privacy risks have been compounded due to the increasingly complex methods of online targeted marketing involving multiple parties, the increased use of cookies and other online identifiers, and new developments in the way that data is handled.[257]

16.5 As noted in the Discussion Paper, targeted advertising is often dependent on a technique known as 'profiling.'[258] Generally, profiling involves analysing aspects of an individual's personality, behaviour, interests and habits to make predictions or decisions about them.[259]

16.6 The Issues Paper asked whether the Privacy Act strikes the right balance between the use of personal information in relation to direct marketing, and whether privacy protections for individuals could be improved. The Discussion Paper indicates that the direct marketing of greatest concern to submitters to the Issues Paper is targeted online advertising, also known as behavioural advertising.[260]

16.7 This is consistent with the OAIC's 2020 ACAPS results, which found that at least 89% of the Australians surveyed are uncomfortable or very uncomfortable with digital platforms and other online businesses like social media sites targeting advertising based on what they have said and done online.[261]

16.8 The 2020 ACAPS results also demonstrated that overall comfort with data practices vary according to the type of information collected, the organisation involved and the purpose

---

[255] OAIC, 'Chapter 7: APP 7 – Direct marketing', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 11 November 2021.

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

[257] OAIC, *Digital Advertising Services Inquiry – Interim Report,* OAIC website, 31 March 2021, accessed 11 November 2021.

[258] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 11 November 2021, p 124.

[259] UK ICO, 'What is automated individual decision-making and profiling?', *Guide to the General Data Protection Regulation (GDPR)*, ico.org.uk, n.d., accessed 11 November 2021.

[260] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 11 November 2021, p 124.

[261] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p 29.

behind it. Commercial profiling activities generally drive higher levels of discomfort among Australians than government data practices. For example:

- 55% of survey respondents were uncomfortable with a business creating profiles about consumers based on data collected about them
- 53% are uncomfortable with a business combining data about their customers (for example, loyalty card transaction history) with other data (for example, IP address, type of browser used) to better profile their customers.[262]

16.9 We consider that proposals 16.1 and 16.4, combined with other key reforms recommended in this submission, will help to address the privacy risks associated with tracking and profiling individuals for the purposes of targeted online advertising, and community concerns associated with these practices. These are discussed in more detail below.

Unqualified right to object to direct marketing

16.10 We support proposal 16.1 to introduce an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. The proposal would also require an organisation that provides marketing material to an individual to notify the individual of their right to object in relation to each marketing product provided.

16.11 We note the right would differ from the general right to object discussed in Part 14 of this submission, as entities would need to stop, not just take 'reasonable steps' to stop, the collection, use or disclosure of personal information for direct marketing purposes. This means that 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.

16.12 This approach aligns with Article 21 of the GDPR and the UK GDPR, which provides individuals with an absolute right to object to the processing of their personal data for direct marketing at any time. It is an absolute right, which means there are no exemptions or grounds for an entity to refuse.[263]

16.13 The introduction of an unqualified right to object in relation to direct marketing would address concerns highlighted by submitters around the limited scope of the existing protections contained in APP 7.

16.14 Specifically, APP 7 does not regulate the *collection* of personal information for direct marketing purposes and therefore does not permit an individual to opt out of having their online behaviour tracked and personal information collected for direct marketing purposes. Instead, individuals are only able to opt out of *receiving* marketing communications. There is no requirement in APP 7 to permit individuals to opt out of their personal information being used or disclosed for direct marketing purposes.

---

[262] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p 32.

[263] UK ICO, 'Right to object', *Guide to the General Data Protection Regulation (GDPR)*, ico.org.uk, n.d., accessed 11 November 2021.

16.15 The unqualified right to object would provide individuals with the ability to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing.

16.16 Relatedly, we also support proposal 16.4 to repeal APP 7 if proposal 16.1 is implemented. As noted in our submission to the Issues Paper, 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* (DNCR Act) or the Spam Act applies. 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 and door-to-door direct marketing, and
- targeted marketing online (including on websites and mobile apps), but only if personal information is used or disclosed to target that marketing.[264]

16.17 Repealing APP 7 would help to address concerns raised by submitters that the regulatory framework which spans APP 7, the Spam Act and the DNCR Act, establishes different obligations for different marketing channels. Submitters to the Issues Paper noted that this creates regulatory fragmentation and confusion for consumers and industry.[265]

16.18 If APP 7 is 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.

16.19 This approach would be enhanced by proposal 10.1 to introduce a requirement that a collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances. This would address concerns about unfair and unreasonably intrusive collections, uses and disclosures of personal information for direct marketing purposes. Proposal 10.1 is discussed in detail in Part 10 of this submission.

16.20 To ensure the existing protections of APP 7 are preserved, we also recommended in our submission to the Issues Paper that the right to object in relation to direct marketing should also include the ability for individuals to request an organisation to identify the source of the personal information that it uses or discloses for direct marketing. An entity should be required to notify the individual of its source, unless that is unreasonable or impracticable.[266]

16.21 To that end, we support proposal 18.1 to require an organisation to identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort (discussed further in Part 18 of this submission).

[264] OAIC, *Direct marketing*, OAIC website, 1 May 2019, accessed 11 November 2021.

[265] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 11 November 2021, p 129.

[266] Recommendation 19. OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, p 46.

Recommendation 59 – Adopt proposal 16.1 that the right to object would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing.

Recommendation 60 – Adopt proposal 16.4 to repeal APP 7 in light of existing protections in the Act and other proposals for reform.

Influencing an individual's behaviour or decisions

16.22 Proposal 16.2 would require that the collection, use or disclosure of personal information for the purposes of influencing an individual's behaviour or decisions must be a primary purpose notified to an individual at the point of collection.

16.23 The Discussion Paper notes that this would encompass not only the collection, use and disclosure of personal information for targeted advertising of goods and services to consumers, but also the use of profiling to target individuals with ideological or political messaging.[267]

16.24 We support the objective of the proposal to increase the transparency of the collection, use and disclosure of information for direct marketing purposes and address concerns about the prevalence of third parties collecting, using and disclosing personal information in the process of delivering targeted advertising to individuals without their knowledge.[268] However, we have recommended some alternative solutions which we consider would achieve the same objective for the reasons outlined below.

16.25 The concept of 'influencing an individual's behaviour or decisions' is very broad. The proposal would require notification where personal information is used to influence behaviour or decisions regardless of whether the influence is positive or negative or whether the conduct occurs in the online or offline context. For example, newsletters from a general practitioner or other health care provider that are intended to notify individuals of health-related services (such as flu shots or new programs to quit smoking) could be construed as 'influencing an individual's behaviour or decisions.'

16.26 Further, it may extend to other practices in the online environment beyond those associated with targeted online advertising. For example, the concept of 'influencing an individual's behaviour or decisions' could include the design of websites and platforms, including personalised features, the order that search results are presented and the selection of default options. This may risk impeding innovative design features developed in the interests of the individual.

16.27 As discussed in Part 10 of this submission, we are also mindful that there may be unintended consequences of proposal 10.4, and by implication proposal 16.2, which links the primary purpose to what is notified to the individual.

---

[267] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 11 November 2021, p 132.

[268] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 11 November 2021, p 132.

16.28 The OAIC's APP guidelines establish that assessing the primary purpose for collection is an objective test informed by the circumstances surrounding the collection.[269] The objective nature of the test places crucial limits on the abilities of APP entities to subjectively define the primary purpose of collection.

16.29 By linking the primary purpose to the purpose notified to the individual, proposal 10.4 and 16.2 will detract from the objective nature of this assessment. It is also not clear how this definition will apply where notice is not necessary under APP 5 or where the Commissioner decides that the primary purpose(s) included in a collection statement is invalid in the context of a privacy determination.

16.30 We consider that the combined effect of proposals 10.4 and 16.2 may also result in an overly legalistic approach to drafting APP 5 notices, given the authorisation to use and disclose personal information would be linked to the purposes notified in a collection notice. This is inconsistent with the intention of these notices, which should be written in clear and plain language to support individuals to understand how their personal information will be handled.

16.31 Similarly, requiring entities to classify a greater range of uses and disclosures as primary purposes will likely increase the length of notices to include an extensive list of activities and/or cause entities to define their primary purposes very broadly and ambiguously to encompass a wide range of different activities.

16.32 Given the concerns associated with influencing an individual's behaviour or decisions for the purposes of targeted online advertising are confined to the online context, we consider that additional requirements to address this practice are more appropriately implemented through the proposed OP code. It is already contemplated that the OP code will make provision in relation to notice of the collection, use and disclosure of personal information.[270]

16.33 We consider that other measures proposed in the Discussion Paper and recommended in this submission will more appropriately and effectively address the privacy risks associated with tracking and profiling individuals for the purposes of targeted online advertising, and community concerns associated with these practices. In addition to proposals 16.1 and 16.4 in this Part, these measures include:

- the fairness and reasonableness requirements outlined in proposal 10.1, which would help to address concerns about unfair and unreasonably intrusive collections, uses and disclosures of personal information for direct marketing purposes (see Part 10 of this submission)
- proposal 11.1 to require APP entities that engage in certain restricted practices to take reasonable steps to identify privacy risks and implement measures to mitigate those risks including 'direct marketing, including online targeted advertising on a large scale' (see Part 11 of this submission)

---

[269] OAIC, 'Chapter B: APP 7 – Key concepts', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 11 November 2021; 'WZ' and CEO of Services Australia (Privacy) [2021] AICmr 12 (13 April 2021) at [148].

[270] Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Exposure Draft), ss 26KC(2)(c), (f) and (g).

- option 1 of proposal 12.1, which would require all settings to be set to privacy protective as default except for the collection, use or disclosure of personal information that reasonably enables provision of the particular product or service. This would help to ensure a higher level of user engagement with, and awareness of, privacy settings before APP entities can collect, use and disclose personal data for a purpose that is not required to reasonably enable provision of the product or service the consumer requested, such as targeted online advertising (see Part 12 of this submission)
- our recommendation to amend APP 3 to expressly require entities to specifically determine, at or before the time of collection, each of the known purposes for which the information is to be collected, used or disclosed and to record those purposes. This will support fundamental data protection concepts of purpose limitation and data minimisation, ensure entities have a clear and specific purpose in mind for the subsequent handling of the information, and help entities to clearly formulate and document the information they must provide to individuals through their APP 1 privacy policy and APP 5 notices (see Part 20 of this submission).

Recommendation 61 – Consider alternative solutions for meeting the objectives of proposal 16.2, including:

- implementing additional requirements to address the privacy risks associated with tracking and profiling individuals for the purposes of targeted online advertising through the OP code
- adopting proposal 10.1
- adopting proposal 11.1
- adopting option 1 of proposal 12.1
- adopting the OAIC's recommendation to amend APP 3 to expressly require entities to specifically determine, at or before the time of collection, each of the known purposes for which the information is to be collected, used or disclosed and to record those purposes.

Information on direct marketing in APP privacy policy

16.34 Under proposal 16.3, APP entities would be required to include the following additional information in their privacy policy:

- whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and

- whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.

16.35 As noted above, influencing behaviour is a broad concept that could apply to a variety of conduct in the online and offline environments, not just targeted online advertising. This may result in overly lengthy privacy policies that do not highlight the key information-handling practices of concern in the online context.

16.36 Entities already have an obligation under APP 1.4 to include information in their APP privacy policy about, amongst other things, the purposes for which the entity collects, holds, uses and discloses personal information. For example, the policy should:

- cover each of these topics for each of the entities key functions and activities involving personal information
- focus in most detail on the particular uses or disclosures that individuals are most likely to be concerned about or interested in
- indicate the functions or activities for which the entity uses third party contractors.[271]

16.37 We understand the objective of proposal 16.3 is to address transparency concerns around certain data practices in the online context. We consider these are more appropriately addressed on a sector-specific basis through APP codes, rather than an economy-wide basis in the Privacy Act itself.

16.38 To this end, we note that the Online Privacy Bill will require the proposed OP code to set out how an OP organisation's APP privacy policy is to comply with APP 1.4(c) in stating the purposes for which the organisation collects, holds, uses and discloses personal information. Consequently, the OP code could provide further prescription around the matters that an OP organisation's privacy policy must address after further input and consultation with industry.

Recommendation 62 – Consider whether the objectives of proposal 16.3 could be achieved through the proposed OP code.

Recommendation 63 – If proposal 16.3 is adopted, consider how the obligations to include the relevant information in an APP privacy policy could be framed to ensure they do not have unintended consequences or require disproportionate effort by entities to meet the requirements.

[271] OAIC, *Guide to developing an APP privacy policy*, OAIC, 5 May 2014, accessed 11 November 2021, pp 12-13.

Part 17: Automated decision-making

17.1 Require privacy policies to include information on whether personal information will be used in ADM which has a legal, or similarly significant effect on people's rights.

Should the concept of a decision with 'legal or similarly significant effect' be supplemented with a list of non-exhaustive examples that may meet this threshold?

17.1 We support proposal 17.1 in principle, which will build on the organisational accountability obligations that we have recommended in relation to automated decision-making (ADM) as a potential restricted purposes in Part 11 of this submission.

17.2 This technology has the potential to create significant opportunities and efficiencies for society, but these benefits will only be fully enabled if the risks are appropriately mitigated. Sensible and proportionate legislation will be an important part of addressing these risks and building trust in this technology.

17.3 The Privacy Act is technology-neutral and already places important obligations on APP entities relying on ADM that uses personal information. This includes 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.

17.4 These existing obligations will be enhanced by proposals in the Discussion Paper, as well as the recommendations in this submission, including recommended privacy by design requirements, and objection and erasure rights. We have also recommended additional organisational accountability requirements in relation to restricted purposes (discussed in Part 11 of this submission) that will be important for ADM systems, including mandatory PIA requirements and regular training. The flexible fair and reasonable test will also be important given that AI technology is evolving and being deployed to handle personal information in increasingly innovative ways.

The OAIC's 2020 ACAPS results found that Australians want more rights in relation to the use of AI technologies:

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.

Enhanced notice provisions

17.5 The personal information handling for the purposes of ADM is often driven by sophisticated technology that may be difficult for individuals to understand. It essential for the Privacy Act to

apply appropriate transparency measures to the use of this technology to ensure that individuals can understand the decisions being made about them and exercise their privacy rights.

17.6 Proposal 17.1 will ensure that individuals that read a privacy policy will understand that ADM may take place. Supplementing this proposal, in Part 2 of this submission, we reiterate the recommendation from our Issues Paper submission that APP privacy policies should contain information about whether information will be anonymised and used for purposes other than those permitted for the initial collection. An important example of this would be the use of anonymised information to train ADM systems.

17.7 We recommend that proposal 17.1 is expanded to also require APP entities to provide more specific information to individuals about any ADM systems or processes. A similar approach has recently been taken in amendments to the Privacy Act in relation to the generation of credit ratings, which are ordinarily derived through automated processes.[272] Under these changes, where an individual seeks information including a credit rating from a credit reporting body, the information provided will have to include:

- the credit rating of the individual
- information that identifies the particular credit information that is held by the body and from which the credit rating was derived
- information about the relative weighting of the credit information described above in deriving the credit rating
- information about what the other ratings on the scale or range are, and how the individual's credit rating relates to those other ratings.

17.8 As highlighted in the Discussion Paper, this approach has been taken internationally including in the GDPR[273] and the Californian Privacy Rights Act,[274] commencing in 2023.[275] This approach is also being considered in Canada.[276]

17.9 We recommend a similar approach is introduced under the APPs to require APP entities to provide a meaningful explanation to individuals about automated decisions in privacy policies and APP 5 notices. This could include information about the types of personal information being used in an automated decision, how that information is weighted and, where appropriate, information about how any ratings given to an individual relates to other information or decisions.

---

[272] *National Consumer Credit Protection Amendment (Mandatory Credit Reporting and Other Measures) Bill 2021, Item 25A* and *Financial Rights Legal Centre Inc. & Others and Veda Advantage Information Services and Solutions Ltd* [2016] AICmr 88 (9 December 2016), [257]

[273] GDPR, Articles 22, 13(2)(f), 14(2)(g) & 15(1)(h)

[274] Californian Privacy Rights Act (n 116) 1798.185(16).

[275] Other jurisdictions include the *Brazilian General Data Protection Law*, Art. 20; *South African Protection of Personal Information Act*, s. 71

[276] Bill C-11 (n 402) sub-cl 63(3).

17.10 The Review should also consider whether to supplement these notice requirements with a requirement to provide a more technical explanation of the ADM process upon request, to more easily help individuals challenge an automated decision made about them. This would have to be appropriately tailored to address issues of commercial confidence. For example, the Privacy Act currently provides an exception 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.

17.11 Given that similar laws have been enacted in comparable laws overseas, the regulatory burden of introducing these reforms may be reduced for APP entities already complying with these laws.

Recommendation 64 – Extend proposal 17.1 to require APP entities engaging in ADM to include a meaningful explanation of these automated decisions in privacy policies and APP 5 notices. This could include information about the types of personal information being used in an automated decision, how that information is weighted and, where appropriate, information about how any ratings given to an individual relate to other information or decisions.

Recommendation 65 – Consider whether these explanations should include more technical information that may assist individuals to contest these decisions and, if so, whether appropriate exceptions are necessary to protect any trade secrets in respect to the ADM system being used.

Application to automated decision-making

17.12 Given that the general protections in the Privacy Act will apply to personal information used in ADM, the additional protections proposed in this section and in relation to restricted purposes should be appropriately tailored and only apply to more high-risk automated decisions.

17.13 As stated in our submission to the Issues Paper, we do not recommend that the test in the GDPR is adopted, as it only applies to decisions based 'solely' on automated processing.[277] We are concerned that this formulation is too narrow and could be avoided by artificially including human involvement in a process. Rather, we suggest that the term 'AI informed decision-making', proposed in the AHRC's Human Rights and Technology Final Report is an appropriate starting point.[278] Submissions to the Discussion Paper will assist to identify any unintended consequences of including this definition in the Privacy Act.

17.14 The Discussion Paper also observes some of the challenges that other jurisdictions have faced in interpreting the term 'similarly significant'. We suggest that additional clarification about this term could be included in the Privacy Act or explanatory materials.

[277] GDPR, Article 22

[278] See AHRC, *Human Rights and Technology Final Report*, AHRC, March 2021.

17.15 Our submission to the Issues Paper highlighted developments in the United States where draft privacy legislation has sought to provide additional clarification on the scope of this term. This included 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.[279] Recently, these Bills have additionally referred to the provision of basic necessities, such as food and water, as potentially significant effects of an automated decision. A reference to social security may also be appropriate in an Australian context.

17.16 This could be an appropriate model, either for inclusion in the Privacy Act or in the explanatory memorandum, which can be further clarified through OAIC guidance. Care should be taken to ensure that these new provisions intersect appropriately with Part IIIA of the Privacy Act.

Recommendation 66 – Ensure that additional protections for ADM apply to AI informed decision-making that has a legal or similarly significant effect.

Recommendation 67 – Introduce clarification around the concept of a decision with 'legal or similar significant effect' in the legislation or explanatory materials.

[279] *Consumer Rights to Personal Data Processing Bill* HF 1492 (Minnesota); *New York Privacy Bill* SB A680A (New York); *Protecting Consumer. Data Bill* SB 5376 – 2019-20 (Washington State).

Part 18: Accessing and correcting personal information

18.1 An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

18.2 Introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:

- the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.

18.3 Clarify the existing access request process in APP 12 to the effect that:

- an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature, and

- where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.

Is there evidence that individuals are being refused access to personal information that is inferred about them? In particular, is the exception at APP 12.3(j) being relied on to refuse individuals' requests to access inferred personal information?

Is there evidence to suggest that organisations are taking longer than a reasonable period after a request is made to grant individuals access to their personal information?

Should an APP entity be required to keep personal information it has published online accurate, up-to-date and complete, and to correct it upon request – to the extent that the entity retains control of the personal information?

Inferred personal information

18.1 APP 12 provides that if an APP entity holds personal information about an individual, the entity must, on request, give the individual access to the information unless an exception applies.

18.2 The Discussion Paper indicates that some submitters to the Issues Paper considered that individuals should have a greater ability to access personal information that is inferred about them by APP entities.[280]

18.3 The Privacy Act defines 'personal information' as information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is

[280] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 140.

true or not, and whether the information or opinion is recorded in a material form or not.[281] OAIC guidance notes that common examples of personal information include commentary or opinion about a person including 'information or opinion inferred about an individual from their activities, such as their tastes and preferences from online purchases they have made using a credit card, or from their web browsing history.'[282]

18.4 Accordingly, the current definition of personal information is sufficiently broad to capture inferred information about an identified or reasonably identifiable individual, meaning individuals currently have a right to seek access to this information under APP 12.

18.5 However, as noted in Part 2 of this submission, it is particularly important that the Privacy Act is clear in its application to inferred information given the risks that may arise from the handling of this type of information.

18.6 Accordingly, we support proposal 2.4, which will clarify that collection under the Privacy Act captures information obtained from any source, including inferred information. This should help to address concerns from some submitters to the Issues Paper that access to inferred information is not necessarily guaranteed under the Act.

Information about an organisation's source of personal information

18.7 We support proposal 18.1 that an organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

18.8 As noted in the Discussion Paper, requiring an organisation to provide information about the source of the personal information it has collected indirectly would enhance transparency in relation to third party collections of personal information, and the sharing of personal information between organisations.[283]

18.9 Proposal 18.1 is also necessary to support other proposed reforms, including proposal 16.4 to repeal APP 7. Currently, under APP 7.6 an individual may request an organisation that uses or discloses personal information about that individual for the purposes of direct marketing to provide its source of the information. Proposal 18.1 will ensure the existing protections of APP 7 are preserved if proposal 16.4 to repeal APP 7 is adopted.

18.10 Proposal 18.1 would also provide individuals with greater control over their personal information by assisting them to exercise proposed new privacy rights including the right to object (see Part 14 of this submission) and the right to erasure (see Part 15 of this submission).

18.11 Specifically, where personal information has been collected by an organisation from another source, the requirement for that organisation to identify the source of the information would enable individuals to contact those entities to object to the use and disclosure of their personal

---

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

[282] OAIC, *What is personal information?*, OAIC website, 5 May 2017, accessed 24 November 2021.

[283] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 141.

information, to seek erasure or to exercise their existing rights of access and correction under APPs 12 and 13 respectively.

Recommendation 68 – Adopt proposal 18.1 that an organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

Exceptions to access

18.12 APP 12.3 sets out several grounds on which APP entities may refuse a request for access to personal information. This includes where, inter alia, giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations.

18.13 The Discussion Paper indicates that submitters to the Issues Paper were concerned that the exception in APP 12.3(e) is not broad enough to cover the internal deliberative documents of an EDR scheme for the duration of the dispute resolution process, potentially undermining the integrity of an EDR scheme.[284]

18.14 We note the intention of proposal 18.2 is to prevent individuals who are engaged in the EDR process from accessing internal working or deliberative documents of an EDR scheme while the dispute resolution in in progress. This recognises that allowing access to such documents could provide an unfair benefit to the requesting individual.

18.15 Accordingly, we support proposal 18.2 to introduce an additional ground on which an organisation may refuse a request for access to personal information in circumstances where the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.

Recommendation 69 – Adopt proposal 18.2 to introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:

- the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.

Dealing with requests for access

18.16 Under APP 12.4, an APP entity must give access to the personal information in the manner requested by the individual, if it is reasonable and practicable to do so.

[284] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 142.

18.17 APP 12.5 applies where an APP entity refuses to give access to personal information under APP 12 on a permitted ground or refuses to give access in the manner requested by the individual. In these circumstances, the entity must take reasonable steps to give access in a way that meets the needs of the entity and the individual.

18.18 Proposal 18.3 seeks to clarify the existing access request process in APP 12 to the effect that:

- an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such as a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature, and
- where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.

18.19 We note that the explanatory memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 provides that the requirement under APP 12.5 for an entity to take reasonable steps to give access in a way that meets the needs of the individual and the entity is intended to 'ensure that entities work with individuals to try to satisfy their request.'[285]

18.20 The OAIC's APP Guidelines set out several examples of alternative methods of access that may meet the needs of the entity and the individual, and may result in more personal information being provided to an individual:

- deleting personal information for which there is a ground for refusing access and giving the redacted version to the individual
- giving a summary of the requested personal information to the individual
- giving access to the requested personal information in an alternative format
- facilitating the inspection of a hard copy of the requested personal information and permitting the individual to take notes
- facilitating access to the requested personal information through a mutually agreed intermediary.[286]

18.21 Accordingly, we support proposal 18.3 to clarify that an APP entity may consult with an individual in relation to a request for access. We consider that clarifying the procedural elements of APP 12 as described in proposal 18.3 could assist entities with providing access in a way that meets the needs of both parties.

18.22 Further, we agree with the commentary in the Discussion Paper that the right of access could be enhanced by enabling individuals to request a general summary or explanation of the personal information held.

---

[285] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 87.

[286] OAIC, 'Chapter 12: APP 12 — Access to personal information', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 24 November 2021.

Recommendation 70 – Adopt proposal 18.3 to clarify the existing access request process in APP 12 to the effect that:

- an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature, and
- where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.

Correction and quality

18.23 The Discussion Paper is seeking feedback about whether an APP entity should be required to keep personal information that it has published online accurate, up-to-date and complete, and to correct it upon request – to the extent that the entity retains control of the personal information.

18.24 APP 13 only applies in relation to personal information that is 'held' by an APP entity. An APP entity 'holds' personal information where it has possession or control of a 'record', which is defined to expressly exclude generally available publications.[287]

18.25 A 'generally available publication' is defined as a magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public regardless of the form in which it is published and whether it is available on payment of a fee.

18.26 Consequently, if an entity collects personal information for inclusion in a generally available publication, such as a publishing the personal information online on a website, APP 13 will not apply. This means that individuals are generally precluded from seeking correction of personal information published online. This is also relevant in the context of the proposed right to erasure discussed in Part 15 of this submission.

18.27 In these circumstances, we recommend that APP 13 is amended to require an APP entity to keep personal information that it has published online accurate, up-to-date and complete, and to correct it upon request – to the extent that the entity retains control of the personal information. Combined with the proposed right of erasure, this will provide individuals with greater control over their personal information and mitigate the risk of harm that may arise from incorrect information being widely available online.

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

Recommendation 71 – Amend the Privacy Act to require APP entities to keep personal information that it has published online accurate, up-to-date and complete, and to correct it upon request – to the extent that the entity retains control of the personal information.

Part 19: Security and destruction of personal information

19.1 Amend APP 11.1 to state that 'reasonable steps' includes technological and organisational measures.

19.2 Include a list of factors that indicate what reasonable steps may be required.

19.3 Amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.

What is the best approach to providing greater clarity about security requirements for APP entities?

Security of personal information

19.1 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.

19.2 The principles-based framing of APP 11 enables APP 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.

19.3 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.

19.4 The OAIC has issued a suite of guidance to support regulated entities to comply with their obligations under APP 11. This includes the APP guidelines, *Guide to securing personal information*, *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988*, and data breach prevention strategies for organisations developed with the ACSC.[288]

19.5 As noted in our submission to the Issues Paper, 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.[289]

[288] These resources are available on the OAIC's website at www.oaic.gov.au.

[289] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, 11 December 2020, accessed 24 November 2021, p 47.

19.6 We note that many submitters to the Issues Paper were supportive of the current security requirements under APP 11.1.[290] However, the Discussion Paper proposes to amend APP 11.1 to:

- state that 'reasonable steps' includes technical and organisational measures (proposal 19.1)
- include a list of factors that indicate what reasonable steps may be required (proposal 19.2).

19.7 The aim of these proposals is to clarify what 'reasonable steps' may require in the context of APP 11. However, as discussed in Part 3 of this submission, we are concerned that proposals 19.2 and 19.2 to introduce greater prescription in APP 11 may result in inconsistency with the other APPs that are also centred around the 'reasonable steps' test. Further, we do not consider that this greater prescription will provide additional certainty to regulated entities.

19.8 We consider the preferable approach is to elevate the status of the OAIC's guidance generally through 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, as recommended in Part 3 of this submission. This would provide regulated entities with further certainty and clarity around the matters that they should consider in determining what reasonable steps are required to meet their obligations under APP 11.

19.9 The changes to the existing privacy regulatory model proposed in the Discussion Paper will likely result in an increased number of privacy determinations and consideration of privacy matters by the courts (see Part 24 (Enforcement) and Part 25 (A direct right of action) of this submission). Judicial decisions around the application of the APPs, including the factors that are relevant to determining what 'reasonable steps' are required in the circumstances, can be quickly reflected in the OAIC's guidance rather than requiring legislative amendment.

19.10 We acknowledge that there may be areas of the law or particular sectors that require further certainty or specificity, or that merit specific privacy protections. To this end, APP codes provide an effective mechanism to adapt and particularise the APPs where appropriate. For example, an APP code could be developed by the Commissioner to enhance security requirements to address specific threats, such as cyber intrusion, or to provide further specificity and particularisation in relation to specific industries or technologies. An APP code could be developed for a specific industry to provide greater clarity around the 'reasonable steps' that they should take to meet their security and destruction obligations under APP 11.

19.11 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
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures.

[290] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 144.

19.12 Proposal 3.1 in the Discussion Paper would provide the Commissioner with greater flexibility and discretion to develop APP codes, which would ensure that further specificity and certainty can be given where required, and emerging privacy risks can be quickly and efficiently addressed (this is discussed in further detail in Part 3 of this submission).

Recommendation 72 – Consider alternative solutions for meeting the objectives of proposals 19.1 and 19.2, including requiring entities to have regard to OAIC guidelines when carrying out their functions or activities and adopting proposal 3.1 to provide the Commissioner with greater flexibility and discretion to develop APP codes.

Destruction of personal information

19.13 Where an entity holds personal information it no longer needs for a purpose that is permitted under the APPs, it must ensure that it takes reasonable steps to destroy or de-identify the information (APP 11.2).

19.14 The requirement to take reasonable steps to destroy or de-identify does not apply if personal information is contained in a Commonwealth record, or if an Australian law or a court/tribunal order requires it to be retained.

19.15 Similar to APP 11.1, 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. However, the Discussion Paper cites evidence that many Australian organisations have poor retention and destruction practices.[291]

19.16 As noted in our submission to the Issues Paper, 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.[292]

19.17 Accordingly, we support proposal 19.3 to amend APP 11.2 so that APP entities must take *all* reasonable steps to destroy or anonymise personal information when it is no longer needed or required. This would strengthen the obligation on entities to take all possible steps to destroy or anonymise information, while preserving the flexibility for entities to tailor their approach to destruction and anonymisation based on their circumstances.

Recommendation 73 – Adopt proposal 19.3 to amend APP 11.2 to require APP entities to take all reasonable steps to destroy the information or ensure that the information is anonymised

[291] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 147.

[292] OAIC, *Guide to data analytics and the Australian Privacy Principles*, OAIC website, 21 March 2018, accessed 24 November 2020.

where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.

Part 20: Organisational accountability

20.1 Introduce further organisational accountability requirements into the Act, targeting measures where there is the greatest privacy risk:

- Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.

Would the proposed additional accountability requirement in relation to restricted practices encourage APP entities to adopt a privacy by design approach?

How might the requirement be framed to reduce the likelihood of APP entities adopting a compliance mentality to the requirement?

What assistance could be provided to APP entities to support them in meeting these accountability requirements?

20.1 As noted in our submission to the Issues Paper, organisational accountability is one of the critical elements needed to support effective privacy regulation in Australia over the next decade.[293] Globally, accountability is also recognised as a key building block for effective privacy regulation and management.[294]

20.2 In the present context, accountability 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. In a practical sense, this requires entities to implement internal privacy management processes that are commensurate with, and scalable to, the risks and threats associated with their personal information handling activities.[295]

20.3 Under the Privacy Act, 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 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
- have a clearly expressed and up to date APP privacy policy describing how they manage personal information (APP 1.3).

20.4 However, unlike other data protection regimes with accountability requirements, APP 1.2 does not prescribe specific measures or practical steps that entities must take to ensure compliance

[293] We consider that there are four key elements needed to support effective privacy regulation: global interoperability; enabling privacy self-management; organisational accountability; and a contemporary approach to regulation.

[294] Centre for Information Policy Leadership (CIPL),*What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework*, CIPL, May 2020, accessed 25 October 2021, p 35.

[295] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, 11 December 2020, accessed 25 October 2021, p 97.

with the APPs. To support entities to comply with their obligations under APP 1.2, the OAIC has produced a suite of non-binding resources, which are described further below.

20.5 We welcome the consideration of additional accountability requirements in the Discussion Paper, including option 1 of proposal 11.1 to require APP entities that engage in certain restricted practices to take reasonable steps to identify privacy risks and implement measures to mitigate those risks. This may require a formal PIA, depending on the level of risk.[296] However, we consider that accountability measures should not be limited to the conduct of PIAs for certain high privacy risk activities.[297]

20.6 Accordingly, we have made several recommendations in this Part designed to enhance the existing accountability requirements under the Act. We recommend that APP 1 is amended to expressly require APP entities to:

- implement a risk-based privacy management program
- implement a 'privacy by design' approach
- appoint a privacy officer or privacy officers
- provide the Commissioner, on request, with evidence of the steps taken to ensure compliance with the APPs and any registered APP code.

20.7 As discussed further below, we consider that these enhancements will provide greater clarity and certainty for entities by elevating the Commissioner's existing expectations and guidance about the steps they should take to meeting their ongoing compliance obligations under APP 1. This will ensure that entities have the appropriate actions and controls in place to demonstrate compliance with the privacy regulatory framework, and, in turn, increase community trust in personal information handling activities.

20.8 The enhanced organisational accountability recommendations outlined in this Part are also necessary to support other proposed reforms to Australia's privacy framework.

20.9 For example, we consider that the reforms to privacy self-management mechanisms outlined in Part 8 (Notice of collection of personal information) and Part 9 (Consent to collection, use and disclosure of personal information) of this submission should be complemented by appropriate organisational accountability obligations to raise the standard of data handling in Australia and ensure that the burden of privacy management does not fall solely on individuals.

20.10 We also support proposal 10.1 to amend APPs 3 and 6 to require that a collection, use or disclosure of personal information must be fair and reasonable in the circumstances. Requiring entities to act fairly and reasonably is about ensuring that entities consider the impact on individuals when handling their personal information. To enable that to happen, entities need to have the necessary structures, policies and procedures in place to properly identify and assess those impacts, which is where strong accountability measures are critical. Part 10 of this submission discusses the proposed fairness and reasonableness requirements in further detail.

---

[296] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 95.

[297] P Leonard, *Privacy Harms: A paper for the Office of the Australian Information Commissioner*, report to OAIC, Data Synergies, June 2020, p 61.

20.11 Enhanced accountability measures will also help entities to assess, identify and select the circumstances in which they will need to implement pro-privacy default settings as discussed in Part 12 of this submission.

20.12 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.[298]

Recommended enhancements to organisational accountability requirements

Risk-based privacy management program

20.13 As legally binding principles, the APPs provide entities with the flexibility to take a risk-based approach to compliance.

20.14 For example, under APP 3, an APP entity must only collect personal information that is reasonably necessary for, or, for agencies, directly related to, one or more of its functions or activities. In evaluating whether a collection of personal information is reasonably necessary for a particular function or activity, consideration should be given to whether any interference with privacy is proportionate to a legitimate aim sought.[299] Similarly, a number of the APPs require an APP entity to take 'reasonable steps', which also requires an evaluation of the facts and circumstances to determine what steps would be required to achieve compliance.[300]

20.15 To facilitate this assessment, entities need to have the internal structures and systems in place to assess the risks associated with their personal information handling activities and to implement measures to mitigate those risks. In this way, risk-based organisational accountability provides the foundation for complying with the APPs.[301]

20.16 Accordingly, we consider that a holistic, demonstrable and ongoing approach to accountability through a risk-based privacy management program is required to ensure entities have the internal structures and systems in place to effectively address current and emerging privacy risks and harms associated with personal information handling practices.

20.17 As noted above, while we support option 1 of proposal 11.1, we consider that additional accountability measures should not be limited to the conduct of PIAs for certain high privacy

---

[298] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, 11 December 2020, accessed 25 October 2021, p 97.

[299] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy)* (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021).

[300] This includes APP 1.2, APP 5.1, APP 8.1, APP 10, APP 11, APP 12.5 and APPs 13.1 and 13.2.

[301] The GDPR enables a similar flexible, risk-based approach to compliance based on key principles. For example, the legitimate interests legal basis for processing 'involves assessing the risks relating to the data processing activities and defining measures to mitigate these risks…' Accordingly, CIPL has stated that 'the legitimate interests legal basis relies on, and promotes, organisational accountability.' See CIPL, *How the "Legitimate Interests" Ground for Processing Enables Responsible Data Use and Innovation*, CIPL, July 2021, accessed 25 October 2021, p 8.

risk activities.[302] PIAs are an essential risk management tool and key to facilitating a privacy by design approach. However, PIAs are usually conducted in an episodic manner at the project or product level. A privacy management program provides a framework to enable regulated entities to identify, assess and mitigate privacy risks on an ongoing basis.[303]

20.18 In a report of its Accountability Mapping Project, the Centre for Information Policy Leadership (CIPL) identified several core accountability elements that are reflected in effective data privacy management programs: leadership and oversight, risk assessment, policies and procedures, transparency, training and awareness, monitoring and verification, response and enforcement.[304]

20.19 While a privacy management program will help to facilitate compliance with privacy obligations, it 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.[305] Entities with established internal processes are also better able to anticipate, adapt and respond to changing business circumstances and regulatory challenges.[306]

20.20 Further, it is relevant to note that the Commissioner considers the specific accountability measures that APP entities have put in place when undertaking enforcement activities. For example, recent privacy determinations have taken account of an organisation's cooperative engagement with us in the investigation process, the effectiveness of the organisation's accountability measures, and the steps taken to remediate and update practices, procedures and systems since the breach.[307]

20.21 Consequently, while the arrangements each entity has put in place will be considered on a case-by-case basis, the existence and ability to provide evidence to demonstrate effective organisational accountability measures and frameworks will be considered by the Commissioner as mitigating factors in enforcement actions and decisions.

20.22 In designing and implementing a risk-based privacy management program, entities are required to consider the risks associated with their personal information handling activities and their compliance policies and processes 'holistically and proportionally, and this should result

---

[302] P Leonard, *Privacy Harms: A paper for the Office of the Australian Information Commissioner*, report to the OAIC, Data Synergies, June 2020, p 61.

[303] P Leonard, *Privacy Harms: A paper for the Office of the Australian Information Commissioner*, report to the OAIC, Data Synergies, June 2020, p 44.

[304] CIPL, *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework*, CIPL, May 2020, accessed 25 October 2021.

[305] CIPL, *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework*, CIPL, May 2020, accessed 25 October 2021, p 7.

[306] P Leonard, *Privacy Harms: A paper for the Office of the Australian Information Commissioner*, report to OAIC, Data Synergies, June 2020, p 61.

[307] See *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy)* (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021); *Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V.* (Privacy) [2021] AICmr 34.

in a more coherent, comprehensive and systematic approach to accountability.'[308] In other words, entities have the flexibility to design and implement a privacy management program in a way that best suits their circumstances.

20.23 A legislated requirement for a regulated entity to implement a privacy management program also aligns with international regulatory developments.

20.24 For example, the UK Government published a consultation paper setting out proposed reforms to the UK's data protection framework.[309] Amongst other measures, the paper proposes to implement 'a more flexible and risk-based accountability framework which is based on privacy management programmes.'[310]

20.25 The paper notes that 'organisations would be required to implement a privacy management programme tailored to their processing activities and ensure data privacy management is embraced holistically rather than just a 'box-ticking' exercise.'[311] In its submission to the consultation paper, the UK ICO observed that 'this means that those organisations whose processing carries the highest risk to people should also have the more robust approaches to accountability.'[312]

20.26 Canada's *Freedom of Information and Protection of Privacy Amendment Act 2021* requires the head of a public body to develop a privacy management program for the public body.[313] Similarly, Canada's Bill C-11 would require every organisation to 'implement a privacy management program that includes the organisation's policies, practices and procedures put in place to fulfil its obligations under this Act…'[314]

20.27 Accordingly, we recommend that APP 1 is amended to introduce an express requirement for entities to implement a risk-based privacy management program. The risk-based approach would provide entities with the flexibility to implement a privacy management program that is commensurate with, and scalable to, the risks associated with their personal information handling activities.

20.28 This approach would address concerns raised by some submitters about the potential regulatory burden that could be imposed on entities from overly prescriptive regulation, while ensuring greater clarity and certainty for entities around the steps they must take to meet their obligations under APP 1.[315]

---

[308] UK Department for Digital, Culture, Media & Sport (DCMS), *Data: A new direction*, gov.uk website, 10 September 2021, accessed 25 October 2021, 55.

[309] The UK's current data protection framework consists of the *Data Protection Act 2018*, the UK General Data Protection Regulation (UK GDPR) and the *Privacy and Electronic Communications Regulations 2003*.

[310] DCMS, *Data: A new direction*, gov.uk website, 10 September 2021, accessed 25 October 2021, 54.

[311] DCMS, *Data: A new direction*, gov.uk website, 10 September 2021, accessed 25 October 2021, 54.

[312] UK ICO, *Response to DCMS consultation "Data: a new direction"* , UK ICO website, 6 October 2021, accessed 25 October 2021, p 39.

[313] *Freedom of Information and Protection of Privacy Amendment Act 2021,* s 36.2.

[314] See section 9 of Bill C-11 – *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*.

[315] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 152.

Privacy by design

20.29 '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. A privacy by design approach shifts the focus of an entity to preventing privacy-related issues, rather than simply complying with privacy laws.[316]

20.30 While the objects of the Privacy Act recognise that 'the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities', the APPs do not, of themselves, specifically encourage entities to consider ways to achieve their objectives that are less privacy intrusive.

20.31 We consider that an express requirement in APP 1 to implement a privacy by design approach, combined with the proposed requirement to handle personal information fairly and reasonably, will facilitate positive privacy outcomes by specifically requiring entities to consider how their activities will impact individuals and whether there are less privacy intrusive options for new projects, activities or initiatives.[317] We note that the majority of submissions that discussed organisational accountability supported the introduction of further accountability measures, including expressly requiring a privacy by design approach.

20.32 For clarity, we recommend that the explanatory memorandum that will accompany the amending Bill notes that conducting PIAs, where appropriate, is central to facilitating a privacy by design approach.

Privacy officers

20.33 The objective of enhancing the accountability of APP entities for their personal information handling practices is similarly supported by the requirement to designate a suitable individual, or individuals, as privacy officer for the entity.

20.34 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.

20.35 As noted in the Discussion Paper, requirements that entities appoint a privacy or data protection officer (DPO) are in place under other international privacy regimes including the GDPR, as well as in the UK, New Zealand and Canada.

20.36 The requirement to appoint a privacy officer or privacy officers would enable the entity to determine the appropriate skills, qualifications and scope of the role, taking into account the risks associated with the entity's personal information handling activities.

---

[316] Information and Privacy Commission New South Wales (IPC NSW), *Fact sheet – Privacy by design*, IPC NSW website, May 2020, accessed 9 December 2021.

[317] S Ghali, 'Organisational accountability key to protecting privacy', *Precedent – Journal of the Australian Lawyers Alliance (ALA)*, October 2021, 166. For more information about the ALA, see: www.lawyersalliance.com.au.

20.37 In this way, our recommendation can be distinguished from the specific requirements that must be met under the GDPR when appointing a DPO, which include that a DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level. While these measures may still be appropriate for large APP entities that handle large volumes of personal information, our recommendation would provide entities with the flexibility to assess the most appropriate way of assigning responsibility for privacy compliance.

20.38 A requirement to appoint a privacy officer is necessary to support the other enhanced accountability requirements outlined in this Part, including implementing a privacy management program and a privacy by design approach.

Demonstrating compliance

20.39 Effective accountability also requires that entities are able to demonstrate the existence and effectiveness of privacy management programs internally (for example, to senior management) and externally (for example, to regulators, individuals and shareholders).[318]

20.40 We consider that APP 1 should be amended to include an express requirement that an APP entity must provide evidence, on request from the Commissioner, of the steps taken to ensure compliance with the APPs and any registered APP code.

20.41 This express requirement will ensure the OAIC is able to verify that entities are complying with their privacy obligations where appropriate. For instance, the Commissioner may require an entity to provide evidence of the policies, practices and procedures that are included in its privacy management program or evidence to demonstrate how it has implemented privacy by design approach.

20.42 Another example may be where the Commissioner requests an entity involved in certain 'high privacy risk' activities, such as the use of location data on a large scale, to provide evidence of the steps taken to meet their compliance obligations.

20.43 A requirement to provide evidence of the steps taken to comply with the APPs and any registered APP code will also necessarily require entities to document their controls and activities, which adds accountability to the process.[319] As noted above, while the arrangements each entity has put in place will be considered on a case-by-case basis, the existence and ability to provide evidence to demonstrate effective organisational accountability measures and frameworks will be considered by the Commissioner as mitigating factors in enforcement actions and decisions.

---

[318] CIPL, *What Good and Effective Data Privacy Accountability Looks Like: Mapping Organisations' Practices to the CIPL Accountability Framework*, CIPL, May 2020, accessed 25 October 2021, p 6.

[319] D Solove, and P.M. Schwartz, 'ALI Data Privacy: Overview and Black Letter Text', *UCLA Law Review*, 2020, 68:27 as cited in P Leonard, *Privacy Harms: A paper for the Office of the Australian Information Commissioner*, report to OAIC, Data Synergies, June 2021, p 47.

Supporting entities to meet enhanced accountability requirements

20.44 The OAIC has published a suite of guidance materials to assist entities to embed strong accountability measures including:

- a privacy management framework
- a privacy management plan template for organisations and agencies
- a guide to undertaking PIAs
- a PIA tool
- a PIA e-learning course
- a privacy officer toolkit.

20.45 The OAIC is therefore well placed to assist APP entities to meet their enhanced accountability obligations, as recommended above.

Recommendation 74 – Amend APP 1 to expressly require APP entities to:

- implement a risk-based privacy management program
- implement a 'privacy by design' approach
- appoint a privacy officer or privacy officers
- provide the Commissioner, on request, with evidence of the steps taken to ensure compliance with the APPs and any registered APP code.

Recommendation 75 – Include a note in the explanatory memorandum that will accompany the amending Bill that PIAs are central to facilitating a 'privacy by design' approach.

Accountability in relation to 'purpose'

20.46 Proposal 20.1 is to amend APP 6 to expressly require APP entities to determine, at or before the use or disclosure of personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.

20.47 The exercise of determining the purposes for which an entity may use and disclose personal information is an essential first step and threshold issue that must be considered before an APP entity collects personal information, not at the point at which the entity seeks to use or disclose it for a particular purpose.

20.48 Accordingly, we recommend that APP 3, rather than APP 6, is amended to expressly require entities to determine, at or before the time of collection, each of the known specific purposes for which the information is to be collected, used or disclosed and to record those purposes. If

an entity sought to use or disclose personal information for a new purpose, it would need to record that new purpose before undertaking the use or disclosure.

20.49 Amending APP 3 would also strengthen fundamental data protection concepts of purpose limitation and data minimisation that are given effect in APP 3.1 and 3.2, which require entities to only collect personal information if it is reasonably necessary for, or, for agencies, directly related to, one or more of the entity's functions or activities. A requirement for entities to consider and document each of the specific purposes for which the information will be collected, used or disclosed will help to inform consideration of whether each item of personal information is 'reasonably necessary' for an entity's functions and activities.

20.50 It will also ensure entities have a clear and specific purpose in mind for the subsequent handling of the information. This is critical to facilitate how information may be used and disclosed under APP 6. As discussed in Part 10 of this submission, requiring that purposes are specific under APP 3 will also help to address issues that arise under APP 6 in relation to overly broad or vague primary purposes.

20.51 Requiring entities under APP 3 to record the known specific purposes for which is collects, uses and discloses personal information will also assist entities to formulate and document the information they must provide to individuals through their APP 1 privacy policy and APP 5 notices. There is a strong connection between transparency and purpose specification. When the specified purpose is clear and transparently notified, individuals have greater control over their information and the protections provided by the APPs can be fully effective. However, this exercise is intended to function as an internal accountability and governance measure, rather than a replication of the transparency requirements contained in APP 1 and APP 5.

20.52 Our recommended amendment to APP 3 would also ensure that entities consider the purposes of collecting the information earlier and not just in the context of the notification requirements in APP 5, which promotes a privacy by design approach to privacy compliance.

Recommendation 76 – Amend APP 3 to expressly require entities to determine, at or before the time of collection, each of the known specific purposes for which the information is to be collected, used or disclosed and to record those purposes.

Part 21: Controllers and processors of personal information

Are there any other advantages or disadvantages of introducing these concepts in the Act?

If limitations in the Act's coverage makes full adoption of these concepts impractical, would partial adoption be beneficial? If yes, how could this occur without being overly complex?

If adopted, what obligations under the Act should processors have (record keeping, security, NDB etc.)?

21.1 A key strength of the Privacy Act is that it is principles-based. It sets out general rules that can be applied to a range of situations across the economy based on the risks posed by specific entities or personal information handling practices. The flexibility of the framework means that it will often impose different standards of conduct depending on the particular circumstances of an APP entity. For example, the notice requirements under APP 5 are subject to a reasonableness test which may mean that entities do not need to notify in some circumstances, such as where an individual has already been notified of the relevant matters.

21.2 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. In this submission, we have recommended the introduction of new measures, and the enhancement of existing mechanisms such as the Commissioner's code-making power, which will introduce additional specificity into the law where appropriate.

21.3 Our recommendation in Part 3 of this submission to require entities to have regard to OAIC guidelines when carrying out their functions or activities will provide further clarity about the interpretation of the APPs. The Discussion Paper's proposed changes to the OAIC's powers, structure and funding, as well as the introduction of a direct right of action, will facilitate increased decision making and enforcement actions in the courts that would be reflected in OAIC guidance.

21.4 Introducing the controller/processor distinction into the Privacy Act may help to clarify application of the APPs and ensure that responsibility between the parties is clearly allocated based on the actual control over the handling of personal information. However, these potential benefits need to be weighed against the potential increase in complexity that the controller/processor distinction may add to the privacy framework.

21.5 These concepts may clarify the application of the APPs where the scope of the controller/processor distinction is clear. However, we understand that the actual operation of these principles under the GDPR has not always been simple, particularly where there are complex data handling arrangements. Similarly, determining the scope of the relationship between the controller and processor may create complexities for the OAIC in regulating the scheme, particularly if the Commissioner is required to assess the obligations of sophisticated entities with complicated data handling contractual arrangements.

21.6 Additionally, the Discussion Paper notes the potential gaps this would create if the small business exemption is maintained. The Discussion Paper suggests that these gaps could be resolve if the controller/processor distinction only applied where both parties are APP entities. We consider that partially introducing this framework would only increase this complexity and uncertainty in the Privacy Act. For example, parties to a transaction may not be in a position to assess whether its counterparties are APP entities.

21.7 Any benefits that may accrue from introducing this framework should be considered against the potential complexities that this regime may impose, as well as the possible difficulties for the regulator in enforcing the Privacy Act.

21.8 If the controller/processor distinction is introduced into the Act, we recommend that processors continue to be subject to organisational accountability obligations under APP 1 and security requirements under APP 11, at a minimum. This reflects the importance of having appropriate technical and operational documents, processes and controls around the handling of any personal information that an APP entity holds, even if the entity is a processor.

21.9 We also recommend requiring contracts between controllers and processors to contain certain mandatory terms.

21.10 Section 95B of the Privacy Act currently contains requirements for Commonwealth contracts between agencies and contracted service providers.[320] This provision ensures that the contracted service provider complies with the APPs as if it were an agency in respect of its activities under the contract.[321] Requirements around data sharing agreements for the sharing of Government data have also been included in the proposed Data Availability and Transparency scheme.[322]

21.11 A similar framework could be created for contracts between controllers and processors modelled on Article 28 of the GDPR. These mandatory contractual requirements could ensure that data sharing agreements require counterparties to embed good privacy practices, including appropriate processes, technical controls and de-identification and deletion practices. Equally, controllers should be required to only engage with processors where the controller reasonably believes that the processor has appropriate technical and organisational capabilities to comply with their obligations under the Privacy Act.

21.12 Mandatory contracting terms could also be used to introduce clear obligations about the assessment and subsequent notification of data breaches. For example, these terms could reflect GDPR requirements for a processor to notify a controller where it becomes aware of an eligible data breach, while the controller remains responsible for notifying individuals and the regulator.

[320] A Commonwealth contract is defined in s 6 as a contract, to which the Commonwealth or an agency is or was a party, under which services are to be, or were to be, provided to an agency.

[321] OAIC, 'Chapter A: Introductory Matters', *Australian Privacy Principles guidelines*, oaic.gov.au, 22 July 2019, accessed 3 October 2021.

[322] Data Availability and Transparency Bill 2020, s 18 and 19.

Recommendation 77 – Consider whether the potential benefits of a controller/processor regime would be outweighed by increases to complexity in compliance and regulation.

Recommendation 78 – If the controller/processor distinction is introduced into the Act:

- require that processors are subject to organisational accountability obligations under APP 1 and security requirements under APP 11, at a minimum
- introduce requirements for certain mandatory terms in contracts between controllers and processors, modelled on Article 28 of the GDPR.

Part 22: Overseas data flows

22.1: Introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

22.2: SCCs for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

22.3: Remove the informed consent exception in APP 8.2(b).

22.4: Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in entity's up-to-date APP privacy policy required to be kept under APP 1.3.

22.5: Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines.

22.6: Amend the Act to clarify what circumstances are relevant to determining what are 'reasonable steps' for the purpose of APP 8.1

Would the other exceptions to APP 8.2, together with proposals such as creating a list of prescribed countries and binding schemes and introducing standard contractual clauses facilitate overseas disclosures of personal information in the absence of the informed consent exception?

22.1 Data increasingly flows across borders as the digital economy develops.[323] It is important for privacy regulation to create appropriate and interoperable frameworks that enable the efficient movement of data across borders while providing strong protections for individual's personal information.[324] Getting these settings right is essential to creating trusted overseas data flows.[325]

22.2 A key way to achieve this is to ensure Australia's Privacy Act is interoperable with global privacy laws. This will facilitate safe and efficient disclosure of personal information from overseas entities to entities based in Australia. This does not necessarily mean adopting other laws but instead considering how to create consistently high privacy standards globally. Many of the OAIC's recommendations in this submission are directed towards achieving these high privacy standards. For example, removing the small business and employee records exemptions would align the protections for personal information held by small business and employers in Australia with those offered overseas.

[323] See United Nations Conference on Trade and Development (UNCTAD), Digital economy report 2021, UNCTAD, 2021, accessed 7 December 2021, pp 18-19, 51.

[324] One of the objectives of the Privacy Act is 'to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected'. See *Privacy Act 1988* (Cth) s 2A(f).

[325] 92% of Australians are concerned about their data being sent overseas. Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to OAIC, September 2020, accessed 6 December 2021, p 67.

22.3 It is also important for the Privacy Act to facilitate the flow of information out of Australia in a way that ensures the privacy of individuals is protected. As explained in the Discussion Paper, APP 8 and s 16C of the Act create a framework for the disclosure of personal information overseas. The Discussion Paper proposes several mechanisms to better protect individuals and support APP entities in disclosing information overseas. These proposals are considered below.

Prescribing countries and certification schemes under APP 8.2(a)

22.4 We support proposal 22.1 to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

22.5 As set out in our submission to the Issues Paper, Australian organisations currently make this assessment based on their own due diligence. This proposal would help to provide confidence to APP entities that they can disclose personal information overseas and to individuals that their privacy will be protected.

22.6 In developing a whitelist, it will be important to maintain high standards for what is considered 'substantially similar to' the APPs so that individuals can trust data flows to countries on the whitelist.

22.7 It will also be important to carefully consider whether the enforcement mechanism in the overseas jurisdiction is accessible and has effective powers to enforce the privacy or data protections in the law or binding scheme. The OAIC's APP guidelines include factors that will be relevant to whether these requirements are satisfied.[326]

22.8 The Discussion Paper suggests that enforcement mechanisms could include reciprocal arrangements between the OAIC and equivalent overseas regulators, or clear dispute resolution processes for certification schemes. The OAIC has strong working relationships with global data protection regulators. Some of these relationships have been formalised through memorandums of understanding (MOU) with our international counterparts, including the UK ICO, the Data Protection Commissioner of Ireland and the Personal Data Protection Commission of Singapore.[327] These MOUs include provisions to cooperate with respect to the enforcement of privacy laws, which can serve as a foundation for reciprocal agreements.

22.9 If proposal 22.1 is adopted, the legislation should also clearly state whether APP entities are able to make the assessment in APP 8.2(a) independently of the government list. This will promote clarity in the scope of APP 8.2(a).

---

[326] OAIC, 'Chapter 8: APP 8 — Cross-border disclosure of personal information', *Australian Privacy Principles guidelines*, OAIC website, 22 July 2019, accessed 3 October 2021, [8.21]-[8.26].

[327] OAIC and UK ICO, *Memorandum of understanding between the Information Commissioner for the United Kingdom of Great Britain & Northern Ireland and the Office of the Australian Information Commissioner for cooperation in the regulation of laws protecting personal data*, OAIC and UK ICO, 28 January 2020, accessed 6 December 2021; OAIC and DPCI, *MOU with DPCI — mutual assistance in the enforcement of laws protection personal information in the private sector*, OAIC and DPCI, n.d., accessed 6 December 2021; OAIC and PDPC, *Memorandum of understanding between the Office of the Australian Information Commissioner and the Personal Data Protection Commission of the Republic of Singapore on cooperation in Personal Data Protection*, OAIC and PDPC, 20 March 2020, accessed 6 December 2021.

22.10 While proposal 22.1 may assist APP entities to some extent, it will be important to retain existing overseas disclosure mechanisms in APP 8, including the accountability approach. The experience of the EU Commission in creating adequacy lists shows that this process can involve long and costly negotiations. To date, only 14 countries have received an Adequacy Decision from the EU Commission. As demonstrated in *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems* (Schrems II), these must be constantly monitored to ensure the receiving country's framework remains adequate.[328]

Responsibility for prescribing countries and certification schemes

22.11 Careful consideration should be given to the appropriate body to prescribe countries and certification schemes. Schrems II highlighted important considerations when making adequacy decisions, such as the need to consider the broader legal framework in the other country.[329] As such, the government body assessing adequacy will need the relevant expertise in foreign laws and resourcing to undertake this analysis.

22.12 In addition, the body should be separate from the regulator. This is consistent with the approach taken in other jurisdictions. In New Zealand, a Minister recommends the Governor-General makes regulations prescribing a country as providing comparable safeguards.[330] The Governor-General makes these regulations on the recommendation of the responsible Minister, who consults with the Privacy Commissioner.[331] In Europe, the EU Commission makes adequacy decisions. This process involves the EU Commission developing a proposal, seeking an opinion from the European Data Protection Board (EDPB) and obtaining approval from representatives of EU countries before adopting a decision.[332] In Australia, it may be most appropriate for the assessment to be carried out by the policy arm of the Department reporting to the Minister who creates a whitelist.

22.13 Although the body should be separate, it may be appropriate for the body to consult with the Information Commissioner when assessing a country or certification scheme under APP 8.2(a).

Recommendation 79 – Adopt proposal 22.1 to introduce a mechanism for Government to prescribe countries and certification schemes under APP 8.2(a).

[328] European Commission, *Adequacy decisions*, European Commission website, n.d., accessed 6 December 2021; *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems* (Court of Justice of the European Union, C-311/18, ECLI:EU:C:2020:559, 16 July 2020).

[329] In this decision the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield because the ability of US public authorities to access personal data were not sufficiently limited or subject to effective redress mechanisms. For more detail see OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, p 112.

[330] *Privacy Act 2020* (NZ) s 214.

[331] *Privacy Act 2020* (NZ) s 214.

[332] European Commission, *Adequacy decisions*, European Commission website, n.d., accessed 6 December 2021.

Standard contractual clauses

22.14 We support proposal 22.2 to make Standard Contractual Clauses (SCCs) for transferring personal information overseas available to APP entities to facilitate overseas disclosures of personal information. We consider this is most appropriate as a support to the accountability approach rather than an exception to APP 8.1.

22.15 SCCs are a globally accepted mechanism to facilitate overseas data flows. In the EU, SCCs have been used for several years and the EU Commission has recently published new SCCs.[333] In New Zealand, the Office of the Privacy Commissioner has developed model contract clauses, which can be used to show that the overseas recipient is required to protect the information that is comparable to the safeguards in the New Zealand Privacy Act.[334]

22.16 The OAIC's APP guidelines on overseas disclosure of personal information recognise contractual arrangements as a key mechanism to ensure an overseas recipient will handle an individual's personal information in accordance with the APPs.[335] These guidelines should be used as a reference for what should be considered in the SCCs.

22.17 Overseas experiences in developing and using SCCs can also be instructive for developing SCCs in Australia. The SCCs in both the EU and NZ promote flexibility to meet the needs of the contracting parties, provided the changes do not override the contractual provisions that promote adequate standards of protection for personal information overseas.[336] A similar approach could be beneficial in Australia.

22.18 While SCCs can serve as a valuable tool, it will be important for APP entities to remember that SCCs should not be adopted without regard to other considerations. As was highlighted by the decision of the Court of Justice of the European Union in Schrems II, it is important for entities to satisfy themselves that the receiving entity is able to comply with the SCCs in a way that provides meaningful equivalent protection.[337]

22.19 SCCs are most effective as a tool to support compliance with APP 8.1 rather than a mechanism to facilitate overseas data flows in their own right. This will promote public confidence in overseas data flows, as APP entities still must ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs and remain accountable if the overseas recipient mishandles the information. This is consistent with approaches in the EU and New Zealand. In these jurisdictions, SCCs are a way of showing that appropriate or comparable safeguards are provided, but do not replace the disclosing entity's obligation to

---

[333] *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* [2021] OJ L 199/31.

[334] Office of the Privacy Commissioner (NZ), *Model clause agreement builder*, Office of the Privacy Commissioner website, n.d., accessed 6 December 2021.

[335] OAIC, 'Chapter 8: APP 8 — Cross-border disclosure of personal information', *Australian Privacy Principles guidelines*, OAIC website, 22 July 2019, accessed 3 October 2021 [8.16].

[336] *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* [2021] OJ L 199/31, p 1; Charles Mabbett, *Model contractual clauses for sending personal information overseas*, Office of the Privacy Commissioner (NZ), 19 November 2020, accessed 7 December 2021.

[337] See *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems* (Court of Justice of the European Union, C-311/18, ECLI:EU:C:2020:559, 16 July 2020).

ensure that the SCCs are indeed appropriate or provide comparable protection to domestic privacy legislation.[338]

Recommendation 80 – Adopt proposal 22.2 to make SCCs for transferring personal information overseas available to APP entities. The SCCs should support the requirement to take reasonable steps in APP 8.1.

Consent

22.20 The Discussion Paper sets out concerns raised in submissions to the Issues Paper about the burden that APP 8.2(b) places on individuals. Expecting individuals to understand and consent to complex overseas data flows may be impracticable, which limits the value of consent. We therefore support proposal 22.3 to remove the informed consent exception in APP 8.2(b).

22.21 While there may be scenarios in which consent is used by business to facilitate overseas data flows (for example, this exception may be relied on in the overseas travel and tourism industry), we consider that consent should not overrule the accountability protections in APP 8.1.

Recommendation 81 – Adopt proposal 22.3 to remove the informed consent exception in APP 8.2(b).

Transparency of overseas disclosures

22.22 We support proposal 22.4 for an APP entity's privacy policy to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas.

22.23 Where an APP entity is likely to disclose personal information to overseas recipients, APP 1 currently requires entities to set out the countries in which the recipients are likely to be located, if practicable.[339] This information is also required in an APP 5 notice.[340]

22.24 The proposal will increase the circumstances in which APP entities are required to list the countries where personal information is disclosed to in their privacy policies, as it lowers the threshold from when personal information 'is likely to be disclosed' to when 'it may be disclosed' and removes consideration of what is practicable. Given the level of concern

[338] GDPR art 46(1); *Privacy Act 2020* (NZ) s 22 Information privacy principle 12(1)(c). Also see *Data Protection Commissioner v Facebook Ireland LTD, Maximillian Schrems* (Court of Justice of the European Union, C-311/18, ECLI:EU:C:2020:559, 16 July 2020); *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* [2021] OJ L 199/31 [18]–[22].

[339] *Privacy Act 1988* (Cth) sch 1 APP 1.4(g).

[340] *Privacy Act 1988* (Cth) sch 1 APP 1.5(j).

individuals have about the disclosure of their personal information overseas this increased transparency is important.

22.25 There is a risk that this requirement could result in long lists of countries being included in privacy policies and overloading the individual with information. The OAIC's APP guidelines suggest measures that can be used to assist readability where personal information is disclosed to numerous overseas locations, such as including the countries in an appendix to the privacy policy.[341] The OAIC will closely monitor the impact this amendment has on privacy policies and provide guidance to entities about how to implement these changes in a way that will be meaningful for individuals.

Recommendation 82 – Adopt proposal 22.4 to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in an entity's up-to-date APP privacy policy required to be kept under APP 1.3.

Clarifying APP 8

Defining disclosure

22.26 We support proposal 22.5 to introduce a definition of 'disclosure' that is consistent with the current definition in the OAIC's APP guidelines. We understand the proposal is intended to provide certainty regarding whether APP 8 applies to cloud service providers.[342]

22.27 The APP guidelines state that an APP entity 'discloses' personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.[343] This definition means that an entity 'uses' personal information when it handles and manages another entity's access to that information within the entity's effective control. The APP guidelines set out circumstances where the provision of personal information to a cloud service provider may be a use rather than a disclosure.[344]

---

[341] OAIC, 'Chapter 1: APP 1 — Open and transparent management of personal information', *Australian Privacy Principles guidelines*, OAIC website, 22 July 2019, accessed 3 October 2021, [1.32].

[342] AMA, *Privacy Act Review: AMA submission to the Attorney General's Department – the Review of the Privacy Act 1988, a response to the Issues Paper*, AMA, December 2020, accessed 24 November 2021, pp 10-11; Avant Mutual, *Avant submission on the Privacy Act Review Issues Paper*, 27 November 2020, accessed 17 November 2021, p 14; Communications Alliance, *Communications Alliance submission to the Attorney General's Department on the Privacy Act Review Issues Paper*, Communications Alliance, 29 November 2020, accessed 7 December 2021, p 12; Optus, *Submission in response to the Attorney-General's Department Issues Paper Privacy Act Review*, Optus, November 2020, accessed 16 June 2021, p 12.

[343] OAIC, 'Chapter B: Key concepts', *Australian Privacy Principles guidelines*, OAIC website, 22 July 2019, accessed 3 October 2021 [B.64].

[344] OAIC, 'Chapter 8: APP 8 — Cross-border disclosure of personal information', *Australian Privacy Principles guidelines*, OAIC website, 22 July 2019, accessed 3 October 2021, [8.14].

22.28 The OAIC notes that there are different interpretations of disclosure in various legal contexts and so it may be useful to include the definition of disclosure from the APP guidelines in legislation.[345] This will create consistency and ensure that the current operation of the law in relation to cloud service providers is preserved.

Recommendation 83 – Adopt proposal 22.5 to introduce a definition of 'disclosure' that is consistent with the current definition in the APP guidelines.

Clarifying what circumstances are relevant to 'reasonable steps' for the purposes of APP 8.1

22.29 Proposal 22.6 suggest that APP 8 should be amended to include greater legislative guidance about the circumstances that are relevant to determining what reasonable steps are for the purpose of APP 8.1. This would have the effect of elevating matters from the APP guidelines into the Privacy Act. The aim of this proposal is to assist entities in understanding what their obligations are before disclosing personal information overseas.

22.30 This proposal appears to primarily respond to concerns raised in submissions to the Issues Paper about the measures that cloud service providers are required to put in place under APP 8 to protect personal information.[346] This suggests that some of the uncertainty about the standard required by APP 8.1 arises in specific contexts. Legislating general factors that are relevant to determining 'reasonable steps' for the purposes of APP 8.1 may not provide the clarity that APP entities are seeking in relation to this issue.

22.31 As set out in Part 3, we consider that the aim of this proposal and the concerns of submitters can be more broadly addressed by elevating the status of the OAIC's guidance, 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.[347] This would provide regulated entities with further certainty and clarity around the matters they should consider to meet their compliance obligations under all the APPs, including APP 8.

---

[345] For example, disclosure for the purposes of continuous disclosure obligations under the *Corporations Act 2001* (Cth) by unlisted entities may entail lodging documents with ASIC or publishing information on a website – see ASIC, *RG 198 Unlisted disclosing entities: Continuous disclosure obligations*, ASIC, 18 June 2009, accessed 7 December 2021. In insurance, disclosure refers to the duty upon both parties to a contract of insurance to reveal in the negotiations leading up to the formation or renewal of the contract, all facts of which they are aware and which are material to the proposed insurance, but does not require the insured to disclose facts that the insurer knows or is presumed to know or are common knowledge – *Carter v Boehm* (1766) 97 ER 1162; *Dalgety and Co Ltd v Australian Mutual Provident Society* [1908] VLR 481.

[346] Information Technology Industry Council, *Submission to Australian Public Consultation on the Review of the Privacy Act 1998*, Information Technology Industry Council, 25 November 2020, accessed 17 November 2021, p 3; Avant Mutual, *Avant submission on the Privacy Act Review Issues Paper*, 27 November 2020, accessed 17 November 2021, p 14; Optus, *Submission in response to the Attorney-General's Department Issues Paper Privacy Act Review*, Optus, November 2020, accessed 16 June 2021, p 12; KPMG Australia, *Review of the Privacy Act 1988 (Cth) — Submission to the Attorney-General's Department Issues Paper*, KPMG Australia, December 2020, accessed 16 June 2021, p 18.

[347] See recommendation 16 from OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021.

22.32 As explained in Part 3 of this submission, we consider that the proposal to introduce greater prescription in relation to APP 8 may result in inconsistency with the other APPs that are also centred around the 'reasonable steps' test.

22.33 Commissioner-issued guidelines could be more easily amended to take account of developments in technology or personal information handling practices in the context of cloud service providers, and can quickly reflect any judicial interpretation of APP 8.

Recommendation 84 – Consider alternative solutions for meeting the objectives of proposal 22.6, including requiring entities to have regard to OAIC guidelines when carrying out their functions or activities.

Part 23: Cross-Border Privacy Rules and domestic certification

Cross-Border Privacy Rules

23.1 Continue to progress implementation of the CBPR system.

23.2 Introduce a voluntary domestic privacy certification scheme that is based on, and works alongside CBPR.

What benefits would CBPR certification have for Australian businesses?

Would there be a benefit in the CBPR system being expanded beyond APEC to include countries beyond the APEC region?

Would Australian businesses (both APP entities and businesses not covered by the Act) be interested in obtaining CBPR certification on a fee for service basis? That is, paying annual certification fees to an Accountability Agent?

What organisations may be suitable to be accredited as an Accountability Agent?

What organisations may be suitable to develop or assist with developing a CBPR code?

Would Australian businesses (both APP entities and businesses not covered by the Act) be interested in obtaining domestic certification scheme based on the requirements of the Act, alongside CBPR certification?

Would Australian businesses be more interested in pursuing domestic certification, CBPR certification or both?

How could the certification process be streamlined for businesses interested in pursuing both forms of certification?

23.1 The Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (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. The CBPR system has not yet been implemented in Australia through the appointment of an Accountability Agent.

23.2 We support proposal 23.1 to progress implementation of the CBPR system in Australia. One possible method of implementing the CBPR system is through an APP code. APP codes are able to impose additional requirements provided they are not contrary to or inconsistent with any of the APPs. To facilitate this, we recommend that a gap analysis between the CBPR and the Privacy Act is carried out, particularly following any changes to the Privacy Act arising out of the Review. This important preliminary step will determine whether an APP code is an appropriate

mechanism to implement the CBPR, and if so, what additional requirements should be included.

23.3 If the CBPR system is implemented through an APP code, a code developer will need to draft the code. As set out in our submission to the Issues Paper, it would be difficult to identify an appropriate code developer that represents the broad range of entities that could be covered by the code. Instead, it could be appropriate for the OAIC to lead the development of this code. Given its regulatory and guidance functions, the OAIC is experienced in consulting across diverse industries and stakeholder groups.[348]

23.4 Regardless of how the CBPR system is implemented, it will be important for the OAIC to have the ability to handle complaints and take enforcement action as the Privacy Enforcement Authority for the CBPR in Australia.

Recommendation 85 – Adopt proposal 23.1 to progress implementation of the CBPR system, with the preliminary step of conducting a gap analysis between the CBPR and the Privacy Act.

Domestic certification

23.5 We support proposal 23.2 to introduce a voluntary domestic privacy certification scheme drawing on best practice in other certification schemes. As noted in our submission to the Issues Paper, a domestic privacy certification scheme could increase the transparency of organisations' data practices by enabling Australians to quickly assess the level of data protection offered by APP entities. A certification scheme could also play a role in facilitating overseas transfers of personal information and assist in ensuring that regulated entities are meeting their obligations under the Privacy Act without the need to substantially increase regulatory action.

23.6 Certification criteria forms an integral part of ensuring trust in any certification mechanism. As noted in our submission to the Issues Paper, we consider that certification criteria should maintain and build on the protections and obligations set out in the Privacy Act, reflect community expectations of privacy and follow the EDPB's Certification Guidelines. To ensure a uniform standard, the OAIC should have a role in approving and publishing a single set of certification criteria to be used by certification agents when certifying businesses.

23.7 We consider that businesses should be able to seek enterprise-wide certification or certification in relation to specific products, data types of business processes. This will ensure that the domestic privacy certification scheme can respond to the particular needs of individual entities.

23.8 The Discussion Paper sets out a model in which the OAIC would develop criteria and use these criteria to accredit private sector organisations as certification agents. Certification agents would then assess businesses for certification. As set out in our submission to the Issues Paper,

[348] As noted in the Discussion Paper, proposal 3.1, if implemented, would amend the code-making power to allow the Commissioner to develop an APP code on the direction of the Attorney-General where a suitable industry representative cannot be identified.

we consider it is preferable for the OAIC to remain independent from the certification process. Instead, we consider it is more appropriate for an independent third party to accredit certification agents. We recommend that the OAIC's involvement in certification is limited to setting the accreditation criteria for certification bodies to meet and the certification criteria for entities wishing to be certified. This is similar to the approach in the CBPR system and the UK, which both involve a body independent from the regulator approving entities that issue certification. Appointing an independent body to accredit certification agents could also provide an opportunity to leverage the experience of government bodies administering other accreditation schemes.

23.9 The Discussion Paper also proposes that the OAIC would be the only body to receive complaints under the certification scheme. While it will be important for the OAIC to be able to regulate breaches of the Privacy Act by certified entities, we consider the certified entities and certification agents should handle complaints in relation to certification requirements. The Review should consider what mechanisms should be included in the certification scheme to manage complaints about an act or practice that breaches the certification scheme and is an interference with privacy under the Privacy Act. For example, certification agents could be required to provide the individual with information about how to make a complaint to the OAIC, or to refer matters to the OAIC directly.

23.10 As noted in the Discussion Paper, a trusted certification model will need to address concerns about potential conflicts of interest. We support re-accreditation requirements and audits to address these issues. The Review should also consider other mechanisms used in certification schemes that promote transparency, such as providing reports to the OAIC of the reasons certification has been granted or revoked.[349]

Recommendation 86 – Adopt proposal 23.2 to introduce a voluntary domestic privacy certification scheme in a way that draws on best practice and works alongside other certification schemes, including the CBPR.

Recommendation 87 – Ensure that the voluntary domestic privacy certification scheme:

- is flexible and enables an entity to seek enterprise-wide certification for all of its operations, or certification for specific products, data types or business processes
- enables the OAIC to develop and publish accreditation requirements for certification bodies and certification criteria for the scheme
- ensures 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.

[349] See GDPR Article 43(5).

Part 24: Enforcement

Civil penalties

24.1 Create tiers of civil penalty provisions to give OAIC more options so they can better target regulatory responses including:

- A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy.

- A series of new low level and clearly defined breaches of certain APPs with an attached infringement notice regime

24.2 Clarify what is a 'serious' or 'repeated' interference with privacy.

24.1 Businesses and government are collecting and holding an increasing amount of data in our modern economy, which is only likely to increase as the digital economy grows. While this will have benefits, we have also seen high-profile misuses of personal information around the world. The Australian community increasingly expects the OAIC to take a more enforcement-focused approach in the face of growing privacy risks.

24.2 Regulating in this environment requires a modern civil penalty regime that provides a credible deterrent against interferences with privacy and ensures that the consequences of mishandling personal information cannot be treated as a cost of doing business. It must also be flexible and responsive to enable the Commissioner to seek penalties from the court that are proportionate to the situation or conduct concerned. Penalties must be appropriate, having regard to the nature of the APP entity, which may be anything from a small health provider to a large multinational corporation.

24.3 We welcome proposal 24.1 to reconsider the civil penalty framework under the Privacy Act. As set out below, we recommend adopting a modified version of proposal 24.1, involving a flexible civil penalty framework supported by a broad infringement notice regime. However, we have also set out observations on how the tiered approach in proposal 24.1 could be implemented under the Privacy Act, should this model be progressed through the Review.

Creating a simpler civil penalty regime

24.4 There are several regulatory options available to the Commissioner in the event of a privacy breach. These include the orders available under the determinations power, the ability to accept enforceable undertakings or to seek injunctions.[350] Financial consequences for misconduct are only available in limited circumstances where the conduct meets a 'serious' or 'repeated' threshold or, as recognised in the Discussion Paper, in limited instances where the Commissioner makes a compensation order. The Commissioner exercises these powers in accordance with the OAIC's Privacy regulatory action policy, which includes consideration of the specific and general educational, deterrent or precedential value of the particular privacy

[350] Privacy Act, ss 52, 80V and 80W

regulatory action.[351] We take a transparent, consistent and proportionate approach to enforcement, similar to comparable domestic and international regulators.[352]

24.5 We strongly support the Discussion Paper's proposal to introduce a civil penalty for interferences with privacy under s 13 of the Privacy Act, which would address this limitation on our ability to seek pecuniary penalties. However, for simplicity, rather than a tiered approach, we recommend creating a single civil penalty under s 13 of the Privacy Act with a maximum fine commensurate with the increased penalties proposed in the Online Privacy Bill.[353] We consider that this will create a more effective civil penalty framework under the Privacy Act.

24.6 Section 13G imposes unnecessary thresholds that the OAIC must demonstrate before orders for civil penalties can be made by the courts. The seriousness of conduct and whether it was repeated are important, however these factors are more appropriate considerations after breach has been established when the Federal Court determines civil penalties using well-established legal principles. The nature and extent of any contravention is also explicitly required for consideration under s 82(6) of the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) (Regulatory Powers Act) when determining pecuniary penalties. Requiring the Commissioner to adduce evidence of these matters to demonstrate a breach of s 13G creates unnecessary duplication which may not be an efficient use of public resources.

24.7 Introducing a civil penalty for interferences with privacy and removing s 13G would provide the Commissioner with a broader discretion to identify the most appropriate regulatory outcome for each enforcement action within a simpler civil penalty regime. This discretion would be exercised transparently, consistently and proportionately in line with our Regulatory action policy and Guide to privacy regulatory action.[354] These policies provide guidance to entities on the factors that inform the Commissioner's discretion when selecting the most appropriate power in the circumstances and will underpin the OAIC's use of any new civil penalty provisions. The Commissioner's choice of powers is also subject to the practical limitations of any regulator, particularly the need to carefully spend public resources to ensure the greatest benefit for the Australian community.

24.8 Facilitating a more flexible approach to privacy enforcement will also have economy-wide benefits. Increasing the Commissioner's ability to seek actions in the Federal Court will have a

---

[351] OAIC, '*Privacy regulatory action policy*', OAIC website, May 2018, accessed on 8 November 2021, [38]

[352] See for example:

- Chapters on Compliance and enforcement strategy and Priority factors, ACCC *Compliance & enforcement policy & priorities*, ACCC website, n.d., accessed on 11 November 2020
- ACCC, *Infringement Notices: Guideline on the use of infringement notices by the Australian Competition and Consumer Commission*, ACCC website, July 2020, p. 3-5
- Discussion of infringement notices and how ASIC decides which enforcement tools to use in ASIC, *Information Sheet 151: ASIC's approach to enforcement*, ASIC website, n.d., p. 4-9
- Compliance and enforcement approach in ACMA, *Compliance and enforcement policy*, ACMA website, n.d., accessed on 11 November 2020
- ACMA, *Regulatory guide No. 5 – Infringement Notices*, ACMA website, 2019, p. 3-4
- UK ICO, *Regulatory Action Policy*, UK ICO website, n.d., accessed on 8 November 2021.

[353] Exposure draft, OP Bill, Schedule 2, Item 5

[354] OAIC, '*Privacy regulatory action policy*', OAIC website, May 2018, accessed on 8 November 2021; OAIC, '*Guide to privacy regulatory action*', OAIC, June 2020, accessed on 8 November 2021

significant educative effect, providing useful case law that will clarify the practical operation of the Privacy Act. It will also help to build greater community confidence that personal information is being protected in the digital economy. This confidence is integral to individuals' trust in the information handling practices of APP entities.

24.9 This would bring the Privacy Act in line with comparable domestic and international regulators. For example, the ACCC and the Australian Securities and Investments Commission (ASIC) both have several civil penalty provisions that are subject to significant civil penalties where the nature and extent of a contravention are only considered when assessing the amount of a pecuniary penalty.[355] In both cases, these regulators have discretion to identify the most appropriate enforcement action in accordance with their respective regulatory action policies.[356]

24.10 The UK ICO has the power to issue penalty notices for failures to comply with various provisions of the UK GDPR, including breaches of the processing principles and failures to comply with the rights of a data subject.[357] The UK ICO Regulatory Action Policy sets out its objectives for regulatory action 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.[358]

24.11 We therefore recommend s 13G of the Privacy Act is repealed and a single civil penalty provision for any interference with privacy is introduced to create a simpler civil penalty framework. The maximum penalty for this single provision should be equal to that being proposed for s 13G in the Online Privacy Bill to ensure that the OAIC's civil penalty provisions are commensurate with that of the ACCC and act as a sufficient deterrent.[359] This should be supported by a broad infringement notice power in relation to any interference with privacy (considered in more detail below).

24.12 If the Review considers that factors are necessary to guide the Commissioner's discretion on when to seek civil penalties, we suggest that these could be modelled on our existing Regulatory action policy.[360]

---

[355] This includes several provisions in the Australian Consumer Law (ACL), notably the unconscionable conduct requirement at s 20, prohibition of false and misleading representations at s 29 and the misleading conduct and representations provisions at s 33, 34 and 37. Pursuant to s 224 (2) and (3A) of the ACL, these sections are subject to significant pecuniary penalties. When assessing the scope of these penalties, the court must have regard to all relevant matters, including the nature and extent of the act or omission.

Similarly, under the Corporations Act, directors and officers have several duties under Chapter 2D including to exercise a degree of care and diligence and to act in good faith. Under s 1317E and 1317G, a court can order that a person pay a civil penalty if it breaches a relevant civil penalty provision.

[356] See for example chapters on compliance and enforcement strategy and priority factors in ACCC, *Compliance & enforcement policy & priorities,* ACCC website, n.d., accessed on 8 November 2021; ASIC, *Information Sheet 151: ASIC's approach to enforcement*, ASIC website, n.d., accessed on 8 November 2021, p. 4-9.

[357] See *Data Protection Act 2018* (UK), s 149 and s 155

[358] UK ICO, *Regulatory Action Policy*, UK ICO website, n.d., accessed 8 November 2021, 6-7 and 10-13

[359] See Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (Cth) sch 2 item 5.

[360] OAIC, '*Privacy regulatory action policy',* OAIC website, May 2018, accessed on 8 November 2021, [38]

A broader infringement notice regime

24.13 The simplified civil penalty regime recommended above will help to facilitate the OAIC's shift to a more strategic privacy regulator, as expected by the community.

24.14 However, regulators will only ever be able to pursue limited numbers of cases due to the time and resource investment required to bring these matters through to the Federal Court. In our submission to the Issues Paper, the OAIC recommended the introduction of an infringement notice regime for any interference with privacy, set at an appropriate and proportionate penalty unit amount.[361] A tiered approach to penalty amounts, commensurate with the infringement notice framework of the ACCC, would ensure that each notice has an appropriate deterrent effect.

24.15 An infringement notice regime will be an important regulatory tool that will support a broader civil penalty framework by allowing the Commissioner to appropriately tailor their regulatory response to a wider range of circumstances.

24.16 An appropriate infringement notice framework is particularly important in the Privacy Act given the wide variety of entities regulated under this regime. Ensuring compliance across the Australian economy means that we cannot only focus on the most serious offences by the largest players. A tailored infringement notice framework will allow the Commissioner to provide a timely, cost-efficient outcome for interferences with privacy. This will be particularly useful when managing medium to low-level matters where a pecuniary penalty is appropriate as a deterrent measure and the factual and legal issues are relatively clear.

24.17 We are concerned that the tier 4 infringement notices proposed at 24.1 will not perform this function sufficiently. While these notices will be useful at the lowest level of breaches, the proposed scope excludes privacy breaches that would benefit from timely and cost-efficient enforcement.

24.18 In addition to the requirements under the OAIC's Regulatory action policy that guide the Commissioner's discretion when selecting an appropriate enforcement tool, a broader infringement notice power would be subject to several practical limitations. In particular, the decision to issue this notice would only be made at the end of an investigation where the Commissioner has formed the view that the conduct in question is an interference with the privacy of an individual. If a recipient refuses to pay the notice, the Commissioner will be required to pursue a court-based resolution. In practice, this means that the Commissioner will only issue infringement notices where a matter has sufficient merits to be enforced in the Federal Court.

24.19 Introducing a broader infringement notice power for any interference with privacy will also bring the OAIC's powers in line with comparable regulators that have found considerable success with a broader infringement notice regime in their respective frameworks.

24.20 For example, the ACCC has described the success of infringement notices. Since their introduction in 2010, the majority of matters that had been resolved by way of an infringement

[361] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, December 2020, accessed 8 November 2021, Recommendation 50

notice involved some form of alleged false or misleading misrepresentation.[362] This reflects the fact that the ACCC's infringement notice power is available for a wide variety of civil penalty provisions, not simply administrative failures. The OAIC and the ACCC deal with similar issues and have an economy-wide regulatory scope. Given these similarities, the consumer regulator's powers have often been used as a model for the OAIC and we suggest that this infringement notice power would be similarly useful for the Commissioner.

24.21 We therefore recommend that an infringement notice regime is attached to the new civil penalty for interferences with privacy of an individual.

Recommendation 88 – Adopt a modified version of proposal 24.1 that:

- introduces a single civil penalty under s 13 with a maximum fine commensurate with the increased penalties proposed in schedule 2 of the exposure draft of the OP Bill.
- repeals s 13G
- introduces a broader infringement notice power for any interference with privacy containing a tiered approach to penalty amounts, commensurate with the infringement notice framework of the ACCC.

Comments on the proposed creation of a tiered model of civil penalty provisions

24.22 If the above recommendation is not adopted, we suggest proposal 24.1 for the creation of tiers of civil penalty provisions is subject to the modifications discussed below.

24.23 It is crucial that the maximum civil penalty set for an interference with privacy is sufficiently high. If s 13G is retained, the increased penalties for this provision in the Online Privacy Bill will apply only to the most significant privacy breaches. The civil penalty unit for interferences with privacy will still need to be large enough to have a real deterrent effect on moderate or even large breaches that may not reach the s 13G threshold. The policy objective of proposal 24.1 may not be achieved if the penalty unit threshold for interferences with privacy is set too low.

Clarifying section 13G

24.24 As stated above, we recommend repealing s 13G of the Privacy Act. In our view, this provision imposes legal concepts of seriousness and repeated conduct that distract from the proper focus on whether the Privacy Act itself has been breached. These concepts are more appropriately addressed after a breach has been established when determining pecuniary penalties.

[362] ACCC, *ALRC Corporate Criminal Responsibility Review – Submission on Discussion Paper*, ALRC website, January 2020, accessed on 8 November 2021

24.25 If this recommendation is not adopted, we support proposal 24.2 in principle, which aims to clarify what is a 'serious' or 'repeated' interference with privacy.

24.26 Section 13G imposes civil penalties where an entity 'does an act, or engages in a practice, that is a serious interference with the privacy of an individual' or 'repeatedly does an act, or engages in a practice, that is an interference with the privacy of one or more individuals.' A serious interference with privacy and a repeated interference with privacy are two distinct concepts, either of which may lead the OAIC to seek a civil penalty against an entity.

24.27 In order to clarify the application of s 13G, we recommend removing the 'repeated' threshold. In our view, a repeated act or practice that interferes with the privacy of individuals would fall within the natural meaning of a 'serious' privacy incident, rather than existing as a separate legal construct. Repealing the 'repeated' threshold would mean that a 'serious' incident will capture, amongst other things, repeated acts or practices that interfere with privacy as well as a single act or practice that interferes with the privacy of individuals repeatedly. This change would also avoid unnecessary arguments about whether actions of an APP entity over time amount to serious or repeated interferences with privacy.

24.28 As suggested in proposal 24.2, additional guidance on what is a 'serious' interference with privacy could then be introduced into the legislation to provide further clarity. The OAIC's Guide to privacy regulatory action sets out several factors that are relevant when considering whether a particular interference with privacy is serious that may be relevant for inclusion in legislation.[363]

24.29 The legislation could also make clear that whether an act or practice is repeated and the cumulative impact of acts or practices may both be relevant to whether there is a serious interference with privacy. It should also clarify that s 13G may potentially capture:

- Breaches affecting a large number of individuals without affecting any one individual seriously. The Discussion Paper highlights that this is a useful matter to consider to ensure that s 13G applies to incidents where people individually suffer serious consequences because of a breach, as well as widespread incidents that have significant impacts on privacy even where the individual privacy impacts are low.
- Incidents that create an increased risk of harm to a large group of individuals, even if actual harm suffered to any specific individual cannot yet be established. This risk-based approach to assessing the consequences of incidents is particularly important in a privacy context where the harms stemming from a breach of the Privacy Act may not be immediately apparent or may be difficult to attribute to any particular incident.
- The extent to which the entity responsible for the incident or conduct has been the subject of prior privacy regulatory action by the OAIC, and the outcome of that action. This will ensure that an entity's prior regulatory history can be taken into account when determining breaches of s 13G, for example if the entity failed to comply with an administrative warning from the OAIC or has a pattern of privacy misconduct.

[363] OAIC, '*Chapter 6: Civil penalties — serious or repeated interference with privacy and other penalty provisions*', *Guide to privacy regulatory action*, oaic.gov.au, June 2020, accessed 8 November 2021

24.30 The suggestions above will clarify the interpretation of the 'serious' threshold in a privacy context for the OAIC, APP entities and the courts.

OAIC powers: investigations, assessments and inquiries

24.3 Make the civil penalty provisions in the Act subject to investigation under Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act) in addition to the IC's current investigation powers.

24.4 Amend the Privacy Act to provide the Commissioner the power to undertake public inquiries and reviews into specified matters

Would each of the enhanced regulatory powers described above assist the OAIC to be a more proactive regulator and encourage better levels of compliance with the Act?

Investigations

24.31 We support proposal 24.3 to provide the Commissioner with search and seizure powers and the ability to prevent the destruction of evidence. Having the right information gathering tools is essential to effectively develop a case in a way that meets evidentiary requirements and ensures successful regulatory outcomes. This will also bring our powers into line with comparable regulators.

24.32 The Privacy Act should have an appropriate framework of civil penalties to ensure that the Commissioner can be confident that their powers under Part 3 of the Regulatory Powers Act are available when investigating incidents. Under the current framework, civil penalties are only available for breaches of the APPs that constitute a serious or repeated interference with privacy. The OAIC's above recommendation to create a civil penalty provision for any interference with privacy should address this issue.

Assessments

24.33 The Commissioner's power to undertake proactive assessments of APP entities is an important function that provides a professional, independent and systematic appraisal of how well an agency or organisation (or discrete part of an agency/organisation) complies with all or part of its privacy obligations.[364] The OAIC approaches assessments as an educative process, intended to drive best practice compliance. Significant issues of concern that are identified as part of an assessment may result in a Commissioner-initiated investigation (CII), if the target entity does not appear willing or capable of taking steps to address these concerns.

24.34 We welcome the new information gathering powers for assessments in the Online Privacy Bill. While the majority of assessments are undertaken with the consent of the target entity, this

[364] OAIC, *Privacy assessment powers*, OAIC website, n.d., accessed 10 November 2021.

power will ensure that the Commissioner can conduct this program efficiently by ensuring that target entities co-operate with our assessments.

24.35 We recommend that these new powers are enhanced by providing that the Commissioner's assessment power is conducted pursuant to the monitoring power under Part 2 of the Regulatory Powers Act. The OAIC currently has the power to enter premises with a warrant, however this only allows us to inspect relevant documents. This recommended change will empower the OAIC to search and seize evidence, where appropriate. This will also ensure that the Commissioner's powers to investigate as part of an assessment, complaint and CII are consistent.

Public inquiries and reviews

24.36 We support proposal 24.4 to provide the Commissioner with the power to undertake public inquiries and reviews as directed by or subject to Ministerial approval.

24.37 Recent public inquiries by comparable regulators have demonstrated the importance of these reviews as effective intelligence gathering measures that can lead to regulatory action or policy changes. This power will enhance the Commissioner's ability to take a more strategic, targeted approach to privacy regulation by closely reviewing relevant sectors where the OAIC believes regulatory action may have a significant impact on the protection and handling of personal information.

Recommendation 89 – Adopt proposal 24.3 to make civil penalty provisions in the Privacy Act subject to investigation under Part 3 of the Regulatory Powers Act in addition to the Commissioner's current investigation powers.

Recommendation 90 – Make assessments under the Privacy Act subject to monitoring under Part 2 of the Regulatory Powers Act in addition to the Commissioner's current assessment powers.

Recommendation 91 – Adopt proposal 24.4 to allow the Commissioner to undertake public inquiries and reviews into specified matters.

Determinations

24.5 Amend paragraph 52(1)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:

- a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals

Is the proposal to allow the OAIC to require an entity to take reasonable steps to prevent future loss occurring reasonable?

24.38 We support proposal 24.5 as an appropriate response for certain types of matters where there may be a reasonable and widely understood risk of loss occurring, particularly after a data breach.

Recommendation 92 – Adopt proposal 24.5 to amend paragraph 52(1)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss.

Range of available Federal Court orders in a civil penalty proceeding

24.6 Give the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established.

Is it necessary and appropriate to give the Federal Court the express power to make any orders it sees fit or should the amendment just enable the Federal Court to make compensation orders in addition to an order imposing a pecuniary penalty?

24.39 We support proposal 24.6 to give the Federal Court the express power to make any orders it sees fit. Allowing the Court to make the same orders as the Commissioner under s 52 will promote clarity and certainty for APP entities and allow the Commissioner to pursue, and the Federal Court to order, tailored remedies that are more appropriate for a particular matter. This reflects the fact that for some breaches of the Privacy Act, even more serious contraventions, a mixture of civil penalties and conduct orders may be the most effective response.

24.40 Similarly, giving the Federal Court the ability to make compensation orders for breaches of civil penalty provisions in addition to pecuniary penalties will promote efficiency for the courts, which will not have to hear subsequent private actions. It will also promote access to justice for individuals who may have reduced court expenses when seeking compensation where the Commissioner has brought civil penalties.

Recommendation 93 – Adopt proposal 24.6 to give the Federal Court the express power to make any orders it sees fit.

Industry funding arrangement

24.7 Introduce an industry funding model similar to ASIC's incorporating two different levies:

1. A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and

2. A statutory levy to fund the OAIC's and investigation and prosecution of high risk entities and industries.

Which of the OAIC's costs should be cost recoverable if a cost recovery levy were adopted?

What are the high privacy risk industries where it would be most appropriate for entities to bear the costs of the OAIC investigating complaints and undertaking enforcement action in the courts

24.41 Our submission to the Issues Paper noted the need for the OAIC to be appropriately funded to effectively carry out its statutory functions and to use the full suite of regulatory powers, including enforcement through the courts, which can be costly and resource intensive. This was echoed in many other submissions to the Issues Paper. We support consideration of ways in which this can be achieved, particularly in light of proposals in the Discussion Paper that would enable us to shift our regulatory posture to become a more strategic and proactive regulator.

24.42 A more enforcement-oriented approach will require the Commissioner to take on more complex investigations and enforcement, aimed at addressing systemic privacy issues associated with new and emerging data-driven business models, often by large and well-resourced multinational corporations. These activities will occur in addition to our existing policy and educative functions and any residual complaint handling functions. This will not only incur potentially expensive court costs, but also require the OAIC to have appropriate technology, systems and people capabilities to handle these matters effectively. This includes legal and document management resources and staff with relevant technical skills. The recent Productivity Commission Information Paper on Regulatory Technology highlighted the potential for regulators to use technology, data collection and analysis to increase internal efficiencies, improve regulatory effectiveness and support regulatory compliance.[365]

24.43 We support consideration of an industry funding model. We suggest that the following issues are considered in the development of such a model:

- Appropriate and effective designation of entities is important to the success of a levy model. The suggested language of 'high risk' entities and industries may not recognise that privacy-invasive activities that require monitoring and regulation can come from all over the economy. It is important that the levy is designed in a way that does not imply

[365] Productivity Commission, *Information Paper: Regulatory Technology*, Productivity Commission website, October 2020, accessed on 12 November 2021, p. 6 & 9.

that sectors that are not subject to the levy do not require the same levels of compliance or regulatory oversight.

- Any industry funding model would need to be designed to preserve the OAIC's regulatory independence and enable the OAIC to direct its resources to priority areas as needed. If particular sectors are identified to pay a levy, it is likely that supplementary budget appropriation would be required to resource OAIC functions and activities not funded by the levy.
- Arrangements for the administration of a levy would need to be considered.

Recommendation 94 – Adopt proposal 24.7 to introduce an industry funding model for the OAIC that is supported by appropriate supplementary budget appropriations for functions and activities not funded by a levy.

Annual reporting requirements

24.8 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground

Would amending the OAIC's annual reporting requirements to require more specific figures assist with transparency for complainants?

24.44 Government-held information is a national resource that should be managed for public purposes. As the regulator of the FOI Act, the OAIC encourages the proactive release of government information and believes that increased scrutiny and participation in government processes promotes better decision-making. Through our Annual Report and website, the OAIC publishes detailed information about our activities, including our complaint handling function. This includes the number of complaints received about each APP, the main remedies agreed in conciliated privacy complaints and amounts of compensation.[366]

24.45 We support proposal 24.8 to provide additional information about complaints, including the numbers dismissed under each ground in s 41 of the Privacy Act. This information has been included in past annual reports.[367] We note that the extent this helps to provide greater clarity around how the Act is being interpreted and applied may be limited. One reason for this is that complaints are often dismissed on multiple grounds and every matter is based on different facts and circumstances.

[366] OAIC, *Annual Report 2020-2021*, OAIC website, 21 October 2021, accessed on 12 November 2021, Appendix D; OAIC, *Privacy complaint outcomes*, OAIC website, n.d., accessed on 12 November 2021

[367] OAIC, *Annual Report 2014-2015*, OAIC website, 2015, accessed on 12 November 2021, Chapter 6

Recommendation 95 – Adopt proposal 24.8 to amend the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.

Regulatory Model

24.9 Alternative regulatory models

- Option 1 - Encourage greater recognition and use of EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them.

- Option 2 - Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes.

- Option 3 - Establish a Deputy Information Commissioner – Enforcement within the OAIC.

Which option would most improve the complaints handling process for complainants and allow the OAIC to focus on more strategic enforcement of the Act?

Are there other options that could achieve this outcome that should be considered?

24.46 The OAIC's core purpose is to promote and uphold privacy rights in Australia. The OAIC seeks to achieve this purpose in many important ways, including promoting awareness of privacy law, educating the community about privacy issues, issuing guidance to assist entities to interpret the Privacy Act, conducting proactive compliance assessments, handling complaints and, where appropriate, taking enforcement action.

24.47 In undertaking these activities, we seek to use our resources in a way that secures the greatest benefit for Australians and the regulated community.

24.48 In our submission to the Issues Paper, we suggested that our ability to achieve this core purpose should be enhanced by enabling the OAIC to take a more targeted approach to priority areas where the OAIC believes privacy regulatory action will have a significant impact on the protection and handling of personal information. We welcome the Discussion Paper's consideration of options to change the current regulatory framework to enable the OAIC to shift to a more strategic, proactive regulator.

24.49 The following considerations are key to achieving this shift in regulatory posture:

- The Commissioner should have the flexibility to utilise their full range of regulatory functions and powers in a pragmatic and proportionate way. The Commissioner should

be empowered to take a risk-based approach to regulation to manage emerging risks and pursue breaches of privacy in the digital environment.[368]

- The Commissioner should be provided with the regulatory tools and resources to enable them to take a more enforcement-focused approach to regulation, as expected by the community.
- There must be an effective pathway for individuals to seek redress in a proportionate and cost-effective way that provides the maximum benefit to the individual and the community.

24.50 We also acknowledge comments from submitters to the Issues Paper about the dual role of the OAIC as conciliator and regulator, and the impacts this may have on public confidence in undertaking these two functions.

24.51 We recommend that elements of each of the options in proposal 24.9 are adopted to facilitate this shift in regulatory posture, subject to the considerations outlined below. Facilitating a greater use of EDR schemes and creating additional senior executive leadership within the OAIC solely focused on privacy enforcement are valuable proposals, which will enhance the existing framework. An independent FPO housed within the OAIC could also be created to signal a shift in the OAIC's regulatory focus to more systemic privacy issues.

24.52 In order to be effective, this new regulatory model will need to be supported by other amendments to the Privacy Act proposed in the Discussion Paper and recommended by the OAIC. These are discussed in more detail below, along with key considerations that should be addressed when taking forward each of the options in proposal 24.9.

Option 1 – Increased use of EDR schemes

24.53 The Privacy Act creates a framework for the Commissioner to recognise external dispute resolution schemes (EDR schemes) to assist in complaint handling.

24.54 Recognised EDR scheme play an important role in the current privacy complaints-handling framework. They can be particularly effective in circumstances where their specialist industry knowledge and ability to address the full range of issues in a complaint can be leveraged to handle complaints in a holistic way. Using EDR schemes can also drive consistent approaches to handling complaints and enhance privacy knowledge at an industry-specific level.

24.55 There is merit in considering the increased use of EDR schemes in the privacy framework. This could provide a well-understood and cost-effective pathway for individuals. An example of this model working effectively is in relation to credit reporting complaints, where membership of an EDR scheme is a requirement that has been built into Part IIIA of the Privacy Act.

24.56 We support in principle the second part of this proposal to require entities to pay a fee for service to the OAIC where a complaint is made against them and they are not part of a recognised EDR scheme. This option has the potential to not only address the resource burden

[368] For more details, see Sparrow, M. (2008). *The Character of Harms: Operational Challenges in Control*. Cambridge: Cambridge University Press.

of handling all complaints but may also encourage APP entities to resolve matters internally before a complaint is made to the OAIC.

24.57 There are several issues that may need to be addressed before this proposal can be implemented in practice.

24.58 Nine EDR schemes are currently recognised to handle complaints under the Privacy Act. For these EDR schemes to take a more prominent role in handling privacy complaints, the structure and funding arrangements for these entities may need to be considered, to ensure that they can handle these complaints appropriately and in line with their respective terms of reference.

24.59 Broad coverage of EDR schemes across the economy would also be required to ensure that APP entities can sign up to an appropriate provider in each industry. The Review provides an opportunity to identify additional EDR schemes in different industries. This could be particularly effective to assist in handling complaints in high volume areas such as health and education sectors. It may even be appropriate to create new EDR schemes where there is no existing coverage, such as to handle complaints about online services, particularly under the proposed OP code.[369]

24.60 Recognised EDR schemes need to be supported by OAIC guidance and training to ensure that complaints are handled consistently and effectively. This is particularly important when recognising new EDR schemes to ensure they have the appropriate resources and knowledge in handling privacy complaints. The OAIC would need to be appropriately resourced to continue to effectively support and oversee an increased use of EDR schemes.

24.61 It will also be necessary to consider how the Commissioner's existing grounds to refuse to investigate complaints will interact with an increased use of EDR schemes. In our submission to the Issues Paper, we recommended that s 41(dc) of the Privacy Act is expanded to allow the Commissioner to decide not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme. This recommendation will become essential if more complaints are handled by EDR schemes.

Option 2 – Create a federal privacy ombudsman

24.62 We suggest that the Review consider whether the benefits of creating a federal privacy ombudsman (FPO) outweigh the potential regulatory complexity that this may introduce into the privacy framework.

24.63 Establishing a FPO may send a strong signal about the OAIC's shift to a regulator focused on addressing systemic privacy issues in the economy. However, there are a number of considerations that should be taken into account in developing this option further. The key issue in facilitating the OAIC's shift to this different type of regulator is not the requirement to handle complaints, which are an important part of the privacy framework. Rather, it is the resource-intensive nature of this function in its current model. This submission makes recommendations about changes to the current complaints-handling framework in the Privacy Act that would assist to address this issue (see below).

[369] Recommendation 23 of the Final Report into the ACCC's Digital Platforms Inquiry recommended the establishment of an ombudsman to resolve complaints and disputes with digital platform providers.

24.64 Other considerations in relation to the creation of an FPO include the need for:

- a high level of engagement between the OAIC and the FPO to ensure that consistent approaches are taken to interpreting the APPs and other key terms.
- the establishment of effective information sharing procedures to ensure that the Commissioner is able to use the intelligence gained from privacy complaint handling to help guide their strategic enforcement work
- the retention of a clear and effective pathway for individuals to seek redress. Creating this new body may result in individuals having to navigate multiple bodies to resolve their complaint, potentially including EDR schemes, the FPO, the OAIC, the courts and the Administrative Appeals Tribunal.

24.65 This proposal may create efficiencies for Government if it is implemented as part of a broader shift in the complaints-handling frameworks across different regulators and jurisdictions. However, we suggest that in isolation, this change may create complexities that outweigh efficiencies.

24.66 If this proposal is adopted, these considerations may be addressed by establishing the FPO as an independent body within the OAIC. A model for this is the Australian Energy Regulator (AER), which is housed within the ACCC but is governed by an independent board. This body would have a separate management structure and staff to the OAIC but could be included in the same budget appropriation, share the OAIC's corporate functions and be accountable to the Commissioner for its governance and efficient management of resources.

24.67 Establishing an independent FPO within the OAIC sends a strong signal about the changing regulatory posture of the OAIC while reducing the resource costs in establishing and maintaining a new agency. The independence of the FPO could address submitters' concerns around the Commissioner's dual conciliatory and regulatory roles, while supporting appropriate information sharing and consistent application of privacy law. This in turn would help ensure a clear, effective pathway for individuals in resolving privacy disputes without adding a separate body to this framework.

24.68 Complaints-handling functions would need to continue to be appropriately resourced wherever they sit, as would the functions that remain with the OAIC as a strategically-focused regulator.

Option 3 – Establish a Deputy Information Commissioner – Enforcement

24.69 We support the proposal to establish a Deputy Information Commissioner – Enforcement within the OAIC. This additional executive capability dedicated to enforcement would play a valuable role as the OAIC transitions to a more strategic regulator with enhanced enforcement powers. Establishing this new executive role would assist in addressing the issues that this regulatory shift is attempting to resolve when combined with other changes to the existing regulatory structure.

Additional changes required to support a new regulatory model

24.70 The Discussion Paper highlights the place of the complaint-handling function in the overall privacy framework. This function plays an important role of deterring inappropriate acts or

practices and providing individuals with a mechanism for redress. This also serves as a source of intelligence for the OAIC on emerging privacy issues.

24.71 However, the Discussion Paper also acknowledges that the requirement for the OAIC to investigate all complaints is very resource intensive. We regularly see circumstances where the resources dedicated to handling a complaint are disproportionate to the result achieved. Directing resources to complaint-handling impacts on our ability to undertake other activities that may be more likely to address systemic privacy issues and have a wider benefit to the community.

24.72 Regardless of whether the complaints-handling functions remain with the Commissioner or are transferred to a new FPO, adjustments are needed to address the resource intensive nature of the current complaint model. To achieve greater flexibility and efficiencies in resolving complaints, we reiterate recommendations 48, 49 and 53 from our submission to the Issues Paper.

24.73 The creation of a direct right of action will work alongside these recommended changes to provide individuals with effective and cost-efficient pathways to resolving their privacy complaints. While there will be costs associated with a direct right of action, these may be limited if matters can be brought subject to a 'small claims procedure' in the Federal Circuit Court (FCC), as noted in Part 25 of the Discussion Paper and recommended in this submission. The potential for a direct right of action will also incentivise APP entities to cooperate in conciliations or risk a more costly hearing and findings against them.

24.74 A number of other OAIC recommendations and proposals in the Discussion Paper will need to be adopted to give full effect to the proposed new regulatory model. For example, the creation of a more flexible civil penalty and infringement notice regime, as well as the introduction of additional investigations and determinations powers for the Commissioner, will allow the OAIC to shift to a more enforcement-oriented approach.

Recommendation 96 – Adopt elements from each of the options in proposal 24.9 to amend the current regulatory framework to enable the OAIC to shift to a more strategic, proactive regulator, subject to the considerations outlined in this submission.

Recommendation 97 – 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 98 – Expand s 41(dc) to instances where a complaint has already been adequately dealt with by an EDR scheme.

Recommendation 99 – 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.

Part 25: A direct right of action

25.1 Create a direct right of action with the following design elements:

- The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.

- The action would be heard by the Federal Court or the Federal Circuit Court.

- The claimant would first need to make a complaint to the OAIC (or FPO) and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.

- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.

- The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.

Is each element of the proposed model fit for purpose? In particular, does the proposed gateway to actions strike the right balance between protecting the court's resources and providing individuals with a more direct avenue for seeking judicial consideration and compensation?

25.1 We welcome proposal 25.1 to create a direct right of action that would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.

25.2 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. The 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 breach of privacy.[370]

25.3 A direct right of action would provide an additional incentive for APP entities to comply with their privacy obligations. It may also encourage APP entities to cooperate more fully in conciliations to avoid potentially costly court proceedings.

25.4 Importantly, a direct right of action, combined with changes to the existing privacy regulatory model (discussed in Part 24 of this submission), will provide increased opportunities for the courts to interpret the Privacy Act. As noted in the Discussion Paper, this would assist the public and APP entities to better understand their rights and obligations.[371]

[370] Lonergan Research, *Australian Community Attitudes to Privacy Survey 2020*, report to the OAIC, September 2020, p 67.

[371] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 187.

25.5 It would also work alongside other recommended changes to the OAIC's complaint-handling model to provide individuals with effective and cost-efficient pathways to resolving their privacy complaints (see Part 24 of this submission).

Design elements of the model

Who can exercise the right and harm threshold

25.6 We support the proposal to enable both individuals and representative classes of individuals who have suffered an alleged interference with their privacy to be able to bring an action in court for damages.

25.7 As noted in our submission to the Issues Paper, the direct right of action should not be limited to 'serious' interferences with privacy.[372] Limiting the action to 'serious' breaches of privacy would substantially curtail its effectiveness by precluding many individuals from seeking recourse in the courts. This would also limit the other potential benefits outlined above.

Forum for the direct right of action and remedies

25.8 We support the proposal that the action would be heard in the Federal Court or the FCC.

25.9 We note that giving complainants the choice to commence proceedings in the FCC could reduce the burden on individuals seeking to exercise the direct right of action. We support the suggestion that a 'small claims procedure' is created for privacy matters in the FCC, which offers reduced filing fees for smaller matters.

25.10 We also support the proposal that remedies available under the right would be any order the court sees fit including any amount of damages. In other words, damages should not be capped, which will enable the courts to set standards for appropriate types and levels of damages for privacy breaches, taking into account the particular facts and circumstances of each case.

25.11 As noted in our submission to the Issues Paper, this would also enable compensation amounts awarded by the courts to reflect, and keep pace with, the changing landscape of privacy harms.

Gateway to enliven the right

25.12 We support the proposal that a claimant would first need to make a complaint to the OAIC (or FPO)[373] and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.

25.13 The Discussion Paper proposes that the complainant could then elect to initiate action in court either:

- instead of pursuing conciliation

[372] See recommendation 51 of *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*.

[373] Part 24 of this submission discusses the proposed Federal Privacy Ombudsman.

- after conciliation has proven unsuccessful
- where the OAIC has determined the matter not suitable for conciliation, or
- where the OAIC has terminated the matter.

25.14 The complainant would also need to seek leave of the court to commence proceedings.

25.15 We consider that this approach strikes the right balance between protecting the court's resources by ensuring that individuals have access to a free dispute resolution mechanism in the first instance, while still providing individuals with a more direct avenue for seeking judicial consideration and compensation.

25.16 As noted in the Discussion Paper, where matters are assessed as suitable for conciliation, the complainant may realise it would be in their best interests to undertake conciliation prior to initiating court action. However, it also recognises that some complaints are unsuitable for conciliation and provides individuals with a more direct pathway to redress in the courts.[374]

25.17 It would also ensure the OAIC continues to have national oversight of privacy issues and the ability to identify potential systemic issues in the system that may warrant further regulatory or enforcement action.

25.18 We note that the proposed approach broadly aligns with the approach for human rights proceedings brought under the *Sex Discrimination Act 1984*, *Disability Discrimination Act 1992, Racial Discrimination Act 1975* or the *Age Discrimination Act 2004*. Specifically, individuals must first make a complaint to the AHRC and the complaint must be formally terminated by the AHRC before they are able to commence a claim in the Federal Court, the FCC or the Family Court of Australia.[375]

25.19 For the avoidance of doubt, we reiterate our comments from our submission to the Issues Paper that the gateway for enlivening the direct right of action should be consistent with the existing complaint-handling process under the Privacy Act.[376]

25.20 That is, where the OAIC considers it is reasonably possible that a complaint may be conciliated successfully there must be a reasonable attempt to conciliate.[377] However, the OAIC is not required to attempt to resolve the complaint through conciliation where we have decided not to investigate, or not to further investigate, a complaint (this is commonly referred to as 'declining a complaint').

25.21 Conciliation should not be a mandatory requirement in order for the direct right of action to be enlivened. The OAIC may at any time during the complaint process exercise the discretion to decline a complaint for a range of reasons set out in s 41 of the Privacy Act.

25.22 In certain circumstances, the Commissioner may consider that the direct right of action would be a more appropriate vehicle for some complaints, particularly representative complaints.

---

[374] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 24 November 2021, p 188.

[375] *Australian Human Rights Commission Act 1986* (Cth) s 46PO.

[376] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, 11 December 2020, accessed 8 November 2021, p 132.

[377] *Privacy Act 1988* (Cth) s 40A(1).

Accordingly, we reiterate recommendation 53 from our submission to the Issues Paper to ensure that the Commissioner has appropriate powers to decline to investigate a complaint or representative complaint, or to continue to investigate a complaint or representative complaint, where it is more appropriately dealt with by the courts.

Representative complaints

25.23 As noted in our submission to the Issues Paper, the existing representative complaint provisions in the Privacy Act 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).[378]

25.24 For example, s 38B(2) of the Privacy Act states that a class member in a representative complaint may opt out at any time if the complaint was lodged without the consent of the member, or otherwise at any time before the Commissioner begins to hold an inquiry into the complaint.

25.25 This means that the Commissioner is unable to put a definite 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.'

25.26 Accordingly, we reiterate recommendation 54 of our submission to the Issues Paper that the representative complaint provisions under Part V of the Privacy Act should be 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.

Role of the OAIC in court proceedings

25.27 We support the proposal that the OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court or on our own motion where the orders sought would affect privacy rights of people generally, the administration of the Act, or where there were other special circumstances in the public interest.

25.28 We note this approach aligns with the approach under other domestic laws, which allow regulators to seek leave of the court to appear as amicus curiae. For example, ASIC may appear as amicus curiae under court rules or, where applicable, the court's own inherent authority. Similarly, the Commissioners of the AHRC have the function of assisting the Federal Court, the FCC and the Family Court of Australia as amicus curie in discrimination matters.[379]

Recommendation 100 – Adopt proposal 25.1 to create a direct right of action with the following design elements:

[378] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, 11 December 2020, accessed 8 November 2021, p 132.

[379] *Australian Human Rights Commission Act 1986*, s 46PV.

- The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity.
- The action would be heard by the Federal Court or the FCC.
- The claimant would first need to make a complaint to the OAIC (or FPO) and have their complaint assessed for conciliation either by the OAIC or a recognised EDR scheme such as a relevant industry ombudsman.
- The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application.
- The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.

Recommendation 101 – 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 102 – 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.

Part 26: A statutory tort of privacy

26.1 Option 1 – Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

26.2 Option 2 – Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts.

26.3 Option 3 – Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person.

26.4 Option 4 – In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.

26.1 Privacy regulation operates against a backdrop of significant technological change. Submissions to the Issues Paper in favour of a statutory tort of privacy highlighted the increasing ease with which serious invasions of privacy occur in the digital age, facilitated by mobile technology and the internet.[380]

26.2 As noted in the ALRC's *Serious Invasions of Privacy in the Digital Era* (ALRC 123 Summary):

> A person's privacy may be invaded in a range of ways. Such invasions may occur with increasing ease and frequency in the digital era, when mobile phones in our pockets are all potential surveillance devices, drones are becoming cheaper and more advanced, and personal information once put online seems impossible to destroy or forget.[381]

26.3 The Privacy Act protects information privacy, which means that the scope of the Act is limited to the handling of 'personal information'. It does not extend to other types of privacy such as bodily[382] or territorial[383] privacy. Further, the Privacy Act regulates the handling of personal information by 'APP entities', which are Australian Government agencies and organisations with an annual turnover of more than $3 million.

26.4 This means that the Privacy Act does not apply to individuals acting in a personal capacity, most small business operators, media organisations acting in the course of journalism, and registered political parties and political representatives.

---

[380] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 7 December 2021, p 191.

[381] ALRC, *Serious Invasions of Privacy in the Digital Era – Summary Report (ALRC Summary Report 123)*, ALRC, June 2014, accessed 7 December 2021, p 5.

[382] The ALRC noted that 'bodily privacy' concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches. See ALRC, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, ALRC, May 2008, accessed 7 December 2021, p 142.

[383] The ALRC noted that 'territorial privacy' concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks. See ALRC, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, ALRC, May 2008, accessed 7 December 2021, p 142.

26.5 For instance, the Privacy Act will not apply to the following examples of invasions of privacy:

- non-consensual sharing of sexual images
- standing on a ladder in a laneway and peering over a back fence to take a video of someone in their backyard[384]
- recording a private conversation with someone without their knowledge or consent[385]
- using technology to film or surveil someone in a place where there is an expectation of privacy (for example, in a public bathroom)
- interfering with, misusing or disclosing an individual's private correspondence or private written, oral or electronic communication[386]
- disclosing or disseminating sensitive facts relating to an individual's private life[387]
- accessing personal information about another person available to an individual through their employment, but for which the employer is not liable because it was a misuse for a personal purpose (such as blackmail or in Family Court proceedings)[388]
- a data breach experienced by a small business not covered by the Privacy Act.

26.6 The preamble to the Privacy Act makes clear that the legislation was intended to implement, at least in part, Australia's obligations relating to privacy under Article 17 of the ICCPR, which 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 or reputation.
- Everyone has the right to the protection of the law against such interference or attacks.

26.7 Given the scope of Privacy Act outlined above, the Act does not fully implement Article 17 of the ICCPR in domestic law.[389] A statutory tort would provide greater coverage and protection to individuals in line with Australia's obligations under Article 17.

26.8 We note that several government inquiries in Australia have recommended the introduction of statutory tort for serious invasions of privacy. This includes ALRC Report 108[390] and ALRC Report

[384] Government of South Australia, *Civil Liability (Serious Invasions of Privacy) Bill – FAQs*, yourSAy website, n.d., accessed 7 December 2021.

[385] Note there is legislation in each state and territory concerning surveillance and listening devices.

[386] ALRC, *Serious Invasions of Privacy in the Digital Era (ALRC Report 123)*, ALRC, June 2014, accessed 7 December 2021, p 86.

[387] ALRC, *Serious Invasions of Privacy in the Digital Era (ALRC Report 123)*, ALRC, June 2014, accessed 7 December 2021, p 86.

[388] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 7 December 2021, p 191.

[389] ALRC, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, ALRC, accessed 7 December 2021, May 2008, p 2539.

[390] See ALRC, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, ALRC, May 2008.

123,[391] the ACCC's DPI Final Report,[392] and the AHRC's Human Rights and Technology Final Report.[393]

26.9 Accordingly, we support proposal 26.1 to introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123 (option 1).

The model of a statutory tort for invasion of privacy

26.10 The ALRC Report 123 sets out a detailed design of a statutory tort for serious invasion of privacy. In summary, the Discussion Paper notes that the ALRC recommended a statutory tort with two limbs:

- intrusion upon seclusion, and
- misuse of private information.

26.11 We note that 'intrusion upon seclusion' would include physical intrusion into private space or by watching, listening to, or recording private activities or private affairs. 'Misuse of private information' includes collecting or disclosing private information.[394]

26.12 This model is also consistent with the model proposed in South Australia's Civil Liability (Serious Invasions of Privacy) Bill 2021, which would enable an individual to bring civil proceedings where there has been a serious intrusion into their seclusion or a serious misuse of privacy information.[395]

26.13 Under the formulation recommended by the ALRC, a plaintiff would need to prove that:

- the public interest in privacy outweighed any countervailing public interest
- the breach of privacy satisfied a seriousness threshold, and
- they had a reasonable expectation of privacy in all the circumstances.

26.14 The model for the statutory tort recommended by the ALRC would be an important addition to the suite of regulatory measures needed to address gaps in the existing privacy protection framework and address current and emerging privacy risks and harms.

26.15 We also reiterate recommendation 58 from our submission to the Issues Paper that the statutory tort should be supplemented by legislative powers for the OAIC to be notified of, and to seek the leave of the court to act in the role of amicus curiae in relevant proceedings. This will be important where proceedings have the potential to impact the evolution of the Act and privacy jurisprudence and policy.

---

[391] See ALRC, *Serious Invasions of Privacy in the Digital Era (ALRC Report 123)*, ALRC, June 2014.

[392] See ACCC, *Digital Platforms Inquiry – Final Report*, ACCC, July 2019.

[393] See AHRC, *Human Rights and Technology Final Report*, AHRC, March 2021.

[394] ALRC, *Serious Invasions of Privacy in the Digital Era – Summary Report (ALRC Summary Report 123)*, ALRC, June 2014, accessed 7 December 2021, p 45.

[395] At the time of writing, a draft of the Bill had been published for public consultation. See https://yoursay.sa.gov.au/privacy-laws

Other options

26.16 As alternatives to proposal 26.1, the Discussion Paper also sets out the following options:

- introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts (proposal 26.2)
- do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information which would be highly offensive to an objective reasonable person (proposal 26.3).

26.17 The courts are yet to recognise a common law cause of action for serious invasions of privacy. As noted in the Discussion Paper, in 2001 the High Court contemplated the possibility of a tort of privacy being developed in Australia in *Australian Broadcasting Corporation v Lenah Game Meats*, however such a tort has yet to evolve at common law.

26.18 The ALRC Report 123 indicated that consultations with legal practitioners suggested that this is because litigants are reluctant to risk lengthy and costly proceedings and appeals arguing a novel point of law.[396] After reviewing the relevant case law, the ALRC also noted that the future development of the common law is difficult to predict.[397]

26.19 Accordingly, we do not support proposals 26.2 and 26.3, which would largely leave the development of a tort of serious invasion of privacy, including its scope and application, to the common law. We consider that the introduction of a statutory tort as recommended by the ALRC would provide clarity, certainty and guidance about the purpose and scope of the new action, the extent of protection it may provide and the impact it may have on potential defendants.

26.20 We note that proposal 26.3 also suggests extending the application of the Act to individuals in a non-business capacity for the collection, use or disclosure of personal information that would be highly offensive to an objective reasonable person.

26.21 This would result in a narrower application than the statutory tort for invasion of privacy, as it would only apply to individuals acting in a non-business capacity and would be limited to the mishandling of personal information. For example, as noted in the Discussion Paper, it would not cover instances where a person's housemate covertly watches them while they are showering, unless they made a recording.

26.22 We also note that the Online Safety Act provides the eSafety Commissioner with the ability to swiftly have damaging images taken down from social media and other online platforms. In the circumstances, we consider that the preferable approach is to implement a statutory tort for invasion of privacy as outlined in proposal 26.1.

[396] ALRC, *Serious Invasions of Privacy in the Digital Era – Summary Report (ALRC Summary Report 123)*, ALRC, June 2014, accessed 7 December 2021, p 9.

[397] ALRC, *Serious Invasions of Privacy in the Digital Era – Summary Report (ALRC Summary Report 123)*, ALRC, June 2014, accessed 7 December 2021, p 11.

Recommendation 103 – Adopt proposal 26.1 to introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123, rather than alternative proposals 26.2 and 26.3, which would leave the development of a tort of serious invasion of privacy to the common law.

Part 27: Notifiable Data Breaches scheme – impact and effectiveness

27.1 Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

In what specific ways could harmonisation with other domestic or international data breach scheme notifications be achieved?

What aspects of other data breach notification schemes might be beneficial to incorporate into the NDB scheme?

27.1 The NDB scheme has been in operation for almost 3 years, and the OAIC has resolved more than 3,000 data breach notifications in this time.[398]

27.2 As noted in our submission to the Issues Paper, we consider that the NDB scheme has been effective in meeting its key objectives of improving consumer protection, increasing accountability through transparency, and driving better security standards for the protection of personal information.[399]

27.3 We note that submitters to the Issues Paper were largely positive about the effectiveness of the NDB scheme in achieving its policy objective of enabling individuals to take action to protect themselves from harm resulting from a data breach.[400]

27.4 The OAIC closely monitors compliance with the NDB scheme and has an effective framework to assess and respond to notifications, and provide guidance to businesses, agencies and the community.[401]

27.5 We review every notice received under the NDB scheme to ensure that the notifying entity has met its obligations. This includes considering whether the notifying entity has:

- taken steps to contain the breach
- assessed whether the breach is likely to result in serious harm to individuals whose personal information was exposed
- taken steps to mitigate the risk of serious harm resulting from the breach

[398] OAIC, *Annual Report 2020-21*, OAIC, 21 October 2021, accessed 28 October 2021, p 9.

[399] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, 11 December 2020, accessed 28 October 2021, p 138.

[400] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 28 October 2021, p 198.

[401] OAIC, *Corporate Plan 2020-21*, OAIC, August 2020, accessed 28 October 2021.

- provided appropriate notification to the OAIC and to affected individuals on the details of the breach and the steps that individuals can take to mitigate the risk of serious harm arising from the breach.[402]

27.6 We will continue to work with notifying entities to ensure breaches are contained and rectified, individuals are informed in a timely manner so they can act swiftly, and measures are put in place to prevent reoccurrence.[403]

27.7 Resources are available on the OAIC's website to support regulated entities to comply with their obligations under the NDB scheme. This includes a guide to assist APP entities to prepare for, and respond to, data breaches in line with their obligations under the Privacy Act and data breach prevention strategies for organisations developed with the ACSC.[404]

27.8 Additionally, we publish six-monthly statistical reports on the causes of data breaches.[405] These reports are intended to provide government and industry with insights into data breach trends and assist to improve awareness and understanding of data breach risks and steps that entities can take to prevent them occurring. The data breach reports also highlight emerging issues and areas for ongoing attention by entities entrusted with protecting personal information.[406]

27.9 We also undertake tailored educational and guidance activities with top reporting sectors. For example, the OAIC has delivered webinars in conjunction with the Royal Australian College of General Practitioners and the Tax Practitioners Board to assist their constituents to understand the scheme and their obligations relating to data breaches.[407] We have published a *Guide to health privacy* to help health service providers – from doctors and private sector hospitals, through to allied health professionals, pharmacists, childcare centres and gyms – understand their obligations under the Privacy Act and embed good privacy in their practices.[408]

27.10 After more than 3 years of operation, we expect that entities should be well equipped to meet their obligations under the NDB scheme and take proactive measures to prevent breaches of personal information.

Harmonising domestic and international frameworks

27.11 From our oversight of the NDB scheme, the OAIC has observed the intersection of data breaches affecting multiple entities, including state and territory government agencies and entities

[402] OAIC, *Annual Report 2020-21*, OAIC, 21 October 2021, accessed 28 October 2021, p 36.

[403] OAIC, *Lessons learned during first 12 months of Notifiable Data Breaches scheme* [media release], OAIC, 13 May 2019, accessed 28 October 2021.

[404] NDB scheme resources are available on the OAIC website at https://www.oaic.gov.au/privacy/notifiable-data-breaches.

[405] NDB scheme statistical reports are available on the OAIC website at https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics.

[406] OAIC, *Annual Report 2020-21*, OAIC, 21 October 2021, accessed 28 October 2021, p 37.

[407] Recordings of these webinars are available on the OAIC's website at https://www.oaic.gov.au/privacy/notifiable-data-breaches.

[408] The *Guide to health privacy* is available at https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy.

covered by the Privacy Act, and the resultant fragmentation of responsibilities and rights in relation to data breaches that transcend borders.[409]

27.12 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, including commensurate protections for personal information such as mandatory data breach notification requirements.[410]

27.13 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. The OAIC's general position is that when a new state or territory data breach reporting scheme is created, to the extent possible, the tests and obligations on entities should align with requirements of the NDB scheme under the Privacy Act.[411]

27.14 Consistency in regulation across domestic jurisdictions will reduce compliance burdens and cost and provide clarity and simplicity for regulated entities and the community. National consistency should therefore be a key goal of mandatory data breach notification schemes and privacy regulation more broadly.

27.15 We acknowledge that there are policy considerations that will justify separate regimes and stronger privacy protections in certain circumstances. For example, at the Commonwealth level, in recognition of the special sensitivity of health information, the *My Health Records Act 2012* (MHR Act) makes it mandatory for certain entities to notify the OAIC and the MHR System Operator of a data breach involving the MHR system.

27.16 While there are similarities between the reporting requirements of both schemes, there are some important differences. For example, data breaches notified under the MHR Act do not need to be reported under the NDB scheme to prevent duplication of reporting.

27.17 Another key difference is that entities must report every MHR data breach that has or may have occurred, whereas only data breaches that are likely to result in serious harm to affected individuals need to be reported under the NDB scheme. MHR data breaches must be reported as soon as practicable under the MHR Act even when remedial action to mitigate the likelihood of harm arising because of the data breach is in progress or has already been taken.

27.18 The lower data breach notification threshold required for information held in the MHR system was designed as a privacy enhancing measure, given that the MHR system is a searchable network of connected registered repositories storing sensitive personal information. Further, the lower reporting threshold ensures visibility of data breaches that may not be likely to result in serious harm to an individual, but which may point to systemic issues in the ecosystem.[412]

---

[409] OAIC, *OAIC Submission to NSW Inquiry into Cybersecurity*, OAIC website, 29 September 2020, accessed 28 October 2021.

[410] OAIC, *OAIC Submission to NSW Inquiry into Cybersecurity*, OAIC website, 29 September 2020, accessed 28 October 2021.

[411] OAIC, *Data Availability and Transparency Bill 2020: exposure draft consultation*, OAIC website, November 2020, accessed 28 October 2021.

[412] OAIC, *Legislation review of the My Health Records Act 2012 – Submission to the Department of Health*, OAIC website, 26 October 2020, accessed 28 October 2021.

27.19 We acknowledge that there are potential challenges for healthcare providers to comply with two schemes with different reporting thresholds, however, in these circumstances there are important policy justifications for maintaining separate reporting requirements given the sensitivity of the personal information held in the MHR system.[413]

27.20 In addition to our recommendations below, the recommendations in Part 28 (Interactions with other frameworks) of this submission will also help to promote regulatory harmonisation and interoperability.

Recommendation 104 – New state and territory data breach reporting schemes should, to the extent possible, align with the requirements of the NDB scheme under the Privacy Act to reduce regulatory fragmentation and increase certainty for regulated entities.

Recommendation 105 – The NDB scheme should remain the baseline for data breach reporting requirements at the federal level and any separate scheme should seek to increase, not replicate, those reporting requirements where warranted.

Importance of timely assessment and notification

27.21 The core objective 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.[414] Entities must provide individuals with clear and timely information about data breaches, including recommendations about the steps they can take to protect themselves from harm.

27.22 An entity must take all reasonable steps to complete the assessment within 30 calendar days after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach.[415] The assessment should be reasonable in scope and conducted expeditiously in the circumstances.[416]

27.23 We expect that entities should generally treat 30 days as the maximum time limit for completing an assessment, and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.[417]

27.24 The Privacy Act is clear that an entity must also notify the OAIC and affected individuals *as soon as practicable* after confirming that there are reasonable grounds to believe an eligible data breach occurred.

---

[413] OAIC, *Legislation review of the My Health Records Act 2012 – Submission to the Department of Health*, OAIC, 26 October 2020, accessed 28 October 2021.

[414] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, p 25.

[415] *Privacy Act 1988* (Cth) s 26WH(2).

[416] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, p 83.

[417] OAIC, 'Part 4: Notifiable Data Breach (NDB) Scheme', *Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)*, oaic.gov.au, 13 July 2019, accessed 28 October 2021.

27.25 Any unnecessary delay in providing this information undermines the purpose of the NDB scheme by denying affected individuals the ability to take timely action to protect themselves from harm.[418] For example, a delay in notification increases the risk of an affected individual becoming a victim of an identity crime such as identity theft, as they may be unaware of the need to take action to mitigate the detrimental consequences of the data breach.[419]

27.26 Section 26WL(2) of the Act provides three ways by which individuals affected may be notified. An entity may notify each individual whose personal information has been involved in the eligible data breach or notify only individuals who are at risk of serious harm. If neither of these options are practicable, an entity may publish a statement about the eligible data breach on its website and publicise the statement.

27.27 The three options recognise that it may not be possible to definitively identify every individual at risk of serious harm in an eligible data breach or provide tailored notifications specific to each individual.

27.28 In determining the appropriate notification option, it is critical that entities have regard to the core objective of the NDB scheme which, as noted above, is to allow individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that may arise from the breach.[420] Consequently, entities should have regard to the need to conduct a thorough assessment, the need to provide information that assists individuals to mitigate harm and the need to provide timely notification to affected individuals.[421]

27.29 We will continue to closely monitor compliance with the NDB scheme and take a proportionate and evidence-based regulatory approach to data breaches exercising enforcement powers where necessary. Changes to legislated timeframes may also require further consideration if the OAIC observes an increase in entities taking too long to comply with their notification obligations.

Addressing the impact of breaches on individuals and mitigating harm

27.30 Under s 26WK(3)(d) of the Privacy Act, 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 individuals to mitigate the adverse impacts or risk of harm that may arise as a result of a data breach.

---

[418] OAIC, *Human factor dominates latest data breach statistics* [media release], OAIC, 28 January 2021, accessed 28 October 2021.

[419] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, p 18.

[420] Explanatory Memorandum, Privacy Amendment (Notifiable Data Breaches) Bill 2016, p 25.

[421] OAIC, *Notifiable Data Breaches Report: July-December 2020*, OAIC, 28 January 2021, accessed 28 October 2021, pp 10-11.

27.31 As noted in the Discussion Paper, the OAIC has observed that best practice entities take responsibility for the costs and impacts of data breaches when they occur, and support individuals to mitigate the impact of a data breach.[422]

27.32 This may include setting up support lines to provide customers with a centralised channel to ask questions, paying for a credit monitoring service that alerts affected individuals if there are changes to their credit report, monitoring the dark web to identify if personal information compromised in a data breach is being traded online, assisting individuals to replace compromised credentials such as passports and drivers licences, and engaging providers such as IDCARE to provide post-incident support to individuals.

27.33 To this end, we support proposal 27.1, which we consider will promote greater transparency and accountability by requiring entities to notify individuals of the steps they have taken or intend to take in response to the breach.

27.34 Additionally, the requirement to notify individuals, where appropriate, of steps taken to reduce any adverse impacts will further promote the consumer protection objectives of the NDB scheme and ensure that individuals have additional relevant information to protect themselves from harm.

27.35 As noted in the Discussion Paper, greater transparency about the actions entities are taking in response to a data breach will help to inform the OAIC's regulatory response. This includes informing the guidance we provide to entities about best practice steps they can take in response to a data breach to reduce adverse impacts on individuals, which entities can benchmark themselves against.[423]

27.36 We also note this approach is consistent with the approach under New Zealand's mandatory data breach reporting laws, thereby promoting regulatory interoperability.

27.37 The existing remedial action exception in s 26WF of the Act also provides an incentive for entities to take positive steps to lessen the harm that may result from a data breach and avoid the need to notify.

27.38 Relatedly, we are also supportive of the reforms to s 52 determinations as outlined in proposal 24.5, which will permit the Commissioner to require an entity to take reasonable steps to mitigate potential future loss or damage resulting from an interference with privacy.

Recommendation 106 – Adopt proposal 27.1 to amend subsections 26WK(3) and 26WR(4) of the Act to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.

[422] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 28 October 2021, p 212.

[423] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 28 October 2021, p 206.

Part 28: Interactions with other schemes

28.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.

28.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

28.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

What aspects of Commonwealth, state and territory privacy laws should be considered for harmonisation by this working group if it is established?

Interaction between the Act and other Commonwealth schemes

28.1 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.[424]

28.2 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.[425] The APPs promote national consistency of regulation by providing a minimum or baseline set of standards that are applicable to both Australian Government agencies and private sector organisations covered by the Act.

28.3 The Discussion Paper notes that the Act provides a baseline of protection upon which more specific requirements can be imposed through the operation of other Commonwealth legislation.[426]

28.4 However, the Privacy Act also contains mechanisms that may be used to address specific privacy risks and concerns, meaning a separate Commonwealth legislative regime may not always be necessary.

28.5 Part IIIB of the Privacy Act allows for the creation of APP codes, which are written codes of practice about information privacy. An APP code must:

- set out how one or more of the APPs are to be applied or complied with
- specify the APP entities that are bound by the code, or a way of determining the APP entities that are bound by the code, and

[424] OAIC, *Privacy Act Review – Issues Paper: Submission by the Office of the Australian Information Commissioner*, OAIC, 11 December 2020, accessed 9 December 2021, p 146.

[425] *Privacy Act 1988* s 2A(c).

[426] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 9 December 2021, p 207.

- set out the period during which the code is in force.[427]

28.6 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.[428]

28.7 A breach of a registered code will be an interference with the privacy of an individual under s 13 of the Privacy Act and subject to investigation by the Commissioner.

28.8 APP codes could be used to address concerns raised by submitters to the Issues Paper about Commonwealth privacy laws spanning different government portfolios, and a lack of consistency in the scope and structure of privacy protections in different pieces of legislation.[429]

28.9 As discussed in Part 3 of this submission, we welcome proposals 3.1 and 3.2 to provide the Commissioner with greater flexibility and discretion to develop APP codes, which would ensure that further specificity and particularisation can be given to the APPs where required and emerging privacy risks can be quickly and efficiently addressed.

28.10 The advantage of using delegated legislation in this way is that it has a greater degree of flexibility for adjustments to be made for sectors that are rapidly evolving, such as digital platforms, to ensure that regulation remains fit for purpose and keeps up with market developments.

28.11 However, we acknowledge that there are policy considerations that will justify separate Commonwealth privacy regimes and stronger privacy protections in certain circumstances. Separate schemes, where appropriate, may also reduce the compliance burden for regulated entities by ensuring that privacy protections are consolidated in scheme-specific legislation rather than requiring an entity to navigate various laws to determine its compliance obligations.

28.12 We note that submissions to the Issues Paper generally supported creating specific legislation to impose more stringent privacy protections where this is justified for high privacy risk activities. For example, the MHR system is supported by additional legislated privacy obligations in recognition of the highly sensitive nature of the personal information held in the system.[430]

28.13 However, if privacy protections are included in other legislative regimes, it is critical to ensure that the Commissioner has regulatory oversight of the privacy-specific aspects of those regimes. This will ensure that regulation and enforcement is clear, consistent and effective.

---

[427] *Privacy Act 1988* (Cth) s 26C(2).

[428] *Privacy Act 1988* (Cth) s 26C(4).

[429] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 9 December 2021, p 208.

[430] AGD, *Privacy Act Review – Discussion Paper*, AGD, October 2021, accessed 9 December 2021, p 209.

Consistency in oversight will also help to reduce regulatory burden, for both regulators and APP entities, by ensuring that entities do not face multiple enforcement actions from different regulators under different laws.

28.14 We welcome proposal 28.1 for the Attorney-General's Department to develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations or that otherwise seek to override the APPs.

28.15 The Discussion Paper notes that the guide could provide information on the types of things to be considered by departments during the policy development and legislative process – including factors relevant to determining when privacy protections above those set out in the APPs are warranted, how additional protections should be drafted, and relevant oversight and enforcement mechanisms recommended to apply to such schemes.

28.16 The OAIC has specific monitoring and advice functions under the Privacy Act, and we regularly provide privacy advice to government about the design and development of proposed laws.[431]

28.17 Accordingly, we recommend that the privacy law design guide should address the following critical issues and matters that should be considered by agencies when developing schemes that require additional privacy protections or otherwise seek to override the APPs:

- The fundamental starting point is that the Privacy Act and the APPs should remain the baseline for privacy protection at the federal level and any new Commonwealth laws that propose to implement new privacy obligations should seek to increase, not replicate, those baseline requirements (where warranted).
- If privacy protections are included in other legislative regimes, it is critical that the Commissioner has full jurisdiction over enforcing those protections and all entities subject to those protections, to ensure that privacy regulation is clear, consistent and effective.[432]
- If an agency is developing legislation that seeks to rely on the required or authorised exception to the APPs (such as legislation authorising the use or disclosure of personal information), they should consider whether the proposed legislation is reasonable, necessary and proportionate to achieving a legitimate public policy objective. A PIA can assist agencies to undertake this assessment, which may also assist with the development of Human Rights Compatibility Statements for legislative projects. Additionally, under the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, agencies have a legal obligation to conduct a PIA for all high privacy risk projects and initiatives. The OAIC has published guidance to help agencies determine when a PIA is required under the Code, which notes that, amongst other matters, one of the factors that may point to the

[431] This includes examining proposed enactments that would require or authorise acts or practices that might otherwise interfere with privacy and ensuring that any adverse impacts of a proposed enactment on the privacy of individuals are minimised 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.

[432] The Commissioner has a range of existing regulatory responsibilities under various Commonwealth laws that also relate to privacy including, but not limited to, the *Telecommunications Act 1997*, *Telecommunications (Interception and Access) Act 1979*, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, *Healthcare Identifiers Act 2010*, *MHR Act 2012* and the privacy aspects of the CDR system under the *Competition and Consumer Act 2010*.

potential for a high privacy risk project is developing legislation that seeks to engage the required or authorised by law exception to the APPs.

28.18 The OAIC is available to provide advice and consult with the Attorney-General's Department on the development of the privacy law design guide.

28.19 More broadly, it's important to note that the proposals in the Discussion Paper and the recommendations made in this submission will, if adopted, raise the baseline standard of data handling in Australia through new and strengthened privacy protections, which will reduce the need to have separate privacy regimes with stronger privacy protections.

Recommendation 107 – Adopt proposal 28.1 to develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations or that otherwise seek to override the APPs.

Recommendation 108 – Ensure that the privacy law design guide addresses the following issues:

- The Privacy Act and the APPs should remain the baseline for privacy protection at the federal level and any new Commonwealth laws that propose to implement new privacy obligations should seek to increase, not replicate, those baseline requirements (where warranted).
- If privacy protections are included in other legislative regimes, the Commissioner should have full jurisdiction over enforcing those protections and all entities subject to those protections, to ensure that privacy regulation is clear, consistent and effective.
- If an agency is developing legislation that seeks to rely on the required or authorised exception to the APPs (such as legislation authorising the use or disclosure of personal information), they should consider whether the proposed legislation is reasonable, necessary and proportionate to achieving a legitimate public policy objective. A PIA can assist agencies to undertake this assessment, which may also assist with the development of Human Rights Compatibility Statements for legislative projects.

Recommendation 109 – Consult the Commissioner in the development of the privacy law design guide.

Interactions between the OAIC and other regulators

28.20 The OAIC has observed growing intersections between domestic frameworks including privacy, competition and consumer law, and online safety and online content regulation.

28.21 We consider that there is increasing intersection and convergence between the different frameworks for the following reasons:

- privacy is growing as a material factor in purchasing decisions, alongside the traditional factors of price and quality of product

- the emergence of data-driven business models, and
- the scale and scope of technological change – including the emergence of new platforms and services – has given rise to new ways for individuals to interact online and created new risks and harms.

28.22 While there are synergies between these frameworks, there are also variances given each regulatory framework is designed to address different economic and societal issues.

28.23 As noted in our submission to the Issues Paper, 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. At the same time, we do not consider that regulatory overlap is necessarily a negative outcome, particularly where it is well managed. It is more problematic if regulatory gaps expose individuals to harm.

28.24 An effective approach must address the importance of institutional coordination between different regulatory bodies in different areas, given the need for complementary expertise.[433]

28.25 Regulatory cooperation can involve informal actions, such as engaging with networks like the ACCC's Scams Awareness Network, to more formal actions, such as collaboration on compliance activities.

28.26 To this end, the OAIC has entered into MOUs with other regulators including the ACCC, ACMA, Australian Digital Health Agency (ADHA) and the Inspector-General of Intelligence and Security (IGIS). We have 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.

28.27 The CDR is a good example of a reform aimed at balancing individuals' right to control and use their data with strong accountability measures, to enable greater competition, consumer benefits and economic growth.

28.28 The OAIC and ACCC have distinct but complementary roles in co-regulating the CDR. The ACCC will enforce serious or systemic breaches of the CDR and the OAIC is responsible for the privacy aspects of the system, as well as being the primary complaint handler. The OAIC and the ACCC have published a joint compliance and enforcement policy to provide transparency and certainty to the regulated community.

28.29 Working with co-regulators that have complementary, but different experience, skills and powers, ensures domestic regulators are able to address a broader scope of issues, and achieve holistic consumer protection outcomes.

28.30 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. To this end, we support the measures in the Online Privacy Bill, which will enhance the OAIC's ability to share information

[433] B Kira, V Sinha and S Srinivasan, 'Regulating digital ecosystems: bridging the gap between competition policy and data protection', *Industrial and Corporate Change*, 2021, 00, 1-24.

with other relevant bodies including law enforcement bodies, alternative complaint bodies, and state, territory or foreign privacy regulators.

28.31 A key focus for the OAIC is working with international and domestic regulators, government, entities, and civil society to help ensure that privacy policy and legislation are interoperable, address contemporary privacy and data protection risks to Australians, and support the Australian economy.[434] Accordingly, we support proposal 28.2 to encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

Recommendation 110 – Adopt proposal 28.2 to encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

Interaction with state and territory privacy laws

28.32 The OAIC considers that harmonisation of privacy protections should be a key goal in the design of any federal, state or territory laws that purport to address privacy issues.

28.33 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.

28.34 As noted above, the Privacy Act and the APPs provide the basis for nationally consistent regulation of privacy and the handling of personal information. 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.

28.35 Consistency in regulation across domestic jurisdictions will reduce compliance burdens and cost and provide clarity and simplicity for regulated entities and the community. National consistency, therefore, should be a key goal in the design of any state or territory laws that purport to address privacy issues.

28.36 By way of example, the DAT Bill includes measures to ensure that personal information shared under the scheme is handled consistently with the privacy obligations in the Commonwealth Privacy Act. Specifically, all data scheme entities must either be subject to the Privacy Act or comparable privacy protections.

28.37 Clause 28(1)(b) of the DAT Bill allows State or Territory authorities in jurisdictions with privacy laws to be covered by those laws, where that coverage is equivalent to the Privacy Act. The Explanatory Memorandum to the DAT Bill states that:

[434] OAIC, *Corporate Plan 2020-21*, OAIC, August 2020, accessed 9 December 2021.

To be deemed equivalent, a jurisdictional law must provide for protection of personal information comparable to the Australian Privacy Principles, monitoring of compliance with the law, and a means of recourse for individuals if their information is handled contrary to the law. This approach is intended to preserve the remit and autonomy of the States and Territories, and their privacy regulators, without diminishing the privacy standards set for personal information by the Privacy Act.[435]

28.38 Accordingly, to promote consistency of privacy law regulation across federal, state and territory jurisdictions we reiterate recommendations 69 and 70 from our submission to the Issues Paper to:

- ensure that the harmonisation of privacy protections is a key goal in the design of any federal, state or territory laws that purport to address privacy issues
- ensure that privacy protections in any state or territory laws that purport to address privacy issues are commensurate with those under the Privacy Act.

28.39 To further these objectives, we support proposal 28.3 to establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

28.40 The Discussion Paper also asks what aspects of Commonwealth, state and territory privacy laws should be considered for harmonisation by the working group if it is established.

28.41 As noted in Part 27 of this submission, in our oversight of the NDB scheme, we have observed the intersection of data breaches affecting multiple entities, including state and territory government agencies and entities covered by the Privacy Act, and the resultant fragmentation of responsibilities and rights regarding data breaches that transcend borders.[436]

28.42 Consequently, we consider that mandatory data breach notification laws across Commonwealth, state and territory jurisdictions is an area that would benefit from consideration by the working group. The OAIC's general position is that when a new state or territory data breach reporting scheme is created, to the extent possible, the tests and obligations on entities should align with requirements of the NDB scheme under the Privacy Act.[437]

Recommendation 111 – 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 112 – Ensure that the privacy protections in any state or territory laws that purport to address privacy issues are commensurate with those under the Privacy Act.

Recommendation 113 – Adopt proposal 28.3 to establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

[435] Explanatory Memorandum, Data Availability and Transparency Bill 2020, pp 35-36.

[436] OAIC, *OAIC Submission to NSW Inquiry into Cybersecurity*, OAIC website, 29 September 2020, accessed 9 December 2021.

[437] OAIC, *Data Availability and Transparency Bill 2020: exposure draft consultation*, OAIC website, November 2020, accessed 9 December 2021.