HERBERT SMITH FREEHILLS

ONLINE PRIVACY BILL AND PRIVACY ACT DISCUSSION PAPER: STRICTER ENFORCEMENT, ONLINE PRIVACY CODE AND THE IMPACT FOR ORGANISATIONS HANDLING PERSONAL INFORMATION

Australia
Legal Briefings – By **Kaman Tsoi and Marine Giral**

This week, two publications by the Australian Attorney-General's Department mark significant steps forward on the long road to reform of Australian privacy legislation:

1. An exposure draft introducing amendments to the Privacy Act 1988 (Cth) (**Online Privacy Bill**), which will strengthen penalties and enforcement measures and introduce a binding privacy code for online platforms.[1]

2. A discussion paper seeking submissions on 67 proposals for, and further questions in relation to, broader reforms to Australian privacy legislation (**Discussion Paper**).[2]

Submissions on the Online Privacy Bill and the Discussion Paper are due by 6 December 2021 and 10 January 2022 respectively.

The publications follow the release of an issue paper in November 2020 outlining and seeking feedback on the Privacy Act, and the Government's December 2019 announcement that it would conduct a review of the Act as part of its response to the Australian Competition and Consumer Commission's Digital Platforms Inquiry report (ACCC Report).[3] We published a detailed overview of the ACCC Report's privacy recommendations and Government response in early 2020, comparing key recommendations to the European Union's General Data Protection Regulation (GDPR) and the 2008 Australian Law Reform Commission report on Australian privacy law (ALRC Report).[4]

We have noted some key issues and themes below, with the two tables which follow summarising the proposals under the Bill and Discussion Paper. We will also separately be publishing further commentary on specific topics raised by the Discussion Paper.

We will be publishing further commentary on specific topics raised by the Bill and the Discussion Paper.

INCREASED PENALTIES AND ENFORCEMENT

As foreshadowed in earlier Government announcements and the ACCC Report, maximum penalties under the Privacy Act will increase to $10 million, three times the value of the benefit obtained from the breach, or in some cases 10% of domestic annual turnover. This aligns with penalties under the Australian Consumer Law. Other changes to the enforcement powers of the Office of the Australian Information Commissioner (OAIC) will likely encourage actions by the OAIC and greater collaboration with other regulators (such as ASIC, APRA, the ACMA and the ACCC), some of which have been increasingly active in dealing with privacy and data issues in recent years.

Please find our detailed analysis on what the reforms signal for future regulatory enforcement of privacy breaches here.

THIRD PARTY COLLECTION

The Discussion Paper proposes requiring privacy notices to identify the specific third parties from which personal information is collected. Entities should also provide this on request in respect of particular personal information unless impossible or it would involve disproportionate effort.

FAIRNESS REQUIREMENTS

The Discussion Paper appears to move away from the ACCC Report's suggestion to make consent the principal basis for collection, use and disclosure. Instead, the Discussion Paper makes recommendations which place greater responsibility on entities handling personal information to ensure that handling is fair and reasonable. These may include requiring them to introduce pro-privacy defaults on a sectoral or other specified basis and take 'reasonable steps' to identify and mitigate risks associated with:

- the collection, use or disclosure, on a large scale, of certain types of information (biometric or genetic data and other sensitive information, children's personal information, location data),
- certain purposes (direct marketing, targeted advertising, profiling, sale, influencing individuals' behaviour or decisions), or
- activities that are otherwise likely to result in a high privacy risk or risk of harm to an individual.

The paper also considers measures to increase an individual's capacity to self-manage their privacy in relation to these practices, including consent and the right to opt-out in respect of an expanded set of sensitive information and restricted practices.

OVERSEAS DATA FLOWS

A number of significant changes are proposed, including:

- providing for the approval of particular countries and certification schemes for receiving personal information,
- standard contractual clauses, and

removal of the consent exception.

INDIVIDUALS' RIGHTS

Similarly, the Discussion Paper introduces greater flexibility around some of the GDPR-inspired rights that the ACCC Report had proposed to introduce, having taken into account some of the submissions made around the challenges of introducing such rights (including legal retention requirements and technical challenges). For example, it proposes that individuals may only request erasure of their personal information where certain specified grounds apply, such as where the personal information must be destroyed or de-identified under Australian Privacy Principle (APP) 11.2, is sensitive or relates to a child, and subject to some exceptions (this could include where personal information is required for a transaction, erasure is technically impractical or for public interest reasons).

DIRECT MARKETING

The Discussion Paper proposes to repeal the current APP 7 (direct marketing) in favour of a number of proposed reforms. These proposals include greater transparency where an individual's personal information will be used to influence their behaviour, risk assessments for large scale direct marketing (including online targeted advertising) and an unqualified right to object to direct marketing.

EMPLOYEE RECORDS AND SMALL BUSINESSES EXEMPTIONS

The Discussion Paper does not make specific proposals in respect of the current exemptions under the Privacy Act, noting further consideration on those issues is required.[5] Rather, it seeks submissions on some suggested options to reform (rather than remove) those exemptions:

> In particular, the paper notes that completely removing the small business exemption could prove too burdensome but options that could be considered include: a reduction of the annual turnover threshold (currently $3 million), limiting the scope of the exemption to some but not all of the APPs, and requiring small businesses to comply with simplified rules or only in relation to high risk activities.

Likewise, the paper notes that removing the employee exemption would make it difficult to administer the employment relationship, but suggests modification to allow better protection of employee records while retaining sufficient flexibility. For example, this paper suggests introducing a standalone exception into APPs 3 (collection) and 6 (use and disclosure) in relation to the collection, use and disclosure of an employee's personal and sensitive information by a current or former employer for any act or practice directly related to the employment relationship while allowing enhanced protection of employee privacy through the application of other APPs, such as APPs 8 (cross-border disclosure) and 11 (security/retention), as well as through workplace relations legislation.

CONTROLLERS AND PROCESSORS OF PERSONAL INFORMATION

The Discussion Paper acknowledges a number of submissions recommended introducing into the Privacy Act the concepts of data controllers and data processors, found in overseas data protection frameworks including the GDPR, to clarify allocation of responsibilities relating to notification, consent and security, but noting this may present challenges including due to the small business exemption. The paper does not make any specific proposals on this issue but poses a number of questions to be considered in submissions.

DIRECT RIGHT OF ACTION

The Discussion Paper proposes creating a direct right of action for interferences with privacy, as a further avenue for impacted individuals and groups following their initial privacy complaint.

TABLE 1 - ONLINE PRIVACY BILL AMENDMENTS

Amendment	Proposed changes
Increased maximum civil penalties	Increasing the maximum civil penalty for a serious and/or repeated interference with privacy to an amount not exceeding the greater of: $10,000,000; three times the value of the benefit obtained by the body corporate from the conduct constituting the serious and repeated interference with privacy; or, if the value cannot be determined, 10% of their domestic annual turnover. The Bill sets out how to calculate turnover for the purposes of this provision.
Other enforcement powers and penalties provisions	• Creating a new infringement notice provision for failing to give information, answer a question or provide a document or record when required to do so as part of an investigation (with associated additional civil penalty provisions). • Creating a new criminal penalty for multiple instances of non-compliance. • Expanding the types of declarations that the Commissioner can make in a determination at the conclusion of an investigation. • ·Enhancing the Commissioner's capacity to conduct assessments. • Improving the Commissioner's information-sharing arrangements with relevant enforcement authorities and the ability for the Commissioner to disclose information in particular circumstances.
Online Privacy Code	Developing an Online Privacy Code applicable to large online platforms (defined as an organisation with at least 2.5 million end-users in Australia in a given year), social media service providers and brokerage service providers. The Code will need to address how certain existing APPs (including in respect of privacy policies, notices and consents) apply to these organisations. The Code will require covered organisations to take such steps (if any) as are reasonable in the circumstances to not use or disclose, or to not further use or disclose, an individual's personal information upon request from that individual. The Code will also address how both existing and new obligations will apply in relation to children and vulnerable groups. The Commissioner will have the power to investigate potential breaches of the Code, either following a complaint or on the Commissioner's own initiative. The Commissioner's full range of enforcement powers will be available in the event that an investigation finds that a breach has occurred. See our detailed briefing on the Online privacy code here.

TABLE 2 - KEY PROPOSALS AND ISSUES IN THE DISCUSSION PAPER

Topics	Key proposals and Issues
Proposals[6]	
Scope (definition of personal information)	Change the word 'about' in the definition of personal information to 'relates to', reversing what some considered a narrow interpretation of the definition in the Telstra v Grubb case. Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information, which could include online identifiers and location data. Define when an individual would be 'reasonably identifiable'. Expressly cover information obtained from any source and by any means, including inferred or generated information. Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments. The Bill proposed to introduce criminal and civil penalties into the Privacy Act for re-identification of de-identified information released by Commonwealth agencies.
Notice of collection of personal information	Require notification at or before the time of collection, or if that is not practicable as soon as possible after collection, unless the individual has already been made aware of the APP 5 matters; or notification would be *impossible* or would involve *disproportionate effort*. This will likely increase the circumstances in which notification is required. Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable. Privacy notices to describe, if the collection occurred via a third party, who that third party was and the circumstances of the collection. Standardised privacy notices could be considered on a sector-specific basis.
Consent to the collection, use and disclosure of personal information	Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action. Standardised consents could be considered on a sector-specific basis.
Additional protections for collection, use and disclosure of personal information	Collection, use and disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances (having regard to reasonable expectation, necessity, proportionality, transparency, best interests (if children are involved), sensitivity and amount of personal information and foreseeable risk of unjustified adverse impacts or harm).
Restricted and prohibited acts and practices	**Option 1:** APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks: • Sale of personal information on a large scale. • Direct marketing and online targeted advertising involving collection, use or disclosure of personal information on a large scale. • The collection, use or disclosure of personal information for influencing individuals' behaviour or decisions on a large scale. • Automated decision making with legal or significant effects. • The collection, use or disclosure of sensitive information, children's information, location data on a large scale. • The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software. • Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual. **Option 2:** In relation to the specified restricted practices, increase an individual's capacity to self-manage their privacy in relation to that practice. Possible measures include consent (by expanding the definition of sensitive information), granting absolute opt-out rights in relation to restricted practices or by ensuring that explicit notice for restricted practices is mandatory.
Pro-privacy default settings	Introduce pro-privacy defaults on a sectoral or other specified basis.
Children and vulnerable individuals	Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16 and include further specific protections for children.
Right to object	An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information.
Data portability (not recommended)	The Discussion Paper does not recommend introducing a right to data portability, noting this could duplicate aspects of the Consumer Data Right scheme and create unnecessary regulatory complexity.
Right to erasure of personal information (limited)	An individual may only request erasure of personal information where certain specified grounds apply (eg where the personal information must be destroyed or de-identified under APP 11.2 or an Australian law, the personal information is sensitive or relates to a child) and subject to some exceptions.
Direct marketing, targeted advertising and profiling	Unqualified right to object to any collection, use or disclosure of personal information for direct marketing. The use or disclosure of personal information for the purpose of influencing an individual's behaviour or decisions must be a primary purpose notified to the individual when their personal information is collected. Privacy policy to describe (i) whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and (ii) third parties used in the provision of online marketing materials. Repeal APP 7 in light of existing protections in the Act and other proposals for reform.
Automated decision-making	Require privacy policies to 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.
Security and destruction of personal information	'Reasonable steps' to protect personal information to include technical and organisational measures (similar language to the GDPR). Include a list of factors that indicate what reasonable steps may be required. APP entities to take *all* reasonable steps to destroy the information or ensure that the information is anonymised where the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under the APPs.
Organisational accountability	Introduce further organisational accountability requirements into the Act, targeting measures to where there is the greatest privacy risk.
Overseas data flows	Amend the Act to introduce a mechanism to approve countries and certification schemes. Standard contractual clauses for transferring personal information overseas to be made available to APP entities to facilitate overseas disclosures of personal information. Remove the informed consent exception in APP 8.2(b). Strengthen the transparency requirements in relation to potential overseas disclosures to include the countries that personal information may be disclosed to, as well as the specific personal information that may be disclosed overseas in the entity's up-to-date APP privacy policy required to be kept under APP 1.3. Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines. Amend the Act to clarify what circumstances are relevant to determining what 'reasonable steps' are, in relation to ensuring a recipient's compliance with the APPs for the purpose of APP 8.1.
Cross border privacy rules and domestic certification	Continue to progress implementation of the APEC Cross-Border Privacy Rules (CBPR). Introduce a voluntary domestic privacy certification scheme that is based on, and works alongside CBPR.
Enforcement	Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses. Clarify what is a 'serious' or 'repeated' interference with privacy. Empower the OAIC to undertake public inquiries and reviews into specified matters. Require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. Give the Federal Court the power to make any order it sees fit after a civil penalty provision has been established. Introduce an industry funding model similar to ASIC's, incorporating two different levies.
A direct right of action	Create a direct right of action with the following design elements: • The action would be available to any individual or group of individuals whose privacy has been interfered with by an APP entity. • The action would be heard by the Federal Court or the Federal Circuit Court. • The claimant would first need to make a complaint to the OAIC (or new Federal Privacy Ombudsman) and have their complaint assessed for conciliation either by the OAIC or a recognised external dispute resolution scheme, such as a relevant industry ombudsman. • The complainant could then elect to initiate action in court where the matter is deemed unsuitable for conciliation, conciliation has failed, or the complainant chooses not to pursue conciliation. The complainant would need to seek leave of the court to make the application. • The OAIC would have the ability to appear as amicus curiae to provide expert evidence at the request of the court. Remedies available under this right would be any order the court sees fit, including any amount of damages.
A statutory tort of privacy	**Option 1:** Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report. **Option 2:** Introduce a minimalist statutory tort that recognises the existence of the cause of action but leaves the scope and application of the tort to be developed by the courts. **Option 3:** Do not introduce a statutory tort and allow the common law to develop as required. However, extend the application of the Act to individuals in a non-business capacity for collection, use or disclosure of personal information that would be highly offensive to an objective reasonable person. **Option 4:** In light of the development of the equitable duty of confidence in Australia, states could consider legislating that damages for emotional distress are available in equitable breach of confidence.
Notifiable data breaches scheme (NDBS)	Statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.
Other issues[7]	
Employee record exemption	• How might the employee records exemption be modified to better protect those records while retaining the flexibility employers need to administer the employment relationship, and address the impact of the Fair Work Commission's decision in Lee v Superior Wood? • To what extent would the fair and reasonable test for the collection, use and disclosure of personal information proposed above be suitable for the employment context? • To what extent would the current exceptions in APPs 12 (access) and 13 (correction) address concerns about the need for employers to conduct investigations and manage employee performance if the exemption were modified? • What would be the benefits and costs associated with requiring employers to take reasonable steps to prevent employees' personal information from misuse, interference or loss? • What challenges or barriers would there be to requiring employers to comply with the NDBS in relation to eligible data breaches involving all employee records? • What would be the benefits and limitations of providing enhanced protections for employees' privacy in workplace relations laws?
Small business exemption	• What high privacy risk acts and practices should be prescribed as exceptions? • What support for small business would assist with adopting the privacy standards in the Act? • What could be the impact of specific proposals including around consent voluntary domestic privacy certification scheme on small business?
Political and journalism exemptions	• What would be the benefits and costs of applying some specific APPs to political parties and their affiliates? • What impact would introducing a public interest requirement into the journalism exemption, have on the free flow of information to the public through the media? • What might be the positive or adverse consequences of applying security obligations under APP 11 to media organisations in the course of journalism?
Controllers and processors of personal information	• Are there any advantages or disadvantages of introducing these concepts in the Act? • If adopted, what obligations under the Act should processors have (record keeping, security, NDBS etc.)?

1. https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/
2. https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/
3. https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
4. https://www.herbertsmithfreehills.com/latest-thinking/australian-privacy-law-reform-and-review-announced
5. Discussion paper, p 8.
6. Table below is not an exhaustive list of the proposals and issues in the Discussion Paper but identifies the most significant ones. Full list of proposals is available at pp 10- 17 of the Discussion Paper.
7. The Discussion Paper does not make recommendations in respect to a number of topics, but raise a number of questions about them.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

KWOK TANG
PARTNER, SYDNEY
+61 2 9225 5569
Kwok.Tang@hsf.com

PETER JONES
PARTNER, SYDNEY
+61 2 9225 5588
peter.jones@hsf.com

KATHERINE GREGOR
PARTNER, MELBOURNE
+61 3 9288 1663
Katherine.Gregor@hsf.com

MICHELLE AGGROMITO
SENIOR ASSOCIATE, MELBOURNE
+61 3 9288 1079
michelle.aggromito@hsf.com

MARINE GIRAL
SOLICITOR, MELBOURNE
+61 3 9288 1496
marine.giral@hsf.com

LEGAL NOTICE