HERBERT SMITH FREEHILLS

1 Further specific details of the proposals can be downloaded here

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
		Exposure Draft proposals	
Increase to penalties for serious breaches	Increasing the penalty or serious and repeated interferences to up to $10m or more.	The Exposure Draft increases the maximum civil penalty for serious and repeated interferences with privacy under section 13G of the Act to: • for individuals, 2,400 penalty units ($532,800). • for a body corporate, either: – $10 million; – three times the value of the benefit obtained by the body corporate from the relevant conduct; or – if the value cannot be determined, 10% of their domestic annual turnover. The current maximum civil penalty is 2,000 penalty units, being $444,00 for individuals and $2.22 million for bodies corporate	 Consistent with the DPI Report and maximum penalties under Australian Consumer Law.
New assessment powers	Allowing the Commissioner to require the production of information or documents in an assessment of any kind.	The Exposure Draft creates a new information-gathering power for the Commissioner to conduct an assessment of any kind. This may include the issuance of notices to produce information or documents relevant to the assessment. This power is subject to safeguards including: • the notice can only be issued to the entity subject to the assessment; • the Commissioner must be satisfied that it is reasonable in the circumstances, including the public interest and impact on the entity; and • a law enforcement body is not required to comply.	 Not previously discussed.

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
		The Exposure Draft also provides the Minister with the ability to request the Commissioner conduct an assessment of whether a social media service is maintaining and handling personal information of children in accordance with the registered OP code. The Commissioner can currently conduct an assessment of an entity's compliance, but does not have specific assessment related powers. Entities can decline to cooperate with assessments.	
Additional consequences for failures to assist in investigations	Creating civil penalty and supplementary infringement notice provisions.	Currently, the Commissioner may require persons to produce a document or record, for example, in the course of an investigation. This is enforced by section 66 of the Act, which provides that it is a criminal offence where a person fails to do what is required under the Act. The Exposure Draft creates an additional civil penalty and supplementary infringement notice provisions, to provide an alternate means of resolving matters without criminal prosecution. The penalty amounts would be as follows: • for an infringement notice, 12 penalty units for individuals or 60 penalty units for bodies corporate; and • the civil penalty for the infringement notice would be 60 penalty units for individuals and 300 penalty units for bodies corporate. A separate criminal offence applies for multiple instances of non-compliance which constitute a system of conduct or pattern or behaviour. The maximum penalty will be increased to 300 penalty units for bodies corporate. The Discussion Paper at Proposal 24.3 provides an additional recommendation, being that the powers in Part 3 of the *Regulatory Powers (Standard Provisions) Act 2014* would apply to investigations of civil penalty provisions in addition to the Commissioner's current investigation powers. This includes powers for an authorised person to exercise general investigation powers, including searching premises, making copies of information specified in a warrant, operating electronic material to determine whether the kinds of information and documents specified in a warrant are accessible and seizing evidential material.	 Not previously discussed.

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
Broader range of powers in issuing determinations	Allowing the Commissioner to make further determinations, including requiring a review or statement on the relevant conduct.	The Commissioner currently has the power to make a determination at the conclusion of a complaint or investigation as to whether it is substantiated, interferes with privacy and whether the respondent must undertake further action such as specific steps to prevent the conduct from repeating or continuing. The Exposure Draft provides the following additional measures: • clarifying that the Commissioner could also require the respondent to engage an independent and suitably qualified adviser to assist this process. This may include the review of any relevant business practices or processes that contributed to the non-compliance, the remediation of the non-compliance, and that the Information Commission is provided detail about their findings; and • creating a new Commissioner's determination power to require the respondent to prepare a statement about the conduct that led to the interference of privacy and steps they have taken or will take to remediate the contravention. This statement may be published or provided to complainants or affected class members. The Discussion Paper at Proposal 24.5 suggested that the Commissioner be given the power to require an APP entity to perform any reasonable act or course of conduct to identify, mitigate and redress actual or reasonably foreseeable loss. This intends to create a requirement on an entity to be proactive in preventing loss.	 Not previously discussed.
Extraterritoriality	Clarification of the extraterritorial application of the Act.	The Exposure Draft provides for the removal of the condition that an organisation must collect or hold personal information from sources inside of Australia in order to be subject to the Act. Under the existing provisions, foreign organisations will be subject to privacy obligations under the Act if the organisation has an Australian link, being the carrying on of business in Australia and collecting or holding information from a source inside Australia. The removal of the source requirement seeks to clarify that foreign organisations carrying on a business in Australia will be subject to the Act, even if they obtain information regarding Australian customers from entities or sources outside of Australia.	 Not previously discussed.

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
Regulatory cooperation	Encourage regulators to cooperate in enforcing matters involving personal information.	The Exposure Draft provides for the OAIC to share information with other regulators. This prevents existing confidentiality provisions from limiting information sharing. The Discussion Paper notes the increase in data-based regulatory enforcement action taken by the ACCC and ASIC. The relationship between regulators is currently governed by memoranda of understanding, dividing regulatory responsibility. The ACCC's submissions to the Discussion Paper noted the importance of the OAIC having adequate enforcement powers – this may indicate that subject to the passing of the Exposure Draft, the OAIC will be taking on an extended enforcement function. The Discussion Paper suggests that the regulators will continue to work collaboratively, with the intention to bring enforcement action under an appropriate framework and prevent duplicative investigations. Similar issues may arise in competition, data and consumer protection laws. It is suggested that overlapping regulatory models is evidence of the development of different legal frameworks and the growing importance of privacy issues. Provided that individuals do not 'fall through the gaps' of different frameworks, this overlap is not presented as an issue.	 Issue discussed in the DPI Report.
Issues raised in the Discussion Paper			
New civil penalty provisions for less serious breaches	Creating a civil penalty (and infringement scheme) for breaches of privacy provisions that are not serious or repeated.	Currently, there is no civil penalty regime for infringements that are not serious or repeated. This creates a potential gap, for example, where organisations have a history of ongoing but relatively minor non-compliance with the Act. Proposal 24.1 of the Discussion Paper suggests a new 3 tier civil penalty provision regime. In addition to the current civil penalty regime for serious and repeated interferences with privacy (Tier 1), this would involve creating: • mid-tier civil penalty provisions for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy (Tier 2); and • a series of new low-level and clearly defined civil penalties for administrative breaches of the APPs, with an attached infringement notice regime for the Information Commissioner (like those that exist for ASIC, the ACCC and others) (Tier 3).	 Not previously discussed.

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
Clarify what is a serious or repeated interference with privacy	New legislative guidance on type of conduct captured.	The ongoing proceedings against Facebook are the first time that the OAIC has brought civil penalty proceedings seeking a civil penalty for serious and repeated interferences with privacy. "Serious and repeated" is not a defined term and there is no judicial guidance to date. Proposal 24.2 suggests that there could be further clarification of these terms, including, for example, to show that they capture highly sensitive information, impacts on large groups of individuals or vulnerable individuals, repeated or wilful misconduct of serious failures to take proper steps to protect personal data.	
Public inquiry powers	Allowing the Commissioner to undertake public inquiries.	The Discussion Paper at Proposal 24.4 suggests that the Act be amended to provide the Commissioner the power to undertake public inquiries and reviews into specified matters, modelled on the powers of the ACCC and the inquiry and review functions of the Australian Human Rights Commission. This power may be as directed by or subject to Ministerial approval, and may allow for the proactive identification of widespread industry practices. Currently, the Commissioner may conduct assessments into the information handling practices of APP entities, but does not have the power to undertake a public inquiry.	 Not previously discussed. However, the power is modelled on the powers of the ACCC and functions of the AHRC.
Expansion of powers of the Federal Court	Empowering the Court to make any orders it sees fit after a contravention of section 13G.	Currently, the Federal Court only has the power to make an order for the respondent to pay a pecuniary penalty after a finding of contravention under section 13G, but the Act does not allow for the Federal Court to make any order it sees fit. The Discussion Paper at Proposal 24.6 suggests that the Federal Court be given the power to make any order it sees fit after a section 13G civil penalty provision has been established. This could include conduct orders and compensation orders for affected individuals. This is consistent with a section 52 determination that can be made by the Information Commissioner.	 Not previously discussed.

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
Direct right of action	Allowing individuals to enforce privacy rights directly after a conciliation attempt and upon a grant of leave. This is a development on a prior proposal in the DPI Report.	More than 50% of submissions supported introduction of a direct right of action. The Discussion Paper at Proposal 25 suggests the creation of a direct right of action with the following design elements: • available to any individual or group of individuals whose privacy has been interfered with by an APP entity. No harm threshold is proposed. • 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 Federal Privacy Ombudsman) and have their complaint assessed for conciliation either by the OAIC or a recognised external dispute resolution (**EDR**) scheme such as a relevant industry ombudsman, but could then elect to initiate court proceedings instead of pursuing conciliation. The complainant would need to seek leave of the court to make the application; and • 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 (compensatory, aggravated and circumstances) for financial and non-financial harm. It was noted that the EU, NZ and Canada do not have a cap on damages for direct rights of action. The intention behind this process was to provide individuals with a direct pathway, while protecting the Court from frivolous claims due to the requirement of conciliation. Currently, Australia does not currently have a direct right of action. Individuals may seek relief by lodging a complaint with the OAIC or seeking an injunction under the Act.	 Further consideration given to issue. The DPI Report recommended the introduction of a direct right of action for individuals seeking compensation for an interference with their privacy. This was considered to be critical to the effectiveness of enforcing rights. The Government noted that this was supported in principle, but was seeking further consideration of how to frame such a right to confer greater control to individuals and greater incentives for compliance while balancing the need to appropriately direct court resources.

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
Statutory tort of privacy	Proposing options for a statutory tort of privacy. This includes the form of tort proposed in the ALRC Report and additional minimalist models.	The Discussion Paper at Proposal 26 raises four options for implementation of a statutory tort, noting submissions were divided as to whether this should occur, and if so, how: • **Option 1**: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report (two limbs, intrusion upon seclusion and misuse of private information, with a requirement to prove that the public interest in privacy outweighed any countervailing public interest, the breach of privacy was sufficiently serious and the individual had a reasonable expectation of privacy in all the circumstances). • **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 which 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. In raising alternative to the ALRC's proposal, the Discussion Paper noted the wide variety of views received in submissions and alternate models adopted in other jurisdictions. Currently, a statutory tort of privacy has not been introduced in Australia (although the possibility has been considered by the courts). The introduction of such a tort is not contained in the Exposure Draft.	 Further consideration given to issue. The ALRC Report recommended the addition of a Commonwealth statutory cause of action for a serious invasion of privacy. This tort may be contravened by intrusion upon seclusion or misuse of private information. The ALRC Report proposal was supported by the DPI Report.
****New proposed funding model**	Introducing a cost recovery levy and statutory levy to obtain further funding.	The majority of submissions recognised the need for the OAIC to have adequate funding, staffing and support to satisfy its regulatory responsibilities, including focused education and industry collaboration to promote development of industry best practice. The OAIC also noted that appropriate resourcing was necessary to engage in substantive regulatory action through the courts. The Discussion Paper at Proposal 24.7 suggests the introduction of an industry funding model incorporating two different levies: • a cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments; and	 Not previously discussed.

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
		• a statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment, such as social media platforms and entities which trade in personal information such as digital marketing businesses. The Discussion Paper seeks further engagement on which high risk industries would be most appropriate in this regard. These types of levies have been implemented successfully by other regulators like ASIC (around 90% of ASIC's regulatory activities are recovered by industry funding levies, and the remaining 10% via fees for service) and the UK ICO (every organisation who processes personal information pays a data protection fee, unless exempt). Entities which operate in a high privacy risk environment may be those which collect, use or disclose significant amounts of personal information, including social media platforms and digital marketing businesses.	The model is similar to that adopted by ASIC.
Transparency in annual reporting	Amend annual reporting requirements to provide information regarding complaints.	The suggestion would require annual reports to publicise data about the complaints lodged, the outcome of all complaints and the basis for the dismissal of complaints. The anticipated benefits of this requirement include: • potential complainants would be more aware of common reasons for dismissals and subsequently be able to manage their expectations; and • the OAIC would be able to identify contentious issues and provide further guidance in light of how the Act is being interpreted and applied.	 Not previously discussed.
New proposed alternate regulatory models	Proposing new regulatory options to separate the OAIC's conciliation and enforcement powers.	Currently, the OAIC acts as both a conciliator and regulator. Submissions raised the tension between these roles, and the OAIC's submission noted a desire to shift to a risk-based regulatory approach, including by being able to exercise discretion to investigate individual complaints and prioritise based on the identification of sectors, acts or practices of concern. (At present it must investigate and attempt to conciliate all complaints which may be an interference with privacy and where it is reasonably possible to conciliate successfully – 2,600 complaints are received annually and a significant portion of efforts are dedicated to resolving individual complaints with no broader deterrent effect).	 Not previously discussed.

Reform proposal	Change at a glance	The proposal in focus	Prior consideration
		The Discussion Paper at Proposal 24.9 raises the following options for alternative regulatory models and further consideration: • **Option 1** – Encourage greater recognition and use of existing EDRs. APP entities that handle personal information could be required to participate in an EDR scheme. APP entities that are not part of a recognised EDR scheme could be required to pay a fee for service to the OAIC as the default complaint handling provider if a complaint is made against them. • **Option 2** – Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR schemes. This would give the OAIC a clearer and narrower mandate as a strategic privacy regulator, consistent with the roles of ASIC and the ACCC. • **Option 3** – Establish a Deputy Information Commissioner – Enforcement within the OAIC.	
Harmonise privacy laws	Establish a Commonwealth, state and territory working group to harmonise privacy laws.	Submissions to the Discussion Paper noted that inconsistencies between state and Commonwealth privacy laws cause confusion and an increase in the regulatory burden on APP entities. Key differences between the regimes which caused concern include definitions (such as the definitions of health information and personal information), issues regarding the treatment of personal information, data breach notification schemes, government contractors and exceptions to protections. Gaps between the regimes, such as universities and healthcare, were also identified. The suggested working group would intend to harmonise aspects of privacy laws. The proposed initial areas of focus include key definitions, the application of privacy laws to state and territory contractors, and the treatment of health information. The working group would also discuss a model for longer-term harmonisation between jurisdictions, including proposals to increase general consistency.	 Not previously discussed.