







INCHING FORWARDS: GOVERNMENT RESPONDS TO PRIVACY ACT REVIEW REPORT

PROPOSAL	AGREED (draft legislation to come)	AGREED-IN-PRINCIPLE (further consultation likely)	KWM COMMENT
Key theme 1: Bringing the Privacy Act into the digital age			
Update objects of Privacy Act to recognise the public interest in protecting privacy (Proposal 3.2), and clarify the focus of the Act is on <i>information</i> privacy (Proposal 3.1).			Industry will want to ensure that this change is not implemented in a way that overrides the current recognition in the Act that protection of privacy must be balanced with the interests of carrying out their functions or activities (i.e. that there be ongoing recognition of the economically and socially beneficial uses of personal information).
Expand the definition of ‘personal information’ (Proposal 4.2) and clarify when an individual will be considered ‘reasonably identifiable’ (Proposal 4.4).			This is potentially one of the most impactful areas of change contemplated in this round of reforms, as it may mean that a large range of data that is currently treated as falling outside the scope of the Act will become relevant to privacy compliance requirements. The Government has indicated that, in its view, an individual will be reasonably identifiable ‘where they are able to be distinguished from all others, even if their identity is not known’. This could have far-reaching consequences for the online advertising industry, amongst others, which often relies upon ‘anonymous’ identifiers to deliver relevant advertising. One of the more controversial recommendations was that the Act be amended to impose obligations in relation to de-identified data sets (Proposal 21.4). The Government has ‘noted’ that idea, which suggests that it will not be pursued as a Privacy Act measure, but indicated that

PROPOSAL	AGREED (draft legislation to come)	AGREED-IN-PRINCIPLE (further consultation likely)	KWM COMMENT
			they will further consider how the policy intent of protecting against risks of re-identification may be achieved.
Remove small business exemption (Proposals 6.1 & 6.2).			The Government recognises the potential impact on small businesses, and has committed to further consultation to assess how privacy obligations should be modified to ease the regulatory burden on small businesses, as well as what support can be provided to help them comply (e.g. through tailored guidance, e-learning modules and other compliance tools).
Remove employee records exemption (Proposal 7.1).			This is another change that may have a significant impact on businesses who currently have greater freedom to manage information about employees. The Government recognises that further consultation is needed to ensure that privacy and workplace relations laws operate in a consistent and complementary fashion.
Key theme 2: Uplift protections			
Introduce a new requirement that collection, use and disclosure of information be fair and reasonable in the circumstances (irrespective of consent) (Proposals 12.1-12.3).			This was a cornerstone of the proposed reforms laid out in the Attorney-General's Privacy Act Review Report. It has received broad support from stakeholders, though the practical impact and effect of such a general duty may only be fully known once it has been tested in court. This is seen by the Government as a key protection for processing that may take place through novel use of technology (e.g. the Government provides the examples of screen-scraping and use of information to power AI engines).
Privacy settings for online services should reflect a 'privacy-by-default' framework (Proposal 11.4).			The Government has indicated that further guidance will be provided to assist entities in understanding this requirement. Careful consideration will be required as to how this proposal should be implemented, as there is clearly a risk that it will drive organisations to

PROPOSAL

AGREED
(draft legislation to come)

AGREED-IN-PRINCIPLE
(further consultation likely)

KWM COMMENT

offer fewer or less granular privacy controls if they must be set by default to what they may consider less business-friendly settings.

Clarify that organisations must deploy both technical and organisational measures to safeguard personal information (Proposal 21.1).



This is a relatively uncontroversial change, but it underscores that organisations cannot treat privacy compliance as something that can be wholly delegated to their IT departments.

Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes (Proposal 21.2).





The Privacy Act Review report gave an example of outcomes-based factors drawn from the GDPR - that entities have the ability to ensure the ongoing confidentiality, integrity and resilience of systems and services which hold personal information. The Government in its response intends to align these baseline outcomes with relevant outcomes of the Government’s 2023-2030 Australian Cyber Security Strategy. Importantly, an organisation’s ability to achieve these outcomes will also have to be considered in context of the continued obligation of APP entities to take *reasonable steps* to keep personal information secure, and the guidance that the OAIC will provide around those *reasonable steps* (see Proposal 21.3).

Organisations should be required to establish minimum and maximum data retention periods for the personal information they hold (Proposal 21.7), and specify those periods in their privacy policies (Proposal 21.8).



This has been an area of particular focus in the wake of recent data breaches, which raised public concerns about the length of time that organisations have been holding onto personal information (including information used for identification). The Government recognises that, in this regard, the Privacy Act cannot be considered in isolation, as there are many other competing laws that may require organisations to collect and hold certain types of information.

In this context, and in the context of the Government’s 2023-2030 Cybersecurity Strategy, the Government has recognised that a review of all legal provisions requiring retention of personal information across both Commonwealth and State and Territory legislation will need to be

PROPOSAL	AGREED (draft legislation to come)	AGREED-IN-PRINCIPLE (further consultation likely)	KWM COMMENT
			<p>undertaken. (This will be no small exercise!). The impact of the Government’s separate proposals around digital identity, which will provide new ways for private sector businesses to verify individual identity (see our alert here), will also be significant in this area, as it may reduce the need for businesses to collect as much identifying information from individual consumers to begin with, although this will not be likely to be realised until the later phases of implementation of those proposals.</p>
<p>Tighten requirements around notifying data breaches, including setting a 72 hour timeframe to notify the OAIC after becoming aware that there are reasonable grounds to believe there has been an eligible data breach (Proposal 28.2).</p>			<p>This time period aligns with the time periods for notification of cyber breaches under the Security of Critical Infrastructure Act 2018 (noting that the notification period for critical breaches under that Act is only 12 hours!) and under APRA Prudential Standard CPS 234 (Information Security). It also reinforces recent messaging from the OAIC about the importance of swiftly responding to data breaches, including to notify regulators and individuals concerned so that they can take mitigating action. For more on the OAIC’s messaging in this area, you can read this recent KWM alert.</p>
<p>The Attorney-General should be able to permit sharing of information with appropriate entities (such as banks) that may be able to reduce the risk of harm in the event of an eligible data breach (Proposal 28.4).</p>			<p>This is a pragmatic step that should help to manage the fallout of future major data breaches that may impact financial information or identification documents that could be used for financial fraud. It has previously been a frustration of Government that there is no mechanism that allows information to be shared for these purposes. For example, specific amendments had to be made to the Telecommunications Regulations in order to permit Optus to disclose relevant information to appropriate entities to mitigate the effects of its cyber incident. See our insight here for more information on these amendments.</p>

PROPOSAL

AGREED
(draft legislation to come)

AGREED-IN-PRINCIPLE
(further consultation likely)

KWM COMMENT

Consider further methods of streamlining multiple reporting obligations (Proposal 28.1).



(for further consultation)

This will come as a relief for many organisations currently struggling to reconcile overlapping and sometimes inconsistent reporting obligations. It is also a proposed initiative that is being considered in the context of the Government’s 2023-2030 Cybersecurity Strategy.

Implement new organisation accountability requirements, such as appointment of a senior employee with responsibility for privacy (Proposal 15.2), taking steps to ensure that information obtained from third parties was collected lawfully (Proposal 13.4), and undertaking Privacy Impact Assessments for high privacy risk activities (Proposal 13.1).



Many organisations already delegate privacy compliance to a privacy or data protection officer (in alignment with the requirements of the GDPR) but this amendment may formalise such appointments. Additional organisational accountability obligations in relation to information obtained from third parties has been proposed in recognition of concerns about the continued use and disclosure of personal information with uncertain origins (including that may have originated from a data breach).

Somewhat surprisingly, the Government has decided to consult further in relation to when and how organisations must conduct Privacy Impact Assessments - these are currently mandatory for Commonwealth Government agencies, and many private sector organisations act consistently with those requirements.

The OAIC should develop practice-specific guidance for new technologies and emergency privacy risks (Proposal 13.3) and further consideration should be given to enhanced requirements in the context of facial recognition technology (Proposal 13.2).



(for further guidance and consultation)

The Government has recognised the need for further consultation in the context of the enhanced risk assessment requirements posed by facial recognition technology and other uses of biometric information. At the same time, the Government is currently seeking to formalise its digital identify and verification regime, and it makes sense for these reforms to be considered in a coordinated fashion. See our recent alert [here](#).

Privacy policies should set out the types of personal information that will be used to make substantially automated decisions that have a



In the wake of the intense public scrutiny regarding use of generative AI and the ‘Robodebt’ fallout, it is hardly surprising that the Government is taking a particularly cautious approach in relation to the use of personal information for automated decision-making. However,

PROPOSAL

AGREED
(draft legislation to come)

AGREED-IN-PRINCIPLE
(further consultation likely)

KWM COMMENT

significant effect on individuals (Proposals 19.1 & 19.2) and individuals should have a right to request meaningful information about how such decisions are made (Proposal 19.3).

this is still a complex area. In particular, it can be hard to draw a bright line between decisions that are partially or ‘substantially’ automated, as in many cases some level of automation will be used in conjunction with human oversight to make decisions at scale. The Government has indicated that further consideration will be given to this to ensure that compliance requirements are ‘appropriately calibrated’.

Certainly what has been proposed falls short of requirements of the GDPR in Europe that requires individuals to be given the right not to be subject to a decision based on automated processing including profiling, which produces legal effects concerning or affecting them.

Define concepts of ‘direct marketing’, ‘targeted advertising’, ‘targeting’ and ‘trading’ in personal information (Proposal 20.1).



This was one of the more confusing areas in the Privacy Act Review Report and will be of keen interest to providers of online services that operate on an ad-supported business model.

Importantly, the Government notes that there should be a distinction drawn between advertising based on tracking online behaviour versus contextual advertising based on the content of a webpage being viewed in real time, with the former clearly being considered more intrusive from a privacy perspective. The Government also notes calls to distinguish between ‘traditional’ forms of direct marketing, such as direct email and SMS marketing, from online targeted advertising (a distinction that is not very apparent in the current form of the Privacy Act).

Perhaps controversially, the Government suggests that ‘trading of personal information’ underpins delivery of targeted content and advertising on many online services, though we expect that many online service providers, who have invested significant energy in developing privacy enhancing technologies to deliver relevant material in a less privacy intrusive manner, would quibble with that characterisation.

PROPOSAL

AGREED
(draft legislation to come)

AGREED-IN-PRINCIPLE
(further consultation likely)

KWM COMMENT

There should be an unqualified right to opt-out of personal information being used or disclosed for direct marketing (Proposal 20.2).



The Government has indicated that further consideration will need to be given to the interaction between the Privacy Act and consent / opt-out frameworks established under specialist spam and telemarketing laws. Notably, as flagged below, the Government has only ‘noted’ (and not ‘agreed’ or ‘agreed-in-principle’) the equivalent unqualified opt-out that was proposed for targeted advertising, and could have threatened the viability of ad-supported online services.

Targeting individuals should be fair and reasonable in the circumstances, and targeting based on sensitive information should be prohibited except for socially beneficial content (Proposal 20.8). The Government has only ‘noted’ and not endorsed the proposal to provide individuals with an unqualified right to opt-out of receiving targeted advertising. (Proposal 20.3).



The Government has indicated that further consideration will be given to how to give individuals more choice and control in relation to the use of their information for targeted advertising. This could include through development of industry codes to specify what control individuals should have over the use of their information in online advertising. This is a clear step back from the proposal in the Privacy Act Review Report to provide an absolute right to opt-out from targeted advertising, and will come as a (perhaps temporary) relief to the online advertising industry. As noted above, the introduction of an unqualified opt-out could have threatened the viability of ad-supported online services, and possibly resulted in consumers having to pay for services that they currently receive for free. The Government’s more cautious approach here stands out, given it is one of the few proposals in the Privacy Act Review Report that it has not positively endorsed. This is likely a response to the concerns that many online service operators undoubtedly raised in their submissions to Government on this issue.

Entities should provide information to online users about the use of targeting systems, including information about the use of algorithms and profiling to



This proposal will need to link closely with Government’s consideration of the Safe and Responsible Use of AI (read KWM’s submission on that consultation [here](#)). Recommendation and profiling engines are underpinned by much sensitive IP, and also to some degree the operation of some automated algorithms may not be comprehensible to a human, and certainly not to an average consumer. It will be

PROPOSAL

AGREED
(draft legislation to come)

AGREED-IN-PRINCIPLE
(further consultation likely)

KWM COMMENT

recommend content to individuals (Proposal 20.9).

important for regulations in this area to remain focussed on information that is meaningful to consumers, and does not threaten valuable investments being made by entities in economically useful technologies.

A child should be defined as a person under the age of 18 (Proposal 16.1), and a Children’s Online Privacy Code should be developed as soon as possible to keep children safe online (Proposal 16.5).



The Government has indicated that a Children’s Online Privacy Code - which could be developed as soon as a supporting legislative framework is in place (and potentially in advance of other broader reforms that would apply to adult users) - should align with international approaches including the UK Age Appropriate Design Code. While The Government agrees that a code is required, it recognises that further consultation with relevant stakeholders is required in order to inform its development.

Key theme 3: Increase clarity and simplicity for entities and individuals

A distinction between controllers and processors of personal information should be introduced into the Act (Proposal 22.1).



The Government’s in-principle support for introducing a controller-processor distinction will come as great news for outsourcers and technology service providers who help their clients manage their data assets. As the Government notes, this will bring Australia into line with other jurisdictions that already make this distinction. It will be particularly relevant, for example, in relation to transparency obligations, reporting data breaches, and dealing with individual data subject rights where data processors who do not have a direct relationship with relevant individuals currently have a hard time complying with the Act.

The ability for the Information Commissioner to make APP codes should be enhanced (Proposals 5.1 & 5.2).



It is clear from the broader package of reforms that the Government sees codes as an important way to supplement the operation of the Act in certain areas - for example, as noted above the Government has committed to the development of a Children’s Online Privacy Code, and elsewhere has signalled that codes may have a role to play in

PROPOSAL

AGREED
(draft legislation to come)

AGREED-IN-PRINCIPLE
(further consultation likely)

KWM COMMENT

A mechanism should be introduced to prescribe countries with substantially similar privacy laws to Australia (Proposal 23.2).



imposing additional requirements around online advertising (e.g. as to specific opt-out controls that must be provided).

This will come as a great relief to organisations that have previously had to make their own independent assessments as to the adequacy of overseas privacy regimes, or else rely on other mechanisms to transfer personal information overseas. It is hoped that this will enable freer exchanges between entities in the UK and the EU, though may not help facilitate transfers to other major trading partners of Australia that have quite different legal regimes which makes it less easy to draw parallels between their privacy frameworks and those in Australia. For example, in the US the lack of a consistent Federal privacy framework may make it less likely that findings of adequacy will be made. Accordingly, it is likely that other cross-border data transfer mechanisms will remain essential.

Undertake further consultation on the extraterritorial provisions of the Privacy Act to determine whether they should be amended to narrow the current scope (Proposal 23.1).



One of the more controversial aspects of the changes to the Privacy Act that were rushed through late last year was the adjustment of the ‘Australian link’ test so that the Act will apply to conduct by a foreign company outside Australia as long as the company is carrying on business in Australia. The previous limitation that the Act would only apply where the company had collected or held relevant information in Australia was deleted.

Following that change, a literal reading of the Act suggests that foreign companies who carry on business here as part of a global enterprise must comply with Australian privacy laws in relation to all information they hold, irrespective of whether that information has any connection with Australia. This could mean that such a company technically must comply with the Act even in relation to information about customers in other jurisdictions. This was a significant, and most likely unintended expansion, and the reintroduction of some additional limitation to

PROPOSAL	AGREED (draft legislation to come)	AGREED-IN-PRINCIPLE (further consultation likely)	KWM COMMENT
			ensure the Act remains suitably focussed on issues affecting Australia and Australians would be welcome.

Key theme 4: Improve transparency and control

Consent should be voluntary, informed, current, specific and unambiguous (Proposal 11.1), with individuals having the right to withdraw consent in an easily accessible manner (Proposal 11.3). The OAIC should prepare guidance on how online services can design consent requests (Proposal 11.2).



The changes requiring consent to be voluntary, informed, current, specific and unambiguous largely align with the way that current consent requirements under the Act are being interpreted and applied by the OAIC. It is interesting to note that the Government has recognised the strong pushback from industry and other stakeholders on consent as the foundation for privacy protection, as consent controls become less effective when overused. Specifically, the Government’s response states that *‘Reserving consent for high privacy risk situations reduces the risk of individuals experiencing consent fatigue and avoids placing an unnecessary compliance burden on entities to obtain consent in situations where a collection, use or disclosure of personal information would be reasonably expected by the individual or broader community.’* Accordingly, consents should be used sparingly and typically only for processing activities that an individual would otherwise not reasonably expect.

However we think that the implementation of the ability of individuals to withdraw consent, not just from direct marketing or collection of sensitive information, but also from collection, use or disclosure could be more difficult to implement in practice. Organisations may not tag information in their systems in a way that easily enables this withdrawal to be effected. Individuals may not realise that withdrawal of consent only applies to consents given for ‘high privacy’ risk situations as discussed above, and may not apply to uses or disclosures that are for a primary purpose or a secondary related purpose (where consent is not the basis of the use or disclosure). We do support further consultation on this issue.

PROPOSAL

AGREED
(draft legislation to come)

AGREED-IN-PRINCIPLE
(further consultation likely)

KWM COMMENT

Privacy notices should be clear, up-to-date, concise and understandable (Proposal 10.1), with standardised templates (including standardised icons, layouts and phrases) developed for voluntary adoption (Proposal 10.3).



Few would argue that a directive to improve the quality of consumer-facing privacy notice is a bad thing. While some may consider a level of standardisation will be helpful to enhance consumer awareness and understanding, it will be equally important to avoid overly prescriptive requirements that prevent businesses (particularly those that operate on a global basis) from providing notices that are tailored to their unique circumstances in a way that best meets the needs of their customer base.

Individuals should have new individual rights to request an explanation of what is being done with their information (Proposal 18.1), to object to the handling of their information (and to require an entity to justify their actions) (Proposal 18.2), to delete / erase their information (Proposal 18.3), to request correction of online publications (Proposal 18.4), and require de-indexation of certain online search results (Proposal 18.5). Individuals should be notified of these rights at the time that their information is collected (Proposal 18.7).





This is one of the areas where the reforms will need to strike a delicate balance. The Government recognises that the introduction of new individual rights will need to be subject to exceptions to reflect countervailing interests in freedom of speech, law enforcement and other public interests. The potential regulatory burden of dealing with requests to exercise the new rights will also need to be considered. It seems likely that this will be an area of further active consultation in order to ensure that all relevant interests are considered.

There will be valuable learnings from the EU and other jurisdictions, where similar rights are already in effect, including as to the potential for these rights to be misused / abused in certain circumstances.

Individuals should have more direct access to the courts to seek remedies for breaches of their privacy (Proposal 26.1).



The Government recognises that some threshold would need to apply to any direct right of action for breaches of the APPs, with individuals having to first lodge and conciliate a complaint with the OAIC or a recognised dispute resolution scheme before being able to pursue the matter further in the courts (similar to the current procedure for

PROPOSAL	AGREED (draft legislation to come)	AGREED-IN-PRINCIPLE (further consultation likely)	KWM COMMENT
<p>A statutory tort for serious invasions of privacy should be introduced, based on a model previously proposed by the ALRC (Proposal 27.1).</p>			<p>conciliation of human rights complaints). Available remedies would include damages.</p> <p>As class actions relating to recent major data breaches continue to proliferate, we foresee that proposals such as this one will inevitably lead to a more combative and litigious privacy landscape in Australia in years to come. Litigators (and litigation funders) will be relishing the prospect of being able to explore the operation of laws that, until recently, have had very little consideration by the judiciary.</p> <p>The Government also agrees in-principle that a statutory tort should be introduced, legislating liability for a serious intrusion into seclusion or a serious misuse of private information. The tort include would include additional thresholds, such as requiring intentional or reckless conduct rather than mere negligence, and a public interest test.</p> <p>This would fill gaps where there are invasions of privacy that do not relate specifically to personal information and so are not fully covered by the Privacy Act. It will also put to an end the speculation as to whether the common law in Australia would ever by itself recognise the existence of a separate privacy-related tort or wider application of the law of confidential information</p>
Key theme 5: Strengthen enforcement			
<p>Remove the word ‘repeated’ from s 13G and clarify that a ‘serious’ interference with privacy can include a repeated interference (Proposal 25.2).</p>			<p>As things currently stand, a court is only able to award a civil penalty under the Act in relation to breaches of the APPs that are ‘serious’ or ‘repeated’. As there is currently no judicial precedent to shine light on the meaning of these terms, the operation of this threshold is currently uncertain and represents a significant barrier to the OAIC in bringing enforcement action under the Act. The amendments proposed by the Government will help refine understanding of these terms, but some</p>

PROPOSAL

AGREED
(draft legislation to come)

AGREED-IN-PRINCIPLE
(further consultation likely)

KWM COMMENT

uncertainty will still remain until the courts have an opportunity to have their say.

Introduce new mid-tier and low-tier civil penalty provisions for breaches that do not meet the ‘serious’ threshold, with powers to issue infringement notices for ‘low-level’, set penalty amounts that can be paid without admissions being made (Proposal 25.1).



We expect that the OAIC will become a much more active enforcer once these new powers are introduced. The ACMA has been comparatively successful in enforcing the Spam Act and has regularly used the infringement notice powers given to them under that Act. We anticipate that the OAIC may take a very similar approach in the future, reserving court actions for only the largest scale and most egregious breaches.

Conduct a strategic organisational review of the OAIC to ensure it is structured to have a greater enforcement focus (Proposal 25.10)



In response to questions by the Senate Economics Reference Committee, the OAIC recently confirmed that they had only 8.6 FTE working in their major investigations branch, though there were a total of 45.7 FTE working in the OAIC’s dispute resolution branch more generally. Given the series of major high-profile data breaches that the OAIC is currently investigating, it is clear that the OAIC’s resources are currently stretched and that there may be limited capacity to fight battles on other fronts until some of those matters are resolved. As public concern about privacy issues grows, and the OAIC gains a greater public profile, we expect that there will be support for continuing to build out the OAIC’s enforcement capability.

Investigate the feasibility of an industry funding model for the OAIC, and of the establishment of a contingency litigation fund and a special account to fund high cost litigation (Proposals 25.7 & 25.8).



This was one of the more under-developed proposals in the Privacy Act Review Report. Everyone recognises that the OAIC requires funding and resources to perform an effective enforcement role, but the method of obtaining that funding will inevitably be controversial, and the Government should not underestimate the complexity and administrative cost of imposing any form of industry levy (particularly

PROPOSAL	AGREED (draft legislation to come)	AGREED-IN-PRINCIPLE (further consultation likely)	KWM COMMENT
<p>Give the Information Commissioner additional powers to conduct investigations (Proposal 25.3) and undertake public inquiries and reviews (Proposal 25.4).</p>			<p>given that almost every organisation in Australia collects and uses personal information to some degree in conducting their business).</p> <p>Most significantly, these reforms will give the Information Commissioner the power to enter premises, make copies of documents, operate electronic equipment and seize evidence (to prevent the destruction of evidence).</p> <p>The Government’s support for these proposals is consistent with both the OAIC’s expanding role and the heightened public interest in this area of policy development.</p>