ASIAN BUSINESS LAW INSTITUTE

FUTURE OF PRIVACY FORUM

ABLI-FPF CONVERGENCE SERIES

Australia

Status of Consent for Processing Personal Data

JUNE 2022

AUTHORED BY

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

PROJECT LEAD

Dr. Clarisse Girot

Honorary Senior Fellow, Asian Business Law Institute

CONTRIBUTOR

Anna Johnston

Principal, Salinger Privacy

ACKNOWLEDGEMENTS

This Report benefitted from contributions and editing support from Dominic Paulger and Catherine Shen and research from Lee Matheson.

DISCLAIMER

TABLE OF CONTENTS

1. INTRODUCTION

This report summarizes the roles played by consent and related provisions, including alternatives to consent, in Australia's data protection framework and highlights provisions which can serve as indicators for convergence of laws and regulations in this area across Asia Pacific.

2. AUSTRALIA'S DATA PROTECTION FRAMEWORK

2.1. Privacy Act

The Privacy Act of 1988 (most recently amended in 2018) ("**Privacy Act**")[1] forms the cornerstone of Australia's privacy protection framework.

The Privacy Act gives effect, among other provisions, to the 13 Australian Privacy Principles ("**APPs**") set out in Schedule 1 of the Privacy Act. Broadly, the APPs establish principles for handling of "personal information"[2] through its entire lifecycle. Specifically, the APPs cover:

- open and transparent management of personal information;[3]
- anonymity and pseudonymity;[4]
- collection of solicited personal information;[5]
- handling of unsolicited personal information;[6]
- notification of collection of personal information;[7]
- use and disclosure of personal information;[8]
- direct marketing;[9]
- cross-border transfer of personal information;[10]
- adoption, use, or disclosure of government-related identifiers;[11]
- quality[12] and security[13] of personal information; and
- access to,[14] and correction of,[15] personal information.

Entities which are subject to the Privacy Act (termed "**APP Entities**")[16] must comply with the APPs and unless an exception applies, are prohibited from doing an act or engaging in a practice which breaches

---

[1] Available at https://www.legislation.gov.au/Series/C2004A03712

[2] "**Personal information**" refers to information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not (Privacy Act, s 6).

[3] APP 1.

[4] APP 2.

[5] APP 3.

[6] APP 4.

[7] APP 5.

[8] APP 6.

[9] APP 7.

[10] APP 8.

[11] APP 9.

[12] APP 10.

[13] APP 11.

[14] APP 12.

[15] APP 13.

[16] The term "**APP Entities**" includes Australian Government agencies and organizations with an annual turnover more than $3 million but excludes: most small business operators (businesses under the AU$3 million turnover threshold) unless they are explicitly covered by, or have opted into, the Privacy Act; registered political parties; media organizations; state or territory authorities (which are mostly covered by separate privacy laws); or prescribed instrumentalities of a state (Privacy Act, s 6)

any of the APPs.[17] Such a breach would be considered an "interference with the privacy of an individual"[18] and could give rise to investigation and enforcement by Australia's data protection authority, the Office of the Australian Information Commissioner ("**OAIC**").

2.2. Recent developments

In recent years, Australian authorities have been contemplating regulation of the digital economy and large digital platforms that have a major impact on the private lives of Australian citizens. In particular, authorities are considering a massive overhaul of the Privacy Act to strengthen the privacy regulator's powers and have also put forward a series of complementary proposals to review other broader regulation of the digital economy, including rules and regulations governing competition, consumer protection, online safety, and content regulation.

The Federal Government initiated this process in response to a groundbreaking "Digital Platforms Inquiry" report ("**DPI Report"**) published by the Australian Competition and Consumer Commission ("**ACCC"**) in June 2019.[19] Although the ACCC considered that privacy could not be considered in isolation from broader issues of competition and consumer protection in digital markets, many of the DPI Report's final recommendations concerned privacy-related issues, including the importance of personal data to the business models of digital platforms and concerns raised by the Facebook/ Cambridge Analytica incident.

a. Review of the Privacy Act

In response to the DPI Report, the Federal Government committed to undertake a review of the Privacy Act and to consult on options for implementing a number of privacy-specific recommendations to better empower consumers, protect their data, and support the digital economy.

In October 2020, the Attorney General's Department ("**AGD"**) released a "Privacy Act Review Issues Paper" ("**Issues Paper"**)[20] followed by a "Privacy Act Review Discussion Paper" ("**Discussion Paper"**) in October 2021.[21]

The Discussion Paper draws from over 200 submissions which the AGD received in response to the Issues Paper.[22] These submissions included many criticisms of the excessive focus placed on consent in Australia's privacy protection ecosystem. The Discussion Paper therefore highlights the potential for privacy reforms to embed greater privacy rights and controls for individuals, including increased controls around notice and consent.

b. OP Bill

Also in October 2021, the AGD published an Exposure Draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021, commonly called the Online Privacy Bill ("**OP Bill"**).[23]

If enacted, the OP Bill would enable the creation of a binding Online Privacy Code ("**OP Code"**) — a registered code under the Privacy Act[24] which would address how certain APPs apply to "Online Privacy Organizations" ("**OP Organizations"**), a term which includes social media services, data brokers, and other large online platforms.

---

[17] Privacy Act, s 15. An act or practice breaches an APP if it is contrary to or inconsistent with the APP (Privacy Act, s 6A).
[18] Privacy Act, s 13(1)(a).
[19] Available at https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf
[20] Available at https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-cth-issues-paper
[21] Available at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/
[22] Available at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/published_select_respondent
[23] Available at https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/
[24] Registered codes under the Privacy Act are discussed in greater detail under "Privacy Codes" below.

As of the date of this Report, the status of the OP Bill is uncertain. The OP Bill had been listed for introduction to the Senate in the last sitting of Parliament before Australia's federal election in May 2022. However, the Bill was not introduced in Parliament before the election and so has technically lapsed.[25] The subsequent election also established a new majority in Parliament, but this new Government has not yet given any indication as to the fate of the OP Bill and AGD's proposals. However, it is still possible that the government will introduce the Bill in its existing form in the next term of Parliament.

3. CONSENT AND "PRIVACY SELF-MANAGEMENT" IN THE PRIVACY ACT

Consent plays an important role in the Privacy Act and is relevant to the operation of a number of APPs.[26] Recent decisions by the OAIC, whose extraterritorial enforcement powers have just been strengthened by a landmark decision of the Federal Court, also reveal a clear intention on the part of the regulator to strictly enforce the existing conditions for valid consent under the Privacy Act, in combination with an extensive interpretation of the notion of personal information.[27]

However, as much of the discussion around reform of the Privacy Act centered on refocusing the role of consent and recognizing the equal importance of the other principles in the Act, it would be advisable to monitor these developments carefully.

3.1. Consent in the APPs

a. Collection of personal information

The APPs do not require consent for collection of personal information directly from an individual, unless the personal information to be collected constitutes "sensitive information" under the Privacy Act.[28]

Where an APP Entity collects personal information directly from an individual, it will be usually sufficient if the personal information is reasonably necessary for a function or activity of the APP Entity,[29] if the collection is by lawful and fair means,[30] and if the APP Entity takes reasonable steps to provide notification to the individual pursuant to APP 5.

However, if the APP Entity seeks to collect sensitive information, then the APP Entity must also obtain express informed consent from the individual for collection of his/her personal information,[31] unless an alternative legal basis exists (e.g., if the collection is required or authorized by law,[32] or if a "permitted general situation" or "permitted health situation"[33] exists).

By default, the APPs also require APPs Entities to collect personal information directly from the individual who is the subject of that personal information.[34] However, this rule is subject to exceptions, including where the individual consents to the collection of the information from someone other than the individual.[35]

---

[25] Denham Sadler, "Govt fails to pass 'landmark' online privacy reforms," *InnovationAus.com* (11 April 2022), available at https://www.innovationaus.com/govt-fails-to-pass-landmark-online-privacy-reforms/

[26] APP Guidelines, B.34.

[27] See "SANCTIONS AND ENFORCEMENT" below for further details.

[28] See ""Sensitive information" under the Privacy Act" below.

[29] APPs 3.1 and 3.2.

[30] APP 3.5.

[31] APP 3.3.

[32] APP 3.4(a).

[33] APPs 3.4(b) and 3.4(c). See "COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW" below for further details.

[34] APP 3.6.

[35] APP 3.6(a)(i).

b. Use and disclosure of personal information

The APPs may require consent for use and disclosure of personal information, depending on the circumstances.

By default, the APPs only permit an APP Entity to use or disclose within the parameters of the purpose for which that personal information was collected (**"primary purpose"**).[36] Where an APP Entity uses or discloses personal information for a primary purpose other than direct marketing (see below), consent would not usually be required.

However, consent is one of several legal bases which permit an APP Entity to use or disclose personal information for a different purpose from the primary purpose (**"secondary purpose"**).[37]

c. Use and disclosure of personal information for the purpose of direct marketing

By default, the APPs also prohibit an APP Entity which holds personal information from using or disclosing that personal information for the purpose of direct marketing.[38] However, this rule is subject to exceptions,[39] including where the individual consents to use of his/her personal information for the purpose of direct marketing and is provided with a simple means to opt out of direct marketing communications.[40]

However, if the APP Entity seeks to use or disclose *sensitive* personal information for the purpose of direct marketing, then the APP Entity has no alternative but to obtain the individual's consent to such use or disclosure.[41]

d. Cross-border transfer of personal information

The default rule under APP 8.1 is that if an APP Entity wishes to disclose personal information to an overseas recipient, then the APP Entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information.[42]

However, this requirement is subject to exceptions,[43] including where the individual consents to the disclosure, after the APP Entity has expressly informed the individual that if the individual consents to the cross-border transfer, then the APP Entity would not be subject to the requirement in APP 8.1.[44]

3.2. Sectoral consent requirements in the Privacy Act

The Privacy Act also makes special provisions for certain types of information processed by specific sectors, such as the credit or health sectors.

These provisions may *exclude* the requirement to obtain the individual's consent where higher interests prevail or, conversely, *require* consent in specific circumstances where individuals need to be able to make decisions as to use of their personal information.

a. Credit sector

Part IIIA of the Privacy Act – which is supported by the Privacy Regulation 2013[45] and the Privacy (Credit Reporting) Code 2014[46] – applies to persons that handle consumer credit reporting information,

---

[36] APP 6.1.
[37] APP 6.1(a).
[38] APP 7.1.
[39] APPs 7.2 and 7.3.
[40] See, generally, APP 7.3.
[41] APP 7.4.
[42] APP 8.1.
[43] See, generally, APP 8.2.
[44] APP 8.2(b).
[45] Available at https://www.legislation.gov.au/Series/F2013L02126
[46] Available at https://www.legislation.gov.au/Details/F2022L00575/

including credit reporting bodies ("**CRBs**"), credit providers (including energy and water utilities and telecommunications providers), and certain other third parties.

By default, a CRB is prohibited from using or disclosing "credit reporting information"[47] about an individual that the CRB holds and may be subject to a penalty for breaching this prohibition.[48] However, this rule is subject to exceptions, some of which are based on consent.

For instance, a CRB may be permitted to disclose credit reporting information in response to requests from certain kinds of financial institutions for specified credit- or insurance-related purposes, where the individual expressly consents to disclosure of the information for such purposes.[49]

Further, where an individual has been a victim of fraud (including identity fraud), Part IIIA enables the individual to request a CRB to commence a ban period, during which the CRB may not disclose or use the individual's credit reporting information unless the individual expressly consents in writing.[50]

b. Health sector

The Privacy Act regards "health information"[51] as one of the most sensitive types of personal information and provides a number of additional protections to this class of personal information.

As health information qualifies as "sensitive personal information" for purposes of the Privacy Act, consent is generally required for collection of health information,[52] unless an exception[53] — such as a "permitted health situation"[54] — applies. This recognizes the need to protect health information from unexpected uses beyond individual healthcare and the important role of health and medical research in advancing public health.

The OAIC has also issued guidelines on handling of health information held in an individual's My Health Record (which contains online summaries of individuals' health information),[55] the privacy aspects of handling healthcare identifiers regulated by the Healthcare Identifiers Act ("**HI Act"**), and the Healthcare Identifiers Regulations ("**HI Regulations"**).[56]

3.3. Privacy codes

Under Part III-B of the Privacy Act, the Information Commissioner can approve and register enforceable codes ("**Codes**") which may be developed either by the Commissioner directly or by entities on their own initiative or at the request of the Commissioner.

---

[47] "**Credit reporting information**" refers to either any personal information (other than sensitive information) about the individual that: (a) is derived by a credit reporting body from credit information about the individual that is held by the body; (b) has any bearing on the individual's credit worthiness; and (c) is used, has been used or could be used in establishing the individual's eligibility for consumer credit (Privacy Act, s 6) or any personal information (other than sensitive personal information) about an individual that falls within the any of the categories of "credit information" in Section 6N of the Privacy Act.

[48] Privacy Act, s 20E(1).

[49] See, generally, Privacy Act, s 20F.

[50] See, generally, Privacy Act, s 20K.

[51] "**Health information**" refers to any of the following: (a) information or an opinion about: (i) the health, including an illness, disability or injury, (at any time) of an individual; or (ii) an individual's expressed wishes about the future provision of health services to the individual; or (iii) a health service provided, or to be provided, to an individual; that is also personal information; (b) other personal information collected to provide, or in providing, a health service to an individual; (c) other personal information collected in connection with the donation, or intended donation, by an individual of his or her body parts, organs or body substances; (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual (Privacy Act, s 6FA).

[52] APP 3.3.

[53] APP 3.4.

[54] APP 3.4(c); Privacy Act, s 16B.

[55] Available at https://www.oaic.gov.au/privacy/other-legislation/my-health-record

[56] OAIC Guidance on Healthcare identifiers available at https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/cr-code

The purpose of a Code is to provide individuals with transparency about how their information will be handled. Codes do not replace the relevant provisions of the Privacy Act but rather, operate in addition to the requirements of the Privacy Act. They are disallowable legislative instruments.

The following Codes are currently in force:

- Privacy (Credit Reporting) Code 2014;[57]
- Privacy (Australian Government Agencies — Governance) APP Code 2017;[58] and
- Privacy (Market and Social Research) Code 2021.[59]

Like the sector- and information-specific laws that intersect with the Privacy Act/APPs, the Codes provide for consent for collection of personal information in specific circumstances.

As mentioned above, the OP Bill mentioned the creation of an **OP Code.** If the Bill is enacted in its current form, then the OP Code would become a registered Code created under the Privacy Act in relation to social media services, data brokers, and other large online platforms and would set out how APPs 3, 5, and 6 about notice and consent are to apply to, or be complied with by, OP Organizations.

3.4. Proposed expansion of the role of consent

The ACCC's DPI Report[60] noted that under the current law, an APP Entity is not required to obtain consent to use or disclose personal information for a primary purpose and that as the term "primary purpose" is not defined, there is no requirement that consumers must be aware of the purpose, or that the purpose must be necessary or beneficial to consumers.

In its broad review of the terms and policies of digital platforms, the ACCC found that digital platforms tend to construe primary purposes broadly and list numerous purposes for collection, use, and disclosure of personal information, only some of which are necessary to provide consumers with a service under their terms of service.

The ACCC concluded that this provided APP Entities with very broad discretion to use and disclose personal information without consent. The ACCC therefore called for stronger consent requirements, which it considered critical to ensuring that consumers have adequate control over use and disclosure of their personal information. While the ACCC acknowledging that consent can be burdensome for consumers and that consent should not be required where use or disclosure occurs in accordance with a contract to which the consumer is a party, the ACCC considered that real and informed consents should always be required where the consumer's personal information is used or disclosed for a purpose that is not in accordance with the consumer's own interests, such as where it is used or disclosed for targeted advertising purposes.

Of course, other protections in the Privacy Act beyond consent would still apply in this case. In this regard the ACCC specifically mentioned that transparency requirements imposed an obligation to implement clear privacy policies, and the activation of privacy-by-default settings, which it found to be currently not common practice in the market.

3.5. Consent and online identifiers

An important question raised in discussion around reform to the Privacy Act is whether to clarify the application of the Privacy Act to technical data and online identifiers.

Australian law does not currently require consent for the placement of cookies or online identifiers, although consent pop-ups are common in practice. Back in 2020, the AGD's Issues Paper noted that it was unclear how the Privacy Act's current definition of "personal information" (i.e., information or an

---

[57] Available at https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/cr-code

[58] Available at https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code

[59] Available at https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/privacy-market-and-social-research-code-2021

[60] DPI Report, page 465.

opinion "about" an identified individual, or an individual who is reasonably identifiable[61]) would generally apply to technical data and online identifiers. The applicability of the Privacy Act to technical information was also called into question following the decision in *Privacy Commissioner v Telstra Corporation Ltd 2017 FCAFC 4 ("**Grubb**")* which held that an individual must be the subject matter of the information for it to be "*about*" an individual and within the scope of the Privacy Act.[62]

The AGD's Discussion Paper proposed to amend the definition of personal information to include information *"related to"* an individual, and to list examples of technical information that could be capable of falling within the definition of personal information.[63] These examples would generally cover "circumstances in which an individual is distinguished from others or has a profile associated with a pseudonym or identifier, despite not being named" and could include an online identifier and one or more specific physical, behavioral, cultural, or economic characteristics of a person. This would bring the processing of technical data and online identifiers, including post-cookie ID initiatives, expressly within the ambit of the Privacy Act.

If the new Federal Government were to adopt these proposals, such clarification would bring the Privacy Act's definition of "personal information" closer to the definitions of equivalent terms in other legislative instruments, such as Australia's **Consumer Data Right** ("**CDR**") legislation[64] and other prominent data protection laws internationally, such as the GDPR.

4. SECTORAL LAWS AND REGULATIONS

There are further additional sectoral laws that intersect with the Privacy Act and the APPs. These laws generally require certain agencies to consult with the OAIC on privacy matters or require the OAIC to perform certain duties or activities. They also make provisions for validity of consent or collection in specific circumstances.

For example:

- Specific provisions of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (**AML/CTF Act**),[65] and the Anti-Money Laundering and Counter-Terrorism Financing Rules[66] require entities regulated by these Acts to comply with the Privacy Act when handling personal information collected for the purposes of compliance with their AML/CTF Act obligations.
- The My Health Records Act 2012 – in addition to establishing the **My Health Record** system – provides for specific modalities of consent collection and withdrawal by individuals' registered treating healthcare providers, including doctors, nurses, and pharmacists across Australia.[67]
- The Treasury Laws Amendment (Consumer Data Right) Act, which instituted the CDR regime, makes special provision for "authorised disclosures or use in accordance with valid consents," by stating that the consumer data rules may include rules about how a "CDR consumer" may give valid consent; what must be included in the consent for it to be valid; what disclosures, uses or other matters a valid consent may cover; and when a consent ceases to be a valid consent.[68]

---

[61] Privacy Act, s 6.
[62] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4, available at https://jade.io/article/518719
[63] Discussion Paper, pages 21 and 26
[64] The CDR was enacted by the Treasury Laws Amendment (Consumer Data Right) Act 2019 *(Cth),* which inserted a new Part IVD the *Competition and Consumer Act 2010* (Cth), available at https://www.legislation.gov.au/Details/C2021C00151 (Note that "CDR consumer" is defined at s 56AI).
[65] Available at https://www.legislation.gov.au/Series/C2006A00169
[66] Available at https://www.legislation.gov.au/Series/F2007L01000
[67] Available at https://www.legislation.gov.au/Details/C2015C00602
[68] Available at https://www.legislation.gov.au/Details/C2019A00063

5. ROLE OF THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER ("OAIC")

5.1. Regulatory guidance

The OAIC has published a number of regulatory guidance documents to help APP Entities to comply with the Privacy Act and other relevant requirements, including consent requirements.[69]

Notably, the OAIC has issued comprehensive guidelines (most recently updated in July 2019) on mandatory requirements under the APPs, how the OAIC interprets the APPs, and matters that the OAIC may take into account when exercising its functions and powers under the Privacy Act ("**APP Guidelines**").[70] These Guidelines are not legally binding[71] but are likely to be highly influential in the OAIC's interpretation of the Privacy Act and the APPs, including the role of consent.[72]

5.2. Public submissions on consent

In 2020, the OAIC publicly welcomed the possibility of reform of the Privacy Act and expressly stated that "issues such as consent requirements, additional privacy rights, accountability measures and the Privacy Act's coverage are fundamental to how we address the privacy challenges of the future."[73] In the same announcement, the Commissioner also identified "enabling privacy self-management" as one of four key elements to support effective privacy regulation over the next decade.

The OAIC's submission[74] in response to the AGD's Issues Paper contains strong language around the need to move away from reliance on consent. For example, the OAIC argued that overuse of notice and consent mechanisms would not address the privacy risks and harms that individuals face in the digital age, that the notice and consent model places an unrealistic burden of understanding the risks of complicated information handling practices on individuals, and that the notice and consent model "does not scale."[75]

In the OAIC's response[76] to the AGD's later Discussion Paper, the Commissioner again specifically emphasized the need for "higher standards of personal information handling to support privacy self-management"[77] and while recognizing the importance of transparency and individual choice and control to the Privacy Act framework, considered such mechanisms limited in their ability to restrain harmful activities and that it would be unrealistic and unfair to expect individuals to consider and understand every collection notice and privacy policy and take steps to protect themselves from privacy harms. [78]

The OAIC further considered that for consent to be meaningful, individuals would need to be provided with genuine choices as to how their personal information will be handled, and that those choices would need to be inherently fair. The OAIC further considered that 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. [79]

---

[69] Available at https://www.oaic.gov.au/privacy/guidance-and-advice
[70] Available at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines
[71] APP Guidelines, A.3.
[72] See APP Guidelines, Chapter B: Key Concepts.
[73] "OAIC welcomes Privacy Act review", available at https://www.oaic.gov.au/updates/news-and-media/oaic-welcomes-privacy-act-review
[74] OAIC Privacy Act Review – Issues Paper Submission by the Office of the Australian Information Commissioner (11 December 2020) ("**OAIC Issues Paper Submission**"), available at https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission
[75] OAIC Issues Paper Submission, paragraphs 5.12 and 5.17.
[76] OAIC, "Privacy Act Review – Discussion Paper Submission by the Office of the Australian Information Commissioner" (23 December 2021) ("**OAIC Discussion Paper Submission**"), available at https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-discussion-paper
[77] OAIC Discussion Paper Submission, page 10.
[78] OAIC Discussion Paper Submission, page 10.
[79] OAIC Discussion Paper Submission, page 10.

6. CONDITIONS FOR CONSENT

6.1. Definition and forms of consent

The Privacy Act provides only a limited definition of "consent" as "express consent or implied consent"[80] and leaves it to the APP Guidelines to specify the four necessary elements of consent,[81] namely that:

- the individual is adequately informed before giving consent;
- the individual gives consent voluntarily;
- the consent is current and specific; and
- the individual has the capacity to understand and communicate consent.

The APP Guidelines appear to only require *express* consent for the collection, use, and disclosure of sensitive personal information.[82] Express consent must be given explicitly, either orally or in writing, and could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.[83]

The APP Guidelines further clarify that implied consent refers to consent which may reasonably be inferred in the circumstances from the conduct of the individual and the APP Entity.[84]

However, the APP Guidelines caution that an APP Entity should not assume that an individual has consented to collection, use, or disclosure of personal information simply on the basis that the collection, use, or disclosure appears to be advantageous to the individual[85] or that the individual did not object to a proposal to handle personal information in a particular way.[86]

In some circumstances, an opt-out option may be sufficient to show implied consent.[87]

6.2. Consent must be voluntary

Under the APP Guidelines, consent is "voluntary" where an individual has a genuine opportunity to provide or withhold consent.[88] Consent is not voluntary where there is duress, coercion, or pressure that could overpower the person's will.[89]

The following factors are relevant to deciding whether consent is voluntary:

- the alternatives open to the individual;
- the seriousness of any consequences; and
- any adverse consequences for family members or associates of the individual, if the individual refuses to consent.[90]

In most jurisdictions, consent given by an employee to an employer is a commonly cited example of consent that may not be "voluntary" due to the hierarchical nature of the relationship. For the most part, this example does not apply to Australian law as private sector "employee records" are excluded from the scope of the Privacy Act.[91] However, it is worth noting that one of the issues under discussion in the current reform process is whether to remove this exemption.

---

[80] Privacy Act, s 6.
[81] APP Guidelines, B.34.
[82] APP Guidelines, B.41.
[83] APP Guidelines, B.36.
[84] APP Guidelines, B.37.
[85] APP Guidelines, B.38.
[86] APP Guidelines, B.39.
[87] APP Guidelines, B.40.
[88] APP Guidelines, B.43.
[89] APP Guidelines, B.43.
[90] APP Guidelines, B.44.
[91] Privacy Act, s 7B(3).

6.3. Consent may be withdrawn

The APPs are silent as to whether consent may be withdrawn.

However, the APP Guidelines provide that an individual may withdraw their consent and require APP Entities to make withdrawal of consent an easy and accessible process and to explain the potential implications of such withdrawal.[92] The APP Guidelines further provide that once an individual has withdrawn consent, an APP Entity can no longer rely on that past consent for any subsequent use or disclosure of the individual's personal information.[93]

6.4. Proposed amendments to refocus consent

The AGD's Discussion Paper proposes to expand the Privacy Act's definition of "consent" to state explicitly that consent should be "voluntary, informed, current, specific, and an unambiguous indication through clear action."[94] This proposal, if adopted, would give legal effect to the OAIC's existing guidance on consent in the APP Guidelines.

6.5. "Bundled consent"

Although the APPs do not expressly prohibit bundled consent, the APP Guidelines warn that bundling consent can undermine the requirement that consent must be "voluntary"[95] and advise APP Entities contemplating use of bundled consent to consider whether:

- it is practicable and reasonable to give the individual the opportunity to refuse consent to one or more proposed collections, uses, and/or disclosures;
- the individual will be sufficiently informed about each of the proposed collections, uses, and/or disclosures;
- the individual will be advised of the consequences (if any) of failing to consent to one or more of the proposed collections, uses and/or disclosures.[96]

Following criticism of bundled consent in the DPI Report,[97] practitioners expect that there to be increased focus on unbundling consents from other consents as well as from provision of services.

7. CONSENT FOR SPECIAL CATEGORIES OR USES OF DATA

7.1. "Sensitive information" under the Privacy Act

The Privacy Act identifies, and imposes more stringent requirements on, several categories of "sensitive" personal information, which are ordinarily seen as highly personal, and which have the potential to give rise to unjustified discrimination.[98] These categories comprise the following:

- information or an opinion about an individual's:
  - racial or ethnic origin;
  - political opinions;
  - membership of a political association, professional or trade association, or trade union;
  - religious beliefs or affiliations;

---

[92] APP Guidelines, B.51
[93] APP Guidelines, B.51
[94] Discussion Paper, Proposal 9.1.
[95] APP Guidelines, B.45.
[96] APP Guidelines, B.46.
[97] See, in particular, DPI Report, section 7.4.3.
[98] For Your Information: Australian Privacy Law and Practice (ALRC Report 108), *Australian Law Reform Commission*, 12 August 2008, available at http://www.austlii.edu.au/au/other/alrc/publications/reports/108/

  - philosophical beliefs;
  - sexual orientation or practices;
  - criminal record, that is also personal information;
- health information about an individual;
- genetic information about an individual that is not otherwise health information;
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; and
- biometric templates.[99]

The original categories in the Privacy Act closely resembled the special categories of personal data in Article 8 of the EU's Data Protection Directive (the predecessor to the GDPR). However, following recommendations in two reports of the Australian Law Reform Committee ("**ALRC**"), the Privacy Act's categories were subsequently expanded to include genetic information, biometric information, and biometric templates.

There is no flexibility in these categories in that the Privacy Act does not contain specific provisions that would enable the government or regulator to designate additional categories of information as "sensitive" through subsidiary legislation or regulations. However, the OAIC, like all privacy regulators, has a measure of latitude in how it interprets each of the categories listed in the Privacy Act. For instance, the APP Guidelines indicate that information may be sensitive where it "clearly implies" one of the prescribed categories[100]

Sensitive information is subject to a number of additional protections in the Privacy Act.

Unless an exception applies, an APP Entity may only collect sensitive information[101] or use or disclose such information for the purpose of direct marketing[102] after obtaining express consent from the individual concerned. The APPs also apply more stringent requirements to disclosure of sensitive information.[103]

7.2. Possible expansion of the categories of "sensitive information"

The Issues Paper and subsequent Discussion Paper have both raised the question of whether to expand the definition of sensitive information to encompass other types of personal information, including financial information, location data, and other forms of biometrics.

a. Financial information

Financial data, particularly for taxation and creditworthiness purposes, is currently governed by parts of the Privacy Act but is not considered "sensitive information" under Section 6.

The reform of the Privacy Act has raised the possibility of including financial information in the Privacy Act's definition of "sensitive information."

The OAIC submission in response to AGD's Discussion Paper notes that financial information is commonly seen as sensitive by the community, that its misuse has a clear potential to cause economic and other harms to individuals, and that the community concern around financial information is clearly reflected in OAIC guidance, which requires higher compliance standards for handling of this class of information.[104] While the OAIC considers that financial information should often be subject to increased protections given the harms that may arise for individuals if this data is misused, it did not recommend legally categorizing financial information as sensitive information under the Privacy Act.[105] Rather, the

[99] Privacy Act, s 6(1).
[100] APP Guidelines, B.139.
[101] APP 3.3(a).
[102] APP 7.4.
[103] APP 6.2.(a).
[104] OAIC Discussion Paper Submission, section 2.32.
[105] OAIC Discussion Paper Submission, section 2.33.

OAIC has expressed the view that imposing additional consent requirements on the handling of financial information may have limited impact as a privacy protection in the majority of circumstances, and that the flexibility of the APPs, enhanced through reforms (e.g., to the fairness and reasonableness obligations) provides a more appropriate and proportionate regulatory response.[106]

b. Location data

Currently, location data is not specifically restricted under Australian law. However, the reform of the Privacy Act presents an opportunity to discuss whether location data should be classified as "sensitive information" under the Privacy Act.

In their response to the Discussion Paper, the OAIC noted that the collection, use, and disclosure of information about where a person is or has been has significant privacy risks as this information can be used to infer sensitive information, such as religious or health information, may be very difficult to anonymize, and can even create safety risks, particularly for vulnerable individuals.[107] The OAIC further noted that the Australian community shares these concerns: approximately two-thirds of Australians surveyed were uncomfortable with online businesses tracking their locations; nearly half of Australians surveyed considered location tracking to be one of the biggest privacy risks today; but only 25% of Australians surveyed felt that their location information was well protected by law.[108]

However, the OAIC does not consider that categorizing location data as sensitive information is the best approach to protecting this type of information.[109] In the OAIC's view, other proposals will provide stronger protection, while also ensuring that the existing categories of sensitive information retain their consistent focus on information that may lead to unjust discrimination.[110]

c. Children's information

Children's personal information is not considered sensitive information *per se* under the Privacy Act.

Under the current law, an organization or agency handling the personal information of an individual under the age of 18 must decide if the individual has the capacity to consent on a case-by-case basis.[111] If it is impractical for an organization or agency to assess the capacity of individuals on a case-by-case basis, then, as a general rule, an organization or agency may presume that an individual over the age of 15 has capacity.[112]

However, if the OP Code is adopted in its current form, organizations would be required to follow stricter rules regarding the handling of the personal information of children and other vulnerable groups, with specific rules for social media services. In particular, organizations would be required to take reasonable steps to verify the age of individuals who use social media services; ensure that the collection, use, or disclosure of children's personal information is fair and reasonable in the circumstances, having regard to the best interests of the child; and obtain express consent from a parent or guardian before collecting, using, or disclosing personal information of a child under the age of 16.

In the Discussion Paper, the AGD also recommends that the Privacy Act should be amended to require a parent or guardian to provide consent where a child is under the age of 16. However, the AGD is seeking additional feedback on whether APP Entities should be permitted to assess capacity on an individualized basis where it is practical to do so.[113]

---

[106] OAIC Discussion Paper Submission, sections 2.35 and 2.36.
[107] OAIC Discussion Paper Submission, section 2.37.
[108] OAIC Discussion Paper Submission, section 2.38.
[109] OAIC Discussion Paper Submission, section 2.39.
[110] OAIC Discussion Paper Submission, section 2.39.
[111] APP Guidelines, B.59.
[112] APP Guidelines, B.58.
[113] Discussion Paper, page 104.

8. CONSENT FOR CROSS-BORDER DATA TRANSFERS

8.1. Operation of APP 8

APP 8 governs the cross-border disclosure of personal information. Chapter 8 of the APP Guidelines (Cross-border disclosure of personal information) further outlines how the OAIC will interpret APP 8.[114]

By default, APP 8 requires an APP Entity that intends to disclose personal information to an overseas recipient to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs (other than APP 1) in relation to that information.[115] If an entity discloses personal information about an individual to an overseas recipient, and APP 8.1 applies to the disclosure of the information, then the entity is accountable for any acts or practices of the overseas recipient that would breach the APPs in relation to the information.[116]

The accountability approach in APP 8 tracks the same principle in the APEC Privacy Framework in 2004, Information Privacy Principle IX (Accountability), itself derived from the accountability principle from the OECD Privacy Guidelines of 1980.

Consent functions as an exception to the accountability principle in APP 8, in ways very similar to the consent exception in EU GDPR. More specifically, APP 8.2(b) permits an APP Entity to disclose personal information to an overseas recipient if the following conditions are met:

- the APP Entity expressly informs the individual that the information will not be protected in a substantially similar way, and
- after being so informed, the individual consents to the disclosure.[117]

Note that the four key elements of consent mentioned above apply here.[118]

The APP Guidelines note that consent is not required before every proposed cross-border disclosure and that an entity can obtain an individual's consent to disclose a particular kind of personal information for the same purpose on multiple occasions.[119]

8.2. AGD proposal: removing the consent exception in APP 8

It is worth noting that the AGD has recommended removing the informed consent exception in APP 8.2(b) in the current reform process.[120]

In this regard, AGD noted that some submissions received in response to the Issues Paper expressed the view that the consent exception places an unfair expectation on consumers to understand the implications of disclosure (i.e., if consumers consent to an overseas disclosure, their personal information may not be subject to any privacy protections).

The AGD recognizes that removing the express consent exception could increase the regulatory burden on entities seeking to disclose personal information overseas. However, it also notes that the extent of reliance by business on this exception is unclear and that the various alternatives which it proposes to implement instead would make it easier for entities to fulfill their accountability obligations.

In fact, in practice, most APP Entities take steps to comply with the accountability principle in APP 8.1 — few appear to take the legal and reputational risks involved in relying on the exception in APP 8.2(b).[121]

---

[114] APP Guidelines, Chapter 8. On the operation of this Chapter, see Peter Leonard, "Australia" in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, May 2018), pages 17-61, available at https://abli.asia/PUBLICATIONS/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia

[115] APP 8.1.

[116] Privacy Act, s 16C.

[117] APP Guidelines, 8.27.

[118] See "CONDITIONS FOR CONSENT" above.

[119] APP Guidelines, 8.32.

[120] Discussion Paper, pages 162-163.

[121] Peter Leonard, "Australia" in *Regulation of Cross-Border Transfers of Personal Data in Asia* (Asian Business Law Institute, May 2018), page 50.

9. TRANSPARENCY AND NOTICE

Currently, APP 1 establishes a general requirement that every APP Entity should have a privacy policy that is kept up to date with regard to the entity's processing activities and includes certain specified information about those activities. Specifically, APP 1 requires that privacy policies state:

- the kinds of personal information the entity collects and holds;[122]
- how information is collected and held;[123]
- the purposes for which the entity collects, holds, uses, and discloses information;[124]
- how an individual may access, and seek correction to, personal information held by the entity; [125]
- how an individual may complain about a breach;[126]
- whether the entity is likely to disclose personal information to overseas recipients;[127] and
- if overseas disclosure is likely, the countries in which overseas recipients are likely to be located.[128]

APP 5.1 requires that at the time of collection, or as soon as is practicable after collection, an APP Entity must take such steps (if any) as are reasonable in the circumstances, to notify, or otherwise ensure that the relevant individual is aware of certain matters.

According to the APP Guidelines, where consent is required (e.g., for collection of sensitive information), the APP Entity must ensure that consent is "informed" – meaning that:

> "*[a]n individual must be aware of the implications of providing or withholding consent, for example, whether access to a service will be denied if consent is not given to collection of a specific item of personal information. An APP Entity should ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent. The information should be written in plain English, without legal or industry jargon*."[129]

In practice, whether consent is "informed" has often been considered in terms of both the privacy policy requirements under APP 1 and notice requirements under APP 5. However, these two sets of requirements are conceptually different, and the OAIC has explicitly stated in several cases that a privacy policy is not a mechanism by which to provide notice under APP 5. Rather, a privacy policy is simply a transparency mechanism.[130]

In the public consultation on reform to the Privacy Act, a large number of submitters to the AGD's Issues Paper expressed the view that notice is an important transparency mechanism in the Privacy Act and a key component of any privacy reform (irrespective of the role of consent) as it is pivotal in communicating to individuals how their personal information is being handled.[131]

However, the AGD noted a common concern that APP Entities currently have significant discretion under APP 5 as to whether individuals are notified about the collection of their personal information and how that notice is provided.[132] Submissions indicated particular concern about the heightened privacy risks to consumers stemming from the use and disclosure of personal information collected by third parties without the awareness of the individual.

The AGD thus proposed:

---

[122] APP 1.4(a).
[123] APP 1.4(b).
[124] APP 1.4(c).
[125] APP 1.4(d).
[126] APP 1.4(e).
[127] APP 1.4(f).
[128] APP 1.4(g).
[129] APP Guidelines, B.47.
[130] See, for example, the OAIC's determination in the 7-Eleven case, available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html (at paragraph 95).
[131] Discussion Paper, page 67.
[132] Discussion Paper, page 68.

- to introduce an express requirement in APP 5 that privacy notices must be clear, current, and understandable, with specific mention of the importance of these requirements "*for any information addressed specifically to a child*;"[133]
- that the "APP 5 notices" be limited to specific matters (identity and contact details of the entity collecting the personal information; types of personal information collected; purpose(s) for collection and use; types of third parties to whom the entity may disclose the personal information, etc.), and specify the location of the entity's privacy policy which sets out further information;[134] and
- noting broad support, that standardized privacy notices could be considered in the development of an APP code, such as the OP Code, including standardized layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardized notices.[135]

Other proposals specifically relate to:

- **notice for targeted advertising and profiling**: the AGD recommended that the use or disclosure of personal information for the purpose of influencing an individual's behavior or decisions must be a primary purpose notified to the individual when their personal information is collected. APP Entities would also be required to include 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 behavior or decisions and if so, the types of information that will be used, generated or inferred to influence the individual."
- **notice for online marketing via third parties**: an APP Entity must disclose when 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.
- **Automated decision-making** (**ADM**): privacy policies should include information on whether personal information will be used in automated decision-making which has a legal, or similarly significant, effect on people's rights.[136]

10. SANCTIONS AND ENFORCEMENT

Strengthening the regulatory and enforcement powers of the OAIC is one of the key themes in the reform of the Privacy Act.[137]

However, without waiting for the hypothetical reinforcement of its intervention capacities, the OAIC has recently adopted a more assertive approach to enforcement by relying on its international cooperation faculties in the Facebook/Cambridge Analytica case and on complaints-based cases.

10.1. OAIC v Facebook

In 2020, the OAIC lodged proceedings against Facebook in the Federal Court, alleging the social media platform has committed serious and/or repeated interferences with privacy in contravention of the Privacy Act in the context of the Cambridge Analytica scandal.[138]

Central to the proceedings was the argument that Facebook (now known as "Meta") had breached APP 6 by disclosing the data of Australian users of the "This is Your Digital Life" app for a purpose other than the purpose for which the information was collected, in breach of the Privacy Act.

The OAIC argued, based on APP 6, that if Facebook held personal information that was collected for a particular (primary) purpose, it could not disclose that personal information for a secondary purpose unless it had the individual's consent or certain exceptions applied.

---

[133] Discussion Paper, pages 68-69.
[134] Discussion Paper, pages 69-70.
[135] Discussion Paper, pages 71-72.
[136] Discussion Paper, pages 13-14.
[137] Discussion Paper, page 173.
[138] Concise statement available at https://www.oaic.gov.au/__data/assets/pdf_file/0020/6482/facebook-federal-court-concise-statement.pdf

However, OAIC argued that Facebook had disclosed those individuals' personal information to the "This is Your Digital Life" app for a different purpose than the primary purpose of enabling those individuals to build an online social network with other users on the Facebook website. The information was exposed to the risk of being disclosed to Cambridge Analytica and used for political profiling purposes, and to other third parties. It was further established that despite the fact that only 53 Australians used the "This is Your Digital Life" app, the personal information of more than 300,000 Australian users of Facebook was harvested. The OAIC argued that Facebook had breached the Privacy Act on each occasion on which it disclosed the personal information of the affected Australian individuals to the "This is Your Digital Life" app.

The other basis of the claim was that it was difficult for users to know they needed to change their default settings to limit disclosures, and that the design of Facebook "made it difficult for users to exercise consent or control over the disclosure of their personal information to apps." This may have broad ramifications for the widespread use of default 'on' settings, bundled consents and broadly worded privacy notices.

Proceedings are still ongoing in the case.

10.2. OAIC determinations in the 7-Eleven, Clearview AI, and Australian Federal Police cases

The OAIC has issued determinations in cases involving use of use of facial recognition technology by 7-Eleven,[139] Clearview AI,[140] and Flight Centre.[141] In each of these cases, the OAIC considered the application of the Privacy Act's consent provisions in practice and found that the organizations in question had not obtained valid consent in compliance with the Privacy Act. The issues raised in relation to the scope of privacy laws are applicable to many other types of data and data use practices, including online behavioral advertising, customer profiling and targeted marketing.[142]

11. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT SUBJECT TO A RISK IMPACT ASSESSMENT

11.1. Reducing reliance on consent: policy options considered (fair and reasonable test, legitimate interests)

Throughout public discussions on review of the Privacy Act, an observation shared by the overwhelming majority of contributors has been that consent is overused. Various different policy options to remedy this situation have been considered at different stages of the process. These variations are worth detailing as they are relevant to comparable discussions in other APAC jurisdictions.

11.2. Expanding v. refocusing consent requirements

A major divergence in thinking around reforms to the Privacy Act's consent provisions is between those who support extending the use of consent as a lawful basis for handling personal information in the first place, and those who support reducing the role of consent by reaffirming the conditions for valid consent.

---

[139] Commissioner initiated investigation into 7-Eleven Stores Pty Ltd [2021] AICmr 50, available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html

[140] Commissioner initiated investigation into Clearview AI, Inc. [2021] AICmr 54, available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html

[141] Flight Centre Travel Group (Privacy) [2020] AICmr 57, available at http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2020/57.html

[142] Anna Johnston, "OAIC determinations shed light on when data is regulated as 'personal information,'" *Salinger Privacy blog* (11 April 2022), available at https://www.salingerprivacy.com.au/2022/04/11/oaic-determinations-blog/

In 2019, the ACCC Digital Platforms Inquiry recommended that the consent requirement should be expanded so that consent would be required for any collection, use, or disclosure of personal information, subject to exceptions where collection, use, or disclosure is necessary for the performance of a contract, a legal requirement, or public interest reason.[143]

In contrast, the OAIC and other entities which submitted responses to the AGD's Issues Paper and Discussion Paper underlined the limited merits of this approach and highlighted that there is significant opposition to expanding consent requirements to include more types of processing activity in favor of other policy options.

Critiques of privacy self-management mechanisms like consent, particularly as applied to internet enabled services, mainly focus upon:

- the impracticability of individuals reading and understanding privacy policies and requests for consent, given the volume and complexity of privacy policies and collection notices;
- "consent fatigue," leading to users simply clicking the 'I agree' button without perusing or thinking about privacy-related terms;
- how consent places a burden on individuals to understand and consider complex data handling practices, unknown privacy harms that may materialize in the future and the many purposes for which their personal information may be handled, rather than allowing them to be confident that the purpose falls within appropriate confines (for example, that the collection, use or disclosure will not be harmful to the individual);
- how consent is only meaningful where the individual has a voluntary choice; this is not the case where individuals feel resigned to consenting to the use of their information to access online services, as they do not consider there is any alternative.[144]

In the words of one submitter, *"'beefing up' consent of itself is unlikely to be an effective regulatory tool to reduce the range of current privacy invasive acts and practices to the point at which the volume of requests for consent become manageable for individuals."*[145]

Although extending regulatory requirements to obtain consent should cause some reduction in the range and number of current privacy invasive acts and practices, the argument goes, *"that range and number is unlikely to reduce to a point where the volume of requests for consent becomes manageable for individuals. Until that point is reached, consent fatigue, and gaming by regulated entities of consent fatigue, are likely to remain characteristic features of online data privacy."*

This theme was discussed in detail during the FPF APAC inaugural event titled "Exploring trends: From consent-centric frameworks to responsible data practices and privacy accountability in Asia Pacific, organized jointly with ABLI on September 26, 2021. As per the event report published on the FPF website, in the view of one of the panelists,

> *"the situation in Australia (...) is that consent is over-relied on, but also under-enforced. There is guidance from the OAIC and there is case-law to back up that guidance, that consent in Australian law is similar to the GDPR: it cannot be bundled up with other things, it cannot be included in mandatory Terms and Conditions, in a Privacy Policy, it cannot even be "opted out" – consent as a lawful basis on which to collect, use or disclose personal information has to be the customer's clear "opt in" choice, made freely, separate from all other choices. However, the law is under-enforced, and so it is still very common to see business practices which follow a model of "bury the customer in fine print and make them*

[143] DPI Report, page 24.

[144] See the summary of submissions to the Issues Paper in the Discussion Paper, at page 75.

[145] Peter Leonard, "Notice, Consent and Accountability: addressing the balance between privacy self-management and organizational accountability Paper for the Office of the Australian Information Commissioner" (June 2020), page 13, available at https://www.oaic.gov.au/assets/about-us/access-our-information/foi-disclosure-log/foireq20-00220.pdf

> *agree to something we know they won't even read", and then claim that the customer has consented to something.*"[146]

From this perspective, in the context of the Privacy Act Review, the general direction seems to be in favor of *strengthening* the legal test for what constitutes a valid consent, while at the same time *reducing* the frequency with which, or circumstances under which, anyone is asked for consent in the first place.

The AGD's Discussion Paper also references the opinions of various stakeholders on how consent should be used for the collection and processing of personal information – specifically, that consent is most appropriate in "high privacy risk" situations, and not in "routine personal information handling," with the concern that blanket consent requirements may "reduce consent to a tick-box exercise."[147]

11.3. "Legitimate interests" v. "fair and reasonable" test

While expressing a clear intention to reduce reliance on the "notice and consent" model of privacy regulation, the AGD's Discussion Paper also subscribes to the approach of imposing stricter limits on collection, use, and disclosure of personal information by including "baseline" protections in the Privacy Act.

However, submitters to the AGD's Issues Paper and commenters have expressed differing views on how minimum acceptable standards for how personal information is collected, used, and disclosed should be set (irrespective of consent being obtained).

Two alternatives were commonly raised, which would consist in the introduction in the Privacy Act of:

- a lawful basis for collection, use, and disclosure modeled on the "legitimate interests" test under Article 6(1)(f) GDPR; or
- the application of a "fair and reasonable" test to collection, use and disclosure of personal information, on top of existing rules around collection necessity and purpose limitation.[148]

While noting that many industry stakeholders had raised the GDPR's legitimate interest basis for processing personal data as a desirable basis for the handling of personal information in Australia, the Discussion Paper eventually opted for the "fair and reasonable" test instead.

Facially, a merit of applying a fair and reasonable test to all processing activities covered by the Privacy Act is that this test extends pre-existing concepts of fairness and reasonableness in the Privacy Act, such as the existing requirement in APP 3.5 that personal information may only be collected "by fair and lawful means." Extending this requirement may help to prevent unfair and unreasonable activities that may result in harms to individuals as the existing APP 3.5 may not prevent other inappropriate practices after collection.

The main argument put forward by the AGD for favoring a "fair and reasonable" approach over the "legitimate interests" approach in EU GDPR is that the Privacy Act does not confer a right to privacy on individuals, but rather protects against arbitrary interferences with privacy as derived from Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**). The AGD therefore took the view that importing a rights-based requirement in Australia's data protection framework may "present difficulties."[149]

Moreover, the AGD noted the ACCC's criticism of the "legitimate interests" approach that "there is considerable uncertainty and concern surrounding the relatively broad and flexible definition of the "legitimate interests" basis for processing personal information under the GDPR" in that the "impact" to an individual's interests, rights, and freedoms may be interpreted broadly in a commensurate manner.[150]

---

[146] Anna Johnston, quoted in FPF Event Report, "Exploring trends: From "consent-centric" frameworks to responsible data practices and privacy accountability in Asia Pacific," available at https://fpf.org/blog/event-report-from-consent-centric-frameworks-to-responsible-data-practices-and-privacy-accountability-in-asia-pacific/

[147] Discussion Paper, pages 74-76.

[148] Discussion Paper, page 83.

[149] Discussion Paper, page 83.

[150] DPI Report, page 466.

11.4. Factors to be applied in the "fair and reasonable" test

Despite a difference in approach between the two concepts, however, many factors that weigh in the balancing test in "legitimate interests" in EU GDPR may also apply to the "fair and reasonable" test if it is incorporated in the Privacy Act.

The proposed test could apply to the existing APPs that regulate collection, use and disclosure, and include a number of legislated factors to assist entities in determining whether a particular collection, use, or disclosure falls within acceptable parameters. The OAIC would have to consider these factors when determining whether acts or practices are fair and reasonable, in context and depending on the circumstances.

The notion of fairness in the data protection law would require entities to "take account of the interests and reasonable expectations of data subjects", and handle personal information in a manner that "does not, in the circumstances, intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity."[151] Such a granular assessment seems very comparable to the "balancing test" which data controllers must apply when they rely on "legitimate interests" for compliance with EU GDPR Art 6(1)(f).

On the whole, contributors to the AGD consultation generally highlighted that any exception to consent for "legitimate interests," "legitimate uses," or "compatible data practices" should only operate and allow a regulated entity to collect, handle, or disclose personal information about individuals if the processing:

- is aligned with the ordinary expectations of affected individuals;
- has regard to transparent privacy policies and notices; and
- is not harmful to direct interests of data subjects.

In practice, therefore, the differences between these options (legitimate interests v. fair and reasonable test) are unlikely to be such that they would oppose actions of convergence between the legal systems implementing them.

12. COLLECTING, USING, AND DISCLOSING DATA WITHOUT CONSENT IN OTHER CIRCUMSTANCES DEFINED BY LAW

"Permitted General Situations" and "Permitted Health Situations" are both alternatives to obtaining consent for certain kinds of collection, use, or disclosure of personal information. There are also standing exceptions for certain enforcement bodies and enforcement purposes, which will not be considered here.

The Discussion Paper does not consider the application of these exceptions, nor how they would be impacted by the introduction of an overarching "fair and reasonable" test in the Privacy Act. However, it is important that the application of such "permitted situations" is not automatic and remains subject to a form of balancing test.

12.1. "Permitted general situations"

The information handling requirements imposed by some APPs do not apply if a "permitted general situation" exists.[152] This exception applies in relation to the collection of sensitive information–including consent requirements (APP 3), the use or disclosure of personal information (APPs 6 and 8) and the use or disclosure of a government-related identifier (APP 9). It is nevertheless open to an APP Entity to comply with the APP requirements even if such an exception applies.

There are seven permitted general situations listed in Section 16A of the Privacy Act:

---

[151] Professor Lee Bygrave, "Core Principles of Data Protection Law" (2001) 7(9) Privacy Law and Policy Reporter 169, cited by the Discussion Paper at page 84.

[152] Privacy Act, s 16A.

- lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d));
- taking appropriate action in relation to suspected unlawful activity or serious misconduct (see APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d));
- locating a person reported as missing (see APPs 3.4(c), 6.2(c) and 8.2(d));
- asserting a legal or equitable claim (see APPs 3.4(c) and 6.2(c));
- conducting an alternative dispute resolution process (see APPs 3.4(b) and 6.2(c));
- performing diplomatic or consular functions – this permitted general situation only applies to agencies (see APP 3.4(b), 6.2(c) and 8.2(d)); and
- conducting specified Defence Force activities – this permitted general situation only applies to the Defence Force (see APP 3.4(b), 6.2(c) and 8.2(d)).

Each of these permitted general situations is discussed generally in Chapter C of the APP Guidelines, which also provide specific examples relevant to each APP.

12.2. "Permitted health situations"

The information handling requirements imposed by APP 3 and APP 6 do not apply to an organization if a "permitted health situation" exists.[153] This exception applies to the collection, use, or disclosure of health information or genetic information by an organization.

There are five permitted health situations listed in Section 16B of the Privacy Act:

- the collection of health information to provide a health service (s 16B(1)) (see APP 3.4(c));
- the collection of health information for certain research and other purposes (s 16B(2)) (see APP 3.4(c));
- the use or disclosure of health information for certain research and other purposes (s 16B(3)) (see APP 6.2(d));
- the use or disclosure of genetic information (s 16B(4)) (see APP 6.2(d)); and
- the disclosure of health information for a secondary purpose to a responsible person for an individual (s 16B(5)) (see APP 6.2(d)).

Each of these permitted health situations is discussed generally in Chapter D of the APP Guidelines, which also provide specific examples relevant to each APP.

12.3. Rule of interpretation

Guidance from the OAIC makes clear that the interpretation of each of these "permitted situations" is strict and reflects lawmakers' goal of balancing privacy against the public interest in each situation. Exceptions generally rely on the necessity test and are explicitly spelled out in the statute and accompanying guidance. The terms "reasonably believes" and "necessary" are discussed in Chapter B (Key concepts) of the APP Guidelines.

For instance:

- Consent will not be required for collection or use an individual's information if it is necessary for "lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety," only upon the dual conditions that:
  - it is "unreasonable or impracticable" to obtain the individual's consent to the collection, use, or disclosure, and an APP Entity should be able to point to one or more clear reasons that make it unreasonable or impracticable to obtain an individual's consent; and

[153] Privacy Act, s 16B.

  - the entity "reasonably believes" that the collection, use, or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A-1).

- The APP Entity must have a "reasonable basis for the belief," and not merely a genuine or subjective belief, and it is the responsibility of an entity to provide justification for this reasonable belief.
- An organization can collect health information about an individual without consent if the collection is "necessary for research relevant to public health or public safety, the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service, and (among other reasons) "it is impracticable to obtain the individual's consent." The OAIC underlines that it is the responsibility of an organization relying on this permitted health situation to be able to justify why it would be impracticable to obtain an individual's consent. The need to incur extra expense or doing extra work to obtain consent would not, by itself, make it impracticable to obtain consent.

ASIAN BUSINESS LAW INSTITUTE

The Asian Business Law Institute (ABLI) is a permanent think tank based in Singapore that initiates, conducts and facilitates research with a view to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws.

1 SUPREME COURT LANE | LEVEL 6 | SINGAPORE 178879 ABLI.ASIA | INFO@ABLI.ASIA

FUTURE OF PRIVACY FORUM

The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

1350 EYE STREET NW | SUITE 350 | WASHINGTON DC 20005 FPF.ORG | INFO@FPF.ORG