HERBERT SMITH FREEHILLS

Australian privacy law reform and review announced

On 12 December 2019, the Australian Government announced its response to the Australian Competition & Consumer Commission's (**ACCC**) Digital Platform Inquiry (**the Inquiry**). Despite the Inquiry's name, only 1 of the 11 recommendations in the report about data practices is targeted at digital platforms. While we discuss the broader issues raised by the Government's response to the Inquiry here, this article focuses specifically on the impacts for Australian privacy law. Those impacts include a set of proposed initial reforms for 2020, along with a more expansive review of privacy law to be completed in 2021.

Key points

Problematic data practices

- The ACCC recommendations, following the Inquiry and another review into customer loyalty schemes (see our briefings here and here), are borne of concerns about 'problematic data practices', such as online tracking for targeted advertising and third party data sharing.

Economy wide impact

- The proposed privacy changes could have implications across all businesses, including small businesses currently not covered by the Privacy Act.
- Recognising the potential for whole of economy effects, the Government announced it would prioritise so called social media privacy reforms, including the introduction of a binding privacy code for digital platforms, and the introduction of tougher penalties, however the other recommendations will require further consideration and engagement (see timeline below).

OAIC influence

- The recommendations are influenced by some Office of the Australian Information Commissioner's (**OAIC**) existing guidance or its submissions to the ACCC during the Inquiry, reflecting the close levels of cooperation between the two regulators.

Prescriptive rules or principle based approach

- The recommended adoption of detailed and prescriptive rules constitutes, arguably, a departure from the technology-neutral high level principle-based approach, which currently underpins the Australian privacy regime.
- Public consultation about the proposed changes confirmed there is a general satisfaction with this approach, however the Government, in its response, states it is also appropriate to consider how the scope of the Privacy Act applies and fits in the digital age and the adequacy of enforcement arrangements.

Holistic approach

- The ACCC's proposed recommendations relating to data are not limited to the Privacy Act but extend to the Australian Consumer Law (**ACL**), consistent with recent enforcement actions by the ACCC[2] and overseas regulators[3], which have treated data privacy as an issue of consumer protection law.

Broader reform

- In addition to the specific amendments to the Privacy Act, several proposed areas for review as part of a broader reform, such as certification schemes and minimum standards of privacy protection, aim to address the limits of a consent based model, by shifting more of the responsibility onto the entities handling personal information.

---

1 The Australian Law Reform Commission, For Your Information: Australian Privacy Law and Practice, ALRC Report 108, 12 August 2008 (ALRC 2008 Report) contained a total of 295 recommendations. The Government at the time responded to 197 of the recommendations, accepting 141 in full or principle (and 34 with qualifications), many of which resulted in amendments to the Privacy Act, including the introduction of the Australian Privacy Principles which took effect in 2014. In its first stage response ('Enhancing National Privacy Protection, Australian Government First Stage Response to ALRC Privacy Report 108') dated October 2009 (First Stage Response), the Government announced it would consider the remaining 98 recommendations in a second stage response. The publication of this second stage response was delayed, and subsequent governments have not picked it up.

2 The ACCC has recently brought cases against online platform Health Engine for misleading and deceptive conduct relating to sharing of patient's personal information with third party insurance brokers and more recently against Google.

3 For example, the US Federal Trade Commission, has, in the absence of federal privacy legislation, been enforcing consumer protection regulation against mishandling of consumer data.

HERBERT SMITH FREEHILLS

Challenges and opportunities ahead

Expanded coverage

- If introduced, the creation of a statutory cause of action for privacy or removal of the current exemptions for employee records and small business, could have considerable impact for businesses and practices that are currently not covered by the Privacy Act.

Cost of compliance

- Reinforced penalties and new avenues of action, combined with increased resources and powers for the OAIC[4] and greater involvement by the ACCC are likely to lead to more actions being brought in relation to data practices by the regulators or consumers.

Increased data flows

- The ACCC, as the ALRC before it, expects the reform will increase the potential for data portability within Australia and overseas, and in particular, assist in achieving EU 'adequacy' status.
- This could create opportunities for Australian businesses.

Global companies

- Australian companies that have already taken steps towards GDPR compliance will likely require less changes to implement the proposed reforms.
- Differences will remain between the two regimes. To navigate different data protection laws, companies may decide to reform their entire data handling practices to comply with the highest standards, or set up patchwork protections for different jurisdictions.

4 In March, the Government announced measures to empower the OAIC to issue administrative penalties of up to $63,000 for bodies corporate and $12,600 for individuals for failure to cooperate with efforts to resolve minor breaches and to publish prominent infringement notices. The latest budget handed down on 2 April 2019 allocated $25.1 million over 3 years to "facilitate timely responses to privacy complaints and to support strengthened enforcement action".

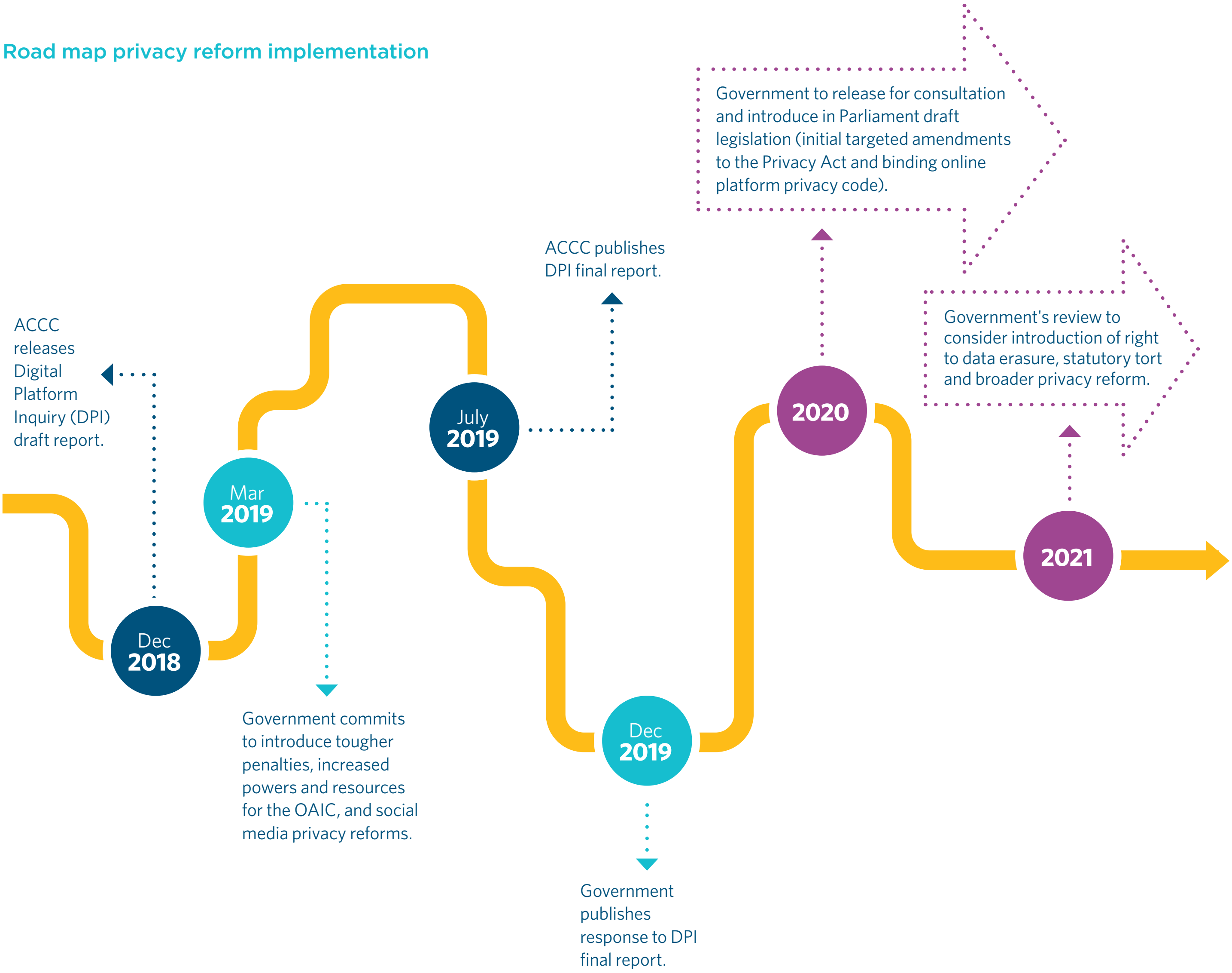
HERBERT SMITH FREEHILLS

Next steps: A staggered implementation process

The Government's response to the Digital Platform Inquiry Final Report outlined a roadmap for actions. While the Government has committed to legislate on some of the recommended amendments to the Privacy Act rapidly, most of the privacy recommendations will require further consultation, and the broader review of Australian privacy law will take another 18 months. Many details on the implementation process remain uncertain.

Given the scale of potential change ahead, and as regulators become increasingly proactive in enforcing existing privacy and consumer protection laws in connection with data practices, Australian businesses should not be complacent. They should stay up-to-date with the reform process, make submissions to put their position and keep aware of the ways enforcement and interpretation of current laws is shifting.

Road map privacy reform implementation



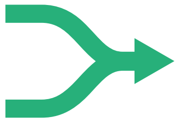
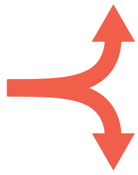
Detailed analysis of the proposed recommendations

Keys

GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR AND/OR THE ARLC 2008 REPORT
Support. Legislation to be introduced in 2020.	Divergence
Support in principle, subject to consultation in 2020.	Some alignment. Differences remain.
To be subject to further review in 2020-2021.	Alignment.

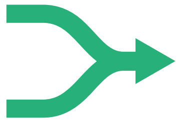
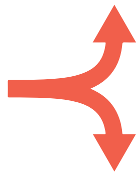
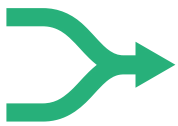
ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
Existing or immediate Government commitments ACCC recommendations which the Government intends to specifically consult and/or legislate on in 2020.				
Increasing penalties for breach of the Privacy Act	Current: $2.1 million Proposed: the greater of: • $10 million • 3 times the value of the benefit received, or • 10% of domestic turnover in the preceding 12 months.		Proposed amounts remain below the GDPR levels (the higher of €20 (A$33) million, or 4% of annual worldwide turnover of the preceding financial year) for the most serious infringements (including conditions for consent, lawfulness or processing and data subject rights).	Report led to the introduction of the $2.1 million penalty in the Privacy Act.

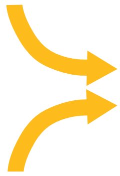
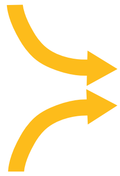
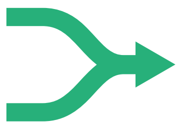
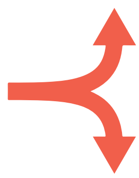
HERBERT SMITH FREEHILLS

ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
Broadening the definition of personal information (PI)	Moving from whether information is about an individual to whether it relates to an individual. The ACCC anticipates this amendment will clarify that PI encompasses all technical data that may be used to identify an individual, a point which was questioned after a 2017 Federal Court case which reasoned that data is only PI if a person is the actual subject matter of that data.[1] In that case, network metadata not sufficiently connected to an individual was not found to constitute PI, regardless of whether it can be linked with other data to identify that individual.	 Definition should capture technical data and other online identifiers that raises privacy concerns but not impose an unreasonable regulatory burden on industry.	 The 'relating to' approach would bring Australia closer to the GDPR definition of 'personal data'. The European Court of Justice has previously ruled that dynamic IP addresses which can be used to identify an individual when linked with other data sets (including data sets held by a third party) constitute personal data.[2]	 The ALRC considered whether the definition of PI should be amended to cover information relating to an individual to bring it in line with overseas definition, but concluded PI should be about an identified or reasonably identifiable individual, consistently with the APEC Privacy Framework (which continues to use the term 'about'). On technical data, the ALRC's position was that, while IP addresses may not be PI, they may become personal in certain circumstances, if they come to be associated with a particular individual as 'information accretes'. In 2009, the then Government endorsed the ALRC's proposed definition which it found sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled.

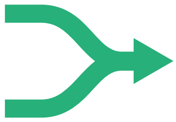
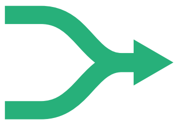
1 *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4.

2 *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14 (19 October 2016).

ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
Strengthening notification requirements	Entities subject to the Australian Privacy Principles (**APPs**) should provide individuals a written notice when collecting PI (directly or indirectly), unless the consumer already has the information or there is an overriding legal or public interest reason. The amendment would remove the 'reasonableness' qualifier in APP 5, which the ACCC considers to give APP entities too much discretion.	 Consultation required to identify appropriate measures that can be taken to improve notification without imposing significant regulatory burden and avoid 'notification fatigue'.	 GDPR notification obligations are not subject to a reasonableness element. The notification obligations under the GDPR do not apply if the data subject already has the information, and – where the information is collected through a third party – if the provision of the notification proves impossible or would involve a disproportionate effort.	 In 2008-2009, both the ALRC and the Government agreed that the notification requirement should continue to be subject to a reasonableness qualifier. The ALRC accepted that the concept of 'reasonableness' involves uncertainty, but considered introducing detailed and prescriptive requirement would be inconsistent with the high-level principles approach. It suggested that it should be for the OAIC's predecessor to develop guidance on when it might be reasonable not to provide notification.
	Notifications should outline the purpose for which each type of data is collected and, where the data will be disclosed to any third parties, the purposes of disclosure. The notice should be concise, transparent, intelligible and easily accessible, written in clear and plain language and be provided free of charge, and delivered in a way that reduces the information burden on consumers (for example, by using layered notices or standardised icons or phrases).		 The ACCC acknowledges that its suggested notification content is based on Articles 13 and 14 of the GDPR. Article 12 of the GDPR requires notifications to be concise, transparent, intelligible and easily accessible, using clear and plain language. It also empowers the European Commission to introduce standardised icons by means of delegated acts. To date, the Commission has not introduced such icons.	**No Position**

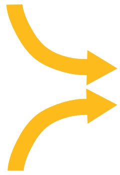
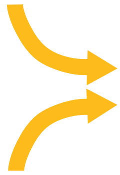
ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
Making affirmative and specific consent the basis for data processing	APP entities should obtain consent for any collection, use or disclosure that is not necessary for the performance of a contract to which the consumer is a party, unless required under the law or for an overriding public reason. Under the current regime, Australian organisations only need to obtain consent in specific circumstances, such as the collection of sensitive information. They don't need consent to use information for the primary purpose of collection, which the ACCC notes is broadly construed, or if the use is within the individual reasonable expectations and for a purpose related to the primary purpose.	 Consultation required to identify the appropriate measures that can be taken to improve consent requirements and pro-consumer defaults, without imposing significant regulatory burden avoid 'consent fatigue'.	 The ACCC does not recommend adopting an exception for use or disclosure for the legitimate interests of the collector or a third party, another lawful basis for processing PI under article 6(1) of the GDPR, which the ACCC considers involve too much uncertainty. Not being able to rely on the legitimate interest basis could create significant challenges for Australian entities. Organisations that must comply with the GDPR frequently rely on the legitimate interest to avoid consent fatigue (albeit it is worth noting this legitimate interest must be balanced against the interests or fundamental rights and freedom of data subjects).	 The ALRC did not propose to introduce a general consent requirement for data processing other than in the specific circumstances already prescribed in the existing privacy principles. Its recommendation to introduce a consent requirement for direct marketing led to the introduction of APP 7.
	The Privacy Act should require consent to be informed, voluntary and specific (as currently recommended by the OAIC). Valid consent should also require an affirmative and unambiguous act. In particular, the proposed rules mean that any settings for data practices relying on consent should be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled (the OAIC current guidance advises caution when relying on 'bundled consent').		 Article 4(11) of the GDPR defines consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which they, by a statement or a clear affirmative action, signify agreement to the processing of their PI. In October in *Planet49*, the European Court of Justice, applying the GDPR's definition of consent to the ePrivacy Directive, ruled that a pre-ticked checkbox does not constitute valid consent to use cookies, and that consents for different processing activities must be separate.[3]	 In 2008, the ALRC considered that amending the Privacy Act to set out in detail what is required to obtain consent would be inconsistent with the ALRC's view that a principles-based approach should continue to be at the heart of the Privacy Act. It further noted that it would be very difficult, if not impossible, to cover every relevant circumstance, a statutory definition of consent may not capture nuances in the evolution of common law and may be interpreted too restrictively, creating undesirable restrictions on the flow of information.

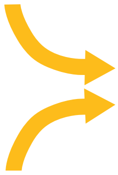
3 *Verbraucherzentrale Bundesverband eV v Planet49 GmbH*, Case C-673/17 (1 October 2019).

ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
				Rather, the ALRC's recommendation, endorsed by the then Government, was that the OAIC's predecessor develop further guidance on consent requirements, covering express and implied consent as well as bundled consent.
Introducing a direct right of action	Individuals should have a right to bring direct court actions and class actions to seek compensation for breach of the Privacy Act, rather than having to go through the OAIC complaint process.	 Consultation required to identify the appropriate measures that can be taken to ensure individuals have adequate remedies for an interference with their privacy under the Privacy Act.	 European data subjects have direct rights of action under the GDPR. Article 79 provides them with a right to an effective judicial remedy where their personal data has been processed in breach of the GDPR. They can also, under article 82, receive compensation for any damage resulting from an infringement of the GDPR.	**No Position**
Further Review (ACCC Recommendations) ACCC recommendations which the Government has suggested be considered as part of the broader Privacy Act review due to be completed in 2021.				
Introducing a 'right to be forgotten'	APP entities should erase PI without undue delay upon receiving a request for erasure from the consumer, unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.		 This recommendation broadly aligns with the principles outlined in article 17 of the GDPR. The ACCC has not specified what procedures organisations will be required to adopt to give effect to the rights of erasure. In Europe, those include informing any third party with whom the data was shared of the erasure request, to ensure effective deletion of links to or copies of the data in question, unless the organisation can demonstrate complying is impossible or would require disproportionate efforts.	**No Position**

ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
Introducing a statutory cause of action for serious breach of privacy	A statutory cause of action should be available where for serious privacy breaches committed intentionally or recklessly, to capture data practices that do not fall within the scope of the Privacy Act.		**No Provision**	The ALRC recommended to introduce a privacy tort in 2008 and 2014. These recommendations never received a Government response.
Further Review (Broader Reform) Topics suggested by the ACCC for further consideration as part of a broader Privacy Act review. The Government has agreed to conduct that review, due to be completed in 2021.				
Reconsider the Privacy Act objectives	Review in particular the merits of balancing the right to privacy against the commercial interests of businesses that handle PI; and whether this consideration places sufficient emphasis on the importance of protecting Australian consumers' right to privacy.		Recital 4 in the GDPR notes that the right to the protection of personal data is not absolute and must be balanced against other fundamental rights, including the freedom to conduct a business.	The ALRC recommended the inclusion of an objects clause in the Privacy Act, which would recognise that the right to privacy is not absolute and must be balanced with other public interests (eg public health and safety). However, it did not recommend that they should be weighed against businesses' commercial interests, as currently prescribed under section 2A of the Privacy Act.

ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
Consider whether Privacy Act exemptions should remain	For example, the exemptions for small businesses (organisations with an annual turnover of less than $3 million) and for employee records.		There is no general exemption for small businesses or employee records under the GDPR.	The ALRC recommended to remove the exemptions for small businesses, employee records and registered political parties. In particular, the ALRC considered that the cost of compliance does not justify an exemption for small businesses. It also made the point that the risk to privacy should be determined based on the amount and nature of PI held, not the size of an organisation. In relation to the employee exemption, the ALRC's conclusion was that the further protection should be in addition to state workplace relation legislations, which it viewed as not offering sufficient protection. These recommendations never received a Government response.
Consider introducing minimum standards of privacy protection	For example, consider introducing a requirement that all use and disclosure of PI be by fair and lawful means. The APPs currently require APP entities to collect PI by fair and lawful means, but does not contain any such requirement for the use and disclosure of PI.		Art 5.1 of GDPR requires that PI shall be processed lawfully, fairly and in a transparent manner. 'Processing' is defined to mean any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.	**No Position**

ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
			The Privacy Act does not use the term 'processing' but the OAIC sometimes refers to 'handling' in a similar way.	
Consider introducing a third-party certification scheme	Consider requiring certain organisations collecting, using or disclosing a large volume of Australians' PI to undergo external audits to monitor, and publicly demonstrate compliance with, applicable privacy laws through the use of a data protection seal or mark.		 It is unclear whether the certification scheme envisioned by the ACCC will be mandatory, as initially recommended in the preliminary report, or voluntary, similarly to the mechanisms described in article 42 of the GDPR, which encourages the establishment of voluntary data protection certification mechanisms and of data protection seals and marks. How the scheme under the GDPR will operate in practice is still to be settled. The ACCC recommends the development and experiences of the European scheme inform the proposed certification mechanism in Australia.	 The ALRC considered that the use of trust marks to demonstrate compliance should be explored, but cautioned the concept should be developed further before it would be appropriate for introduction as a mechanism under the Privacy Act.

ACCC PROPOSED AMENDMENT	DETAILS	GOVERNMENT'S RESPONSE	ALIGNMENT WITH GDPR?	ALIGNMENT WITH ALRC 2008 REPORT?
Consider whether the Privacy Act should set out additional requirements for inferred information and de-identified information.	For example, by setting standards to protect against increasing risks of inference or re-identification as more information becomes available, multiple datasets are combined, and advances in data analytics are made.		 The GDPR defines pseudonymisation as the processing of PI in such a manner that the PI can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the PI is not attributed to an identified or identifiable individual. The GDPR does not apply to anonymous information, where the data subject is no longer identifiable (the process must be irreversible). However, PI which has undergone pseudonymisation, and which could be attributed to an individual by the use of additional information is considered to be information on an identifiable natural person and is subject to the GDPR.	**No Position**

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**