Submission to the Australian Privacy Act Review Discussion Paper

31 JANUARY 2022

Meta

EXECUTIVE SUMMARY

Meta commends the Australian Government on its review of the Privacy Act 1988 (Cth), and appreciates the opportunity to comment on the wide range of proposals contained in the Privacy Act Review Discussion Paper.

It is essential for Australia to have the right framework in place for privacy and data protection. Privacy laws should enable the growth of Australia's digital economy, facilitate cross-border trade and e-commerce, and minimise costs on small businesses and consumers - while providing Australians with confidence about how their data is collected and used online.

Meta has been calling for stronger privacy protections for consumers for some time.[1] Privacy and the protection of people's information are fundamental to our business. Consumers should have meaningful transparency and control over how their information is collected, used and disclosed.

Meta has built industry-leading tools to achieve this for our users. In our submission to the issues paper[2], we outlined information about these tools, such as Off-Facebook Activity, which provides users with a summary of information that other businesses send Meta in order to show them relevant ads, and provides consumers with options to delete that information.

This submission includes information about additional work we have launched since the issues paper was released. We have continued our transparency efforts, launching a new consumer-friendly Privacy Centre to help communicate with consumers about tools we make available to protect their privacy.[3] We have announced privacy-protective changes to how we use data, including: changing how advertisers can reach young people with ads by removing certain targeting options;[4] removing detailed targeting options for all users that relate to topics people may find sensitive, such as health, race or ethnicity, political affiliation, religion, or sexual orientation;[5] and shutting down the Face Recognition system on Facebook as part of our company-wide move to limit the use of facial recognition in our products.[6] We have publicly signalled the innovative work we are doing to develop privacy-enhancing technologies, which minimise the amount of data processed to help protect personal information. And we provide more information about the substantial work Meta has undertaken to ensure our users have age-appropriate experiences on our platforms.

In line with our commitment to stronger privacy protections for Australian consumers, there are many proposals in the discussion paper that we support. Of the 62 proposals discussed in this submission, we support 48 of them in full or in part. We raise concerns in relation to 7 proposals, and there are an additional 7 proposals where we do not have any comment. (Note:

---

[1] M Zuckerberg, 'The Internet needs new rules. Let's start in these four areas', *The Washington Post*, 30 March 2019, https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html.

[2] Meta, 'Submission to the Australian Privacy Act Issues Paper', *Attorney General Website,* https://www.ag.gov.au/integrity/publications/submissions-received-review-privacy-act-1988-issues-paper

[3] Meta, 'Introducing Privacy Centre', *Meta Newsroom,* 7 January 2022, https://about.fb.com/news/2022/01/introducing-privacy-center/

[4] Meta, 'Giving young people a safer, more private experience on Instagram', *Meta Newsroom,* 27 July 2021, https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/

[5] G Mudd, 'Removing certain ad targeting options and expanding our ad controls' *Meta for Business*, 9 November 2021, https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls?ref=search_new_1

[6] J Pesenti, 'An update on our use of face recognition', *Meta Newsroom*, 2 November 2021, https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/

we do not make any comment related to the exceptions for small business, journalism, political parties or employee records).

In particular, we are very supportive of efforts to align Australian privacy law with international privacy standards, such as the European Union General Data Protection Regulation (GDPR).

A global contest is currently underway between differing visions for the internet. The values that underpin the open internet are being challenged by a more authoritarian and closed approach. We encourage countries like Australia to pursue privacy and data protection regulation that is as consistent as possible with the best practice privacy frameworks of leading digital economies in the world, like the GDPR. As the OECD and others have stated, ensuring alignment with global norms enhances Australia's global competitiveness and this type of regulatory harmonisation reduces unnecessary compliance costs and leads to increases in productivity.[7] Crucially, a globally harmonised privacy and data protection framework will ensure that Australians, and people around the world, can continue to benefit from the opportunities afforded by access to an internet which is not fragmented by localised regulatory barriers.

We support many of the discussion paper's proposals that would bring Australia's regime into greater alignment with the GDPR. These include a right to erasure of personal information in certain circumstances, a requirement for entities that engage in certain restricted practices to take reasonable steps to identify and mitigate privacy risks, and measures to facilitate the efficient transfer of data internationally while protecting individuals' privacy.

We also strongly support those measures that seek to give consumers more meaningful and genuine transparency around how their information is collected, used and disclosed. We support new requirements for privacy notices to be clear, current and understandable, for easily accessible privacy settings, for new mandatory disclosure of automated decision making in certain contexts, and for stronger transparency around potential overseas disclosures. We also support the introduction of a statutory tort for invasion of privacy.

In other areas, while we support the proposal in principle, we have highlighted some key areas that we recommend the Australian Government considers. In particular, the establishment of a 'right to object' (requirements to cease using or disclosing consumers' data on request) should be implemented cautiously, especially as it relates to direct marketing. While we strongly support arming consumers with rights to opt out of direct marketing services such as marketing email newsletters, a blanket right to object could impede services that are enabled by advertising-supported business models.

Eroding the ability for businesses to offer free, ad-supported services would adversely impact both consumers and small businesses.

- Australian consumers benefit from being able to access free digital services, funded by personalised advertising that is relevant and useful. Ad-supported business models help ensure easy accessibility of digital services to all consumers - including those who are disadvantaged or otherwise may not be able to afford to pay. In a recent survey, when asked whether they prefer an ad-supported internet where most services are free or an ad-free internet where everything costs money, 84.1 per cent of respondents indicated they would prefer an ad-supported internet.[8]

---

[7] OECD, *OECD Privacy Framework*, https://www.oecd.org/sti/ieconomy/oecd%20privacy%20framework.pdf

[8] Digital Advertising Alliance, 'Americans value free ad-supported online services at $1,400 a year', *Digital Advertising Alliance Website,* September 2020, https://digitaladvertisingalliance.org/press-release/americans-value-free-ad-supported-online-services-1400year-annual-value-jumps-more-200

- The personalised ads-supported internet directly benefits small businesses. A recent report by Deloitte found that 82 per cent of Australian small businesses reported using free, ad-supported Meta apps to help them start their business.[9] It also found that 71 per cent of Australian small businesses that use personalised advertising reported that it is important for the success of their business. Particularly over the past two years, personalised advertising has helped businesses target new customers as they have needed to pivot away from bricks-and-mortar operations during the pandemic.

We recommend clarifying the Government's apparent intention as per the discussion paper to specifically ensure that any right to object - including for direct marketing - should allow companies to cease providing services to individuals who object to their personal information being used in ways that are necessary to provide the service (including the delivery of personalised ads that enable the service without charge).

Similarly, the proposals to change key definitions - such as the definition of 'personal information' or 'consent' - need to be implemented carefully. We recommend including caveats in both instances (that a person must be identified or reasonably identifiable from information for it to constitute personal information; and that consent can continue to be express or implied) to avoid unintended consequences.

Lastly, there are some proposals that are likely to make privacy settings more confusing for consumers. Introducing standardised notices and consents are more likely to increase confusion for consumers, given the diversity of ways in which businesses may use data. A proliferation of codes that set different requirements for different types of businesses will make it more challenging for consumers to understand and exercise their privacy rights. For this reason, we believe the Information Commissioner should allow industry to develop any codes in the first instance and any exemptions to that rule should be carefully targeted. And - as outlined in our submission to the Online Privacy Code - we believe many of the matters proposed in that separate piece of draft legislation would be better considered as part of this cross-economy process.

Finally, we suggest that two proposals in particular are impractical and raise concerns. The first is the requirement to notify consumers as a primary purpose when use or disclosure of the information is "to influence an individual's behaviour or decisions". This proposal seems narrowly designed to disparage online targeted advertising, while overlooking other forms of advertising (and, indeed, non-advertising businesses) that use data in very similar ways. It is also unlikely to result in improved consumer privacy outcomes, given that consumers already understand that advertising services may raise awareness about products, services, events or causes that they were not previously aware of.

We also have concerns about the proposal for the Government to introduce an industry funded model for the Office of the Australian Information Commissioner (OAIC) via a narrow and arbitrary statutory levy limited to certain categories of entities, such as social media companies. While we believe the regulator should have sufficient resourcing to implement its duties, any industry contribution requirements should be equitable. It is illogical to require social media companies to be primarily responsible for industry contributions to the regulator when the OAIC's own annual report indicates that the finance sector, the Australian Government, the health sector and the retail industry all garner more complaints than online services.

We would welcome the opportunity to discuss any of these comments further with Australian policymakers.

---

[9] Deloitte, 'Dynamic Markets Report: Australia - unlocking small business innovation and growth through the personalised economy', *Meta Australia blog,* October 2021, https://australia.fb.com/economic-empowerment/

SUMMARY OF META'S SUBMISSION

Section of the discussion paper	Summary of Meta's response
1.1 Objects of the act	We have no comments on this proposal.
2.1 Amend 'about' to 'relates to' in the definition of personal information	**Support** on the basis that 'personal information' retains the requirement that a person must be identifiable for it to constitute personal information.
2.2 Non-exhaustive list of information covered by personal information	**Support** on the basis that examples should not include technical data that has little bearing on an individual's privacy, and the list should be drafted in a way that is flexible and technology-neutral.
2.3 'Reasonably identifiable' includes when an individual can be identified, directly or indirectly	**Support** this proposal.
2.4 Definition of 'collection' to include information obtained by any source or means	**Support** this proposal. However, we believe the law can protect individual privacy while also respecting the unique nature of generated information, which may be the product of significant intellectual effort. Rights to access, objection or erasure should not be extended in such a way that would reduce the incentives for businesses to engage in technical innovation that may result in generated information.
2.5 Anonymisation of personal information	**Support** in principle, provided there are clear guidelines around the definition and standard of 'anonymisation'.
2.6 Reintroduction of the *Privacy Amendment (Re-identification) Offence Bill 2016*	**Support** this proposal.
3.1 Enable the Information Commissioner to make an APP Code on direction of the Attorney-General	**Recommend** that industry is given the first chance to develop any industry codes under privacy legislation, to ensure the Code best considers industry-specific dynamics before inviting direct intervention by the Information Commission. There are already a number of examples, such as the Industry Code of Practice on Misinformation and Disinformation, that demonstrate industry can effectively develop regulatory codes.
3.2 Temporary APP Code on the direction of the Attorney General	**Support** in principle however we recommend, in line with 3.1, that industry be provided the opportunity to comment on the Code before it is put into practice.
3.3 Emergency Declarations	**Support** this proposal.
3.4 Engagement with state and territory authorities during an Emergency Declaration	**Support** this proposal.
8.1 Express requirement that APP 5 privacy notices are clear,	**Support** this proposal. At Meta, we are committed to upholding people's basic rights to be informed about how

current and understandable	their information is collected and processed. We believe this empowers them to make choices about how they participate online and share their data.
8.2 APP 5 notices limited to the following matters under APP 5.2	**Support** this proposal.
8.3 Standardised privacy notices	**Recommend** the introduction of an express requirement that privacy notices must be clear, current and understandable, rather than standardised. This will reduce the risk that standardised notices lead to consumer confusion, and recognises that businesses should clearly explain their own unique approach to privacy.
8.4 Strengthened requirement for when an APP 5 collection notice is required	**Support** in principle, as we strongly support privacy notice requirements. However we believe that the "impossibility" standard sets a remarkably high bar. We consider that a more balanced position should apply where any privacy benefits derived from the collection notice need to be weighed against the costs of providing the notice. There should also be an express acknowledgement that a separate collection notice is not required where personal information is collected by a third party service, so long as the information is only being processed within the scope of the customer's directions.
9.1 Consent is voluntary, informed, current and specific	**Support** in principle, provided that the role of consent remains as it currently is under the APPs. In particular, valid consent should continue to be either express or implied, and the definition of 'current' should not be drafted so as to necessitate renewal where there has been no change to the scope of using the information.
9.2 Standardised consents	**Recommend** the introduction of an express requirement that privacy notices must be clear, current and understandable, rather than standardised, in line with our response to proposal 8.3.
10.1 Collection, use or disclosure under APP 3 and APP 6 must be fair and reasonable	**Support** this proposal.
10.2 Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable	**Support** this proposal. However, in implementing these changes, it will be important to ensure that there is no unnecessary duplication of compliance obligations under the APPs in a way that could lead to uncertainty or inconsistency in the way different APPs are applied in practice.
10.3 Reasonable steps to collect information under APP 3	**Support** in principle, subject to seeing further guidance as to how the "reasonable steps" standard will be applied in practice. We consider that in almost all cases this standard should be satisfied by obtaining a suitable contractual warranty or other written assurance from the third party.
10.4 Definition of 'primary' and 'secondary' purpose	**Support** on the basis that organisations will have flexibility to clearly define the relevant primary purposes for which they

	collect personal information. Otherwise, the effect of narrowing the range of permitted "secondary purposes" will be to force organisations to rely more heavily upon consent.
11.1 Restricted and prohibited acts and practices	**Support Option 1**, which broadly aligns with obligations that apply under the GDPR as well as the way that we understand the OAIC is currently applying existing general compliance obligations under APP 1.2 in practice.
12.1 Pro-privacy default settings	**Strongly support Option 2** as it provides businesses with the flexibility to offer differing privacy defaults depending on the nature of the service and the age of the user, and also provides users with the control to choose privacy settings that best suit their individual wishes.
13.1 Children and vulnerable individuals	**Recommend** that any changes to the Act in this regard should be aligned with the equivalent rules within the Online Privacy Bill and Online Privacy Code.
13.2 APP 5 notices clear, current and understandable, specifically for a child	**Support** this proposal.
14.1 Right to object and portability	**Support** in principle, however this proposal is significantly broader than the equivalent right under the GDPR. It is critical that allowance is made for continued collection, use or disclosure in appropriate circumstances. In particular, an entity should not be required to fundamentally alter its business model in order to comply with the right to object.
15.1 Right to erasure where one of the grounds applies	**Support** this proposal.
15.1 Provide for exceptions to an individual's right to erasure of personal information	**Support** this proposal and consider that, if a right to erasure is introduced, it should be subject to appropriate exceptions equivalent to those that apply under Article 17 of the GDPR at a minimum. This would necessitate providing exceptions where the retention of the personal information is required for freedom of expression, for a public interest purpose, for complying with a legal obligation, or for establishing or defending a legal claim.
15.3 An APP entity must respond to an erasure request within a reasonable period.	**Support** this proposal.
16.1 The right to object include an unqualified right to object to any collection, use or disclosure for the purpose of direct marketing	**Recommend** that, in line with our response to proposal 14.1, if a right to object is introduced as contemplated by this proposal, it should be expressly stated that a service provider may deny access to an ad-supported service if a user objects to the collection, use or disclosure of their personal information for the purposes of providing personalised ads on that service.
16.2 Use of disclosure of personal information for the purpose of influencing an	**Raise concerns** about the effects of this proposal. While we support transparency for consumers in how their data is used, it is not clear (1) why this proposal takes such a narrowly

individual's behaviour must be a primary purpose notified to the individual	defined view of "influence" or (2) why other proposed legislative changes would not already address any policy concerns here.
16.3 APP entities would be required to include the following additional information in their privacy policy	Please refer to our comments in response to proposal 16.2 above.
16.4 Repeal APP 7	**Support** this proposal.
17.1 Automated decision-making	**Support** this proposal.
18.1 Identifying the source of personal information on request by the individual	**Support** this proposal but suggest that any amendment requires organisations to provide 'any available information' as to the source of personal information. This would achieve closer alignment with requirements under GDPR Article 15.
18.2 Introduce additional grounds on which an APP organisation may refuse a request for access	**Support** this proposal.
18.3 Clarify the existing access request process in APP 12	**Support** this proposal.
19.1 Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.	**Support** this proposal.
19.2 List of factors that indicate what reasonable steps	**Support** this proposal.
19.3 Amend APP 11.2 to require entities to take *all* reasonable steps to destroy the information or ensure that the information is *anonymised*	**Support** this proposal, subject to our comments on proposal 2.5 above.
20.1 Organisational accountability requirements targeting measures to where there is the greatest privacy risk	**We do not object to this proposal, though we query** whether it would add meaningfully to the level of privacy protection that individuals would enjoy under the Act, particularly taking into account other protections contemplated within the discussion paper.
22.1 Mechanism to prescribe countries and certification schemes under APP 8.2	**Support** this proposal.
22.2 Standard Contractual Clause	**Support** this proposal.
22.3 Remove the informed consent exception in APP 8.2	**Support** this proposal.
22.4 Transparency requirements in relation to potential overseas	**Support** this proposal.

disclosures	
22.5 Definition of 'disclosure'	**Support** this proposal.
22.6 Clarify what circumstances are relevant to determining what 'reasonable steps' are for the purpose of APP 8.1.	**Support** this proposal.
23.1 Implementation of the CBPR system	**Strongly support** this proposal.
23.2 Voluntary domestic privacy certification scheme	**Support** this proposal.
24.1 Tiers for civil penalty provisions	We have no comments on this proposal.
24.2 Clarify what is a 'serious' or 'repeated' interference with privacy.	**Support** clarification on the list of factors to be considered in determining whether or not a breach is captured by s13G. However, the relevant test should always be whether or not the breach was "serious" or "repeated", especially given the substantial penalties associated with s13G.
24.3 Powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014	We have no comments on this proposal.
24.4 IC powers to undertake public inquiries and reviews	We have no comments on this proposal.
24.5 APP entity to identify, mitigate and redress actual or reasonably foreseeable loss	We have no comments on this proposal.
24.6 Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established	**Support** this proposal. However, in order to avoid risk of overlapping or inconsistent orders, it should be made clear that where the Court finds that there has been a serious breach and makes orders under section 13G, the Information Commissioner should not be allowed to separately issue a determination on the same matter under section 52.
24.7 Industry funding model	**Recommend** that any industry contributions to a funding model be considered more broadly than is contemplated in the discussion paper, and consider those industries that are responsible for the majority of privacy complaints.
24.8 Annual reporting requirements	We have no comments on this proposal.
24.9 Alternative regulatory models	We have no comments on this proposal.
25.1 Direct right of action	**Raise concerns** with the introduction of a direct right of action and instead recommend that the introduction of a statutory tort of privacy would sufficiently achieve the underlying policy objectives here. A direct right of action should only be allowed where:

	• the Commissioner confirms that attempts at conciliation by the Commissioner have not been successful; and • the proceeding relates to a serious interference with privacy. Care should be taken to ensure consistency with a statutory tort for serious invasions of privacy.
26. A statutory tort of privacy	**Support** the introduction of a statutory tort for serious invasions of privacy as was recommended by the ALRC in Report 123. Care should be taken to ensure consistency with any direct right of action.
27.1 Notifiable Data Breaches scheme	**Support** this proposal. However, it would be helpful to expressly clarify that there will be no requirement to include any confidential information in the notice, or anything else that may compromise any information security procedures that the reporting entity may have in place.
28. Interactions with other schemes	**Strongly support** any attempts to harmonise privacy rules and regulations, both in line with domestic regulatory reforms, and global frameworks. This will reduce the risk of overlap or inconsistency across different laws, both domestically or internationally, which could result in an inconsistent or confusing experience for users, and a high compliance burden for businesses.

TABLE OF CONTENTS

PRIVACY AT META

Privacy and the protection of people's data are fundamental to our business - our company's success is dependent on ensuring digital trust, and privacy and protecting data are at the heart of this.

In addition to building privacy into our products and empowering users to control their privacy, we regularly work with policymakers, regulators, academics, civil society, businesses and other stakeholders to develop new and innovative approaches to a range of privacy issues.

Our submission to the issues paper outlined in detail the innovative and industry-leading work that we have been doing to provide all our users, including in Australia, with transparency and control of their data. Given that submission was made 12 months ago, we outline here a number of relevant updates, in order to provide information about our proactive work.

Below we provide more information about developments over the last year in relation to:

- Announcements of privacy-protective changes in how we use data;
- Updates on our privacy tools;
- Privacy-enhancing technologies; and
- Age-appropriate experiences (given the data of young people is a key priority for the Australian Government, as flagged in the Online Privacy Code draft legislation).

Recent announcements

We regularly review and update our products to reflect feedback from stakeholders on privacy expectations. Over the last twelve months, we have announced a number of privacy-protective changes in how we use data, including:

- **Limiting the use of facial recognition.** In November 2021, as part of a company-wide move to limit the use of facial recognition in our products, we announced we will shut down the Facial Recognition system on Facebook.[10] This means that those who have opted in to our Face Recognition setting will no longer be automatically recognised in photos and videos, and we will delete the facial recognition template used to identify them. This change will represent one of the largest shifts in facial recognition usage in the technology's history, and will result in the deletion of more than a billion people's individual facial recognition templates.

  Looking ahead, we still see facial recognition technology as a powerful tool in specific instances, such as helping someone gain access to a locked account, or to unlock a personal device. We believe facial recognition can help products like these when privacy, transparency and controls are in place, and when a user has the ability to determine how and how their face is used. However, there are many concerns about the place of facial recognition technology in society, and regulators are still in the process of providing a clear set of rules governing its use. Amid this ongoing uncertainty, we believe that limiting the use of facial recognition to a narrow set of use cases is appropriate. We will continue working on these technologies and engaging outside experts.

- **Removing certain ad targeting options and expanding ad controls.** In November 2021, we announced we would remove Detailed Targeting options that relate to topics people

[10] J Pesenti, 'An update on our use of face recognition', *Meta Newsroom*, 2 November 2021, https://about.fb.com/news/2021/11/update-on-use-of-face-recognition/

may perceive as sensitive.[11] This means that topics such as those that relate to health or sexual orientation, will no longer be used to define an advertisement's audience. In addition to these updates, we have announced new controls to help people determine the types of ads they see, and opt to see fewer ads related to certain topics such as politics, parenting, alcohol, gambling and weight loss.

These changes have been informed by extensive consultation with experts. They demonstrate our commitment to better matching people's evolving expectations for how advertisers may reach them on our platform, and address feedback from civil rights experts, policymakers and other stakeholders on the importance of preventing advertisers from abusing the targeting options we make available.

- **Changing how advertisers can reach young people.** In July 2021, we announced we will only allow advertisers to target ads to people under 18 based on their age, gender and location.[12] This means that previously available targeting options, like those based on interests or on their activity on other apps and websites, are no longer available to advertisers. When young people turn 18, we'll notify them about targeting options that advertisers can use to reach them, and outline tools we provide to control their ad experience.

  We believe in showing people relevant ads so they can discover and purchase products that are interesting to them, and we give users a number of controls to manage their experience and interests in their ad settings. However, we've heard from youth advocates that young people may not be well equipped to make these decisions. This is why we're taking a more precautionary approach in how advertisers can reach young people with ads.

Privacy tools

We seek to build every product to be transparent so that people can understand how we collect, use and share data on demand. We also focus on communicating important information proactively, clearly and contextually.

Meta also maintains a public help center where anyone who visits the site can access and learn about privacy, safety, policies, reporting, how to use Facebook, and Facebook account management. People can also visit Meta's Privacy Shortcuts page for quick access to privacy and security settings, as well as our Data Policy page for an explanation of the information we process to support Facebook, Instagram, Messenger and other products and features offered by Meta.[13]

We have also recently announced the launch of a new, global Privacy Centre. The Privacy Centre will be a user-friendly, centralised hub for users to learn about our approach to privacy across our apps and technologies.

The Privacy Centre will provide up to date, transparent and understandable information on our approach to collecting and using user information. This will include modules on five common privacy topics: sharing, security, data collection, data use and ads; education on user's privacy

---

[11] G Mudd, 'Removing certain ad targeting options and expanding our ad controls' *Meta for Business*, 9 November 2021, https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls?ref=search_new_1

[12] Meta, 'Giving young people a safer, more private experience on Instagram', *Meta Newsroom*, 27 July 2021, https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/

[13] Facebook, *Facebook Help Center*, https://www.facebook.com/help/; Facebook, *Tools to help you control your privacy and security on Facebook*, https://www.facebook.com/privacy/

options and our privacy tools; and communications about our privacy updates. The Privacy Centre is being trialed initially, and will roll out to more people and apps in the coming months.[14]

Our last submission outlined the tools that Meta has built to give people transparency and control over how their data is used. These tools include:

- **Manage Activity.** Manage Activity puts in one place the functions users need to search their activity and archive or delete as they choose.
- **Privacy Checkup.** In 2014, we launched the Privacy Checkup tool which gives users a prompt to double-check their existing privacy settings and make sure they are still comfortable with them.[15] We continue to update this tool, and in January 2021 we introduced a new module that provides users with more information about how their ads are personalised.

  In 2021 to mark Data Privacy Day, we showed a notification in News Feed encouraging people to review their privacy settings using the Privacy Checkup tool.[16]
- **Off-Facebook Activity.** From January 2020, we have made a new tool available around the world called Off-Facebook Activity, which marks a new level of transparency and control.[17] This tool was unprecedented when it was launched, and we believe it remains unmatched today.

  Some businesses send Facebook information about users' activity on their sites and we use that information to show ads that are relevant to those users. Off-Facebook Activity provides users with a summary of that information and gives a control for users to clear that information from their account.
- **"Why am I seeing this ad?".** Users are able to understand why they are seeing an ad, including how factors like basic demographic details, interests and website visits contribute to the ads in News Feed. Users are able to change their Ad Preferences through the tool, if they decide that they want to take steps to ensure they don't see similar ads in future.

Privacy enhancing technologies

We continue to invest in research and development of privacy-enhancing technologies (PETs), which can help to protect personal information in a variety of contexts. In August 2021, we announced that we are investing in a multi-year effort, in partnership with academics, global organisations and developers to build new, privacy-enhancing solutions for the next generation of advertising.[18]

PETs involve advanced techniques drawn from the fields of cryptography and statistics to help minimise the data that's processed for advertising, while preserving critical functionality like ad

---

[14] Meta, 'Introducing Privacy Centre', *Meta Newsroom,* 7 January 2022, https://about.fb.com/news/2022/01/introducing-privacy-center/
[15] Meta, 'Guiding You Through Your Privacy Choices', *Meta Newsroom*, 6 January 2020, https://about.fb.com/news/2020/01/privacy-checkup/
[16] Meta, 'Recapping on our privacy controls on Data Privacy Day', *Meta Newsroom,* 28 January 2021, https://about.fb.com/news/2021/01/recapping-our-privacy-controls-on-data-privacy-day/
[17] M Zuckerberg, 'Starting the Decade By Giving You More Control Over Your Privacy', *Meta Newsroom*, 28 January 2020, https://about.fb.com/news/2020/01/data-privacy-day-2020/
[18] Meta, 'What are privacy-enhancing technologies (PETS) and how will they apply to ads?', *Meta Newsroom,* 11 August 2021, https://about.fb.com/news/2021/08/privacy-enhancing-technologies-and-ads/

measurement and personalisation. For example, one PET we have developed, known as On-Device Learning, trains an algorithm from insights processed right on a user's device without having to send individual data to a remote service or cloud. This technology could help us find new ways to show people relevant ads, without needing to ever learn about specific actions individuals take on other apps and websites.

We continue to invest in research and innovation to inform these new PET products. In 2020, we funded $2USD million towards research on privacy preserving technologies, user experiences in privacy, and privacy in AR/VR and smart device products. In 2021, we focussed our funding on Privacy-Enhancing Technologies. Australian researchers Taeho Jung (University of Notre Dame), Olya Ohrimenko (University of Melbourne) and Kanchana Thilakarathna and Albert Zomaya (University of Sydney) were all granted funding towards their privacy-enhancing research.[19]

Ensuring age-appropriate experiences

Protecting our users - particularly young people - is of paramount importance. Meta works hard to proactively offer products, tools and controls that give young people age-appropriate and privacy-protective experiences.

Meta recognises that regulation has an important role to play in ensuring that young people have safe and age-appropriate experiences online. For this reason, Meta has supported the Government's enhancement of online safety laws via the Online Safety Act.

Globally, the UK's Age Appropriate Design Code has set a benchmark for regulation in this space. In the consultations held by the eSafety Commissioner on age verification and the Attorney-General's Department on the Online Privacy Code, we commended the United Kingdom's Age Appropriate Design Code as a good starting point for regulators in Australia considering new requirements for protecting the data of young people.

Facebook and Instagram already have a number of measures in place to provide an age-appropriate experience to those between the ages of 13 and 18, including but not limited to:[20]

- **Defaulting new teen accounts to private.** We default all new Instagram users who are under the age of 16 in Australia onto a private account.
- **Implementing privacy-protective default settings.** There are a range of other default limits that are placed on a minor's account on Facebook. For example, profiles of minors cannot be found on Facebook nor do we allow search engines to index profiles of minors off our platform; Post and Story audiences are defaulted to Friends (rather than public); and Location is turned off by default.
- **Encouraging existing teen accounts to be private.** For young people who already have a public account on Instagram, we show them a notification highlighting the benefits of a private account and how to change their privacy settings. We'll still give young people the choice to switch to a private account or keep their current account public if they wish.

---

[19] Meta, 'Facebook announces winners of research awards in privacy', *Meta Research*, 13 May 2020, https://research.facebook.com/blog/2020/05/facebook-announces-winners-of-research-awards-in-privacy/; Meta, 'Announcing the winners of the explorations of trust in AR, VR, and Smart Devices request for proposals', *Meta Research,* 16 September 2020, https://research.facebook.com/blog/2020/09/announcing-the-winners-of-the-explorations-of-trust-in-ar-vr-and-smart-devices-request-for-proposals/

[20] Meta, 'Giving young people a safer, more private experience on Instagram', *Meta Newsroom,* 27 July 2021, https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/

These controls put a number of default protections in place for those under the age of 18. They also help to empower young people to make the right choices about their experience online, and the information they want to see and share.

We're continuing to invest in research and innovation that will help us build privacy-safe products and develop new ways to process data. We'll continue working with policymakers, privacy experts and others on emerging privacy areas as we build solutions to ensure people feel safe and comfortable using our products.

SPECIFIC RESPONSES TO DISCUSSION PAPER PROPOSALS

1. Objects of the Act

1.1 Amend the objects in section 2A, to clarify the Act's scope and introduce the concept of public interest, as follows:

(a) to promote the protection of the privacy of individuals *with regard to their personal information*, and

(b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities *undertaken in the public interest*.

We have no comments on this proposal.

2. Definition of personal information

2.1 Change the word 'about' in the definition of personal information to 'relates to'.

We broadly support this proposal but only on the basis that any change to the definition of 'personal information' retains the requirement that a person must be identified or reasonably identifiable from information for it to constitute personal information.

The definition should not be updated in such a way as to remove the need for some meaningful link between the information in question and the relevant identified or identifiable individual. This link ensures that companies are required to put in place protections that are proportionate. Without it, large swathes of operational and technical information could be caught within the scope of Australian privacy legislation, to the extent that it may become simply unworkable to provide services that are beneficial for consumers.

2.2 Include a non-exhaustive list of the types of information capable of being covered by the definition of personal information.

We broadly support this proposal. Providing non-exhaustive examples can assist companies in understanding the Government's intended scope of the legislation.

However, there are two critical issues to note.

First, care should be taken not to include such expansive examples as to capture technical data that has little bearing on the individual's privacy. Doing so may cause significant operational issues for businesses, especially if rights to object and erasure are to apply, with little corresponding gain from the perspective of the individual. In this regard, we note that proposal 18.3 (under which a general summary or explanation would suffice where an access request would otherwise require the provision of personal information that is highly technical in nature) already implicitly recognises that there is little direct value to the individual in having access to or control over technical data. Privacy regulations should focus on information that is meaningful to the individual and so a cautious approach should be taken to including examples in the Act.

Secondly, any list should be drafted in such a way that it remains flexible and technology-neutral. The guidance produced by the OAIC on this topic acknowledges that "The definition is technologically neutral to ensure sufficient flexibility to encompass changes in information-handling practices over time. It is also consistent with international standards and precedents."[21] References to specific categories of technical data may undermine the flexibility of the Privacy Act.

2.3 Define 'reasonably identifiable' to cover circumstances in which an individual could be identified, directly or indirectly. Include a list of factors to support this assessment.

We support this proposal.

2.4 Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.

We broadly support this proposal. However, we believe the law can protect individual privacy while also respecting the unique nature of generated information, which may be the product of significant intellectual effort and investment by the party that is responsible for generating it.

---

[21] See: OAIC, '*What is personal information?',* 5 May 2017, https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/.

The value of that effort should not be undermined by extending individual rights of access, objection and erasure to generated information, without recognition of legitimate business interests. These rights should not be extended in such a way that would reduce incentives for businesses to engage in technical innovation, research and development, and other productive activities that may result in generated information.

For example, as raised in our submission on the Issues Paper,[22] consider how such individual rights could apply to information generated about a job applicant in the course of a recruitment process, such as in the form of opinions generated by an interviewer or results of specific aptitude testing developed by the organisation in question. The organisation's legitimate recruitment activities could be significantly disrupted if an individual job applicant could seek access to that information (as in that case the interviewer will be less likely to make an honest assessment of the applicant) or object to its use or ask for it to be erased (as in that case the value of generating the information would be clearly undermined). Specific exceptions to those individual rights should apply in order to protect the investment made in producing generated information. Unless this investment is protected, incentives to generate useful information that may improve economic efficiency and productivity will decline.

Similar concerns could also arise in an online safety context. Under the Online Safety Act 2021 (Cth), and various supporting frameworks, online service providers will be required to take proactive steps to create and maintain a safe online environment, including to proactively detect and prevent distribution of certain types of harmful content. To meet those requirements, service providers may need to use inferred or generated information to help identify potentially harmful content or to identify end-users that may be involved in the distribution of such content. Clearly it would be disruptive to those safety efforts if individuals could seek to object to that activity or have the inferred or generated information erased.

On that basis, we have suggested that there should be exceptions to the right to object and erasure where personal information is required for safety, security and integrity purposes. Again, individual rights should not necessarily be allowed to undermine the significant broader value, both from a business and from a community perspective, that this type of information may offer.

2.5 Require personal information to be anonymous before it is no longer protected by the Act.

We broadly support this proposal, provided there are clear guidelines so that organisations bound by the Act can objectively assess whether they have met the requisite standard of "anonymisation". It is important that the standard not be set too high as in that case organisations may be deterred from ever seeking to rely on anonymisation and that, in turn, may reduce opportunities to generate value from information even where there is minimal privacy risk. In this regard, we consider that the reference in the discussion paper to information only being "anonymous" where the risk of re-identification is "extremely remote or hypothetical" is unhelpful in assisting entities and consumers to understand the requisite standard. Hypothetical scenarios may not necessarily be remote, and reasonable assessments of risk remoteness may differ.

Any standard of anonymisation should clearly align with requirements under the GDPR, so that a consistent approach can be taken by organisations operating across different jurisdictions. This includes relevant notions of reasonableness as reflected in Recital 26 of the GDPR. Recital 26 indicates that principles of data protection should not apply to data that is rendered anonymous such that the data subject is no longer "identifiable". On the subject of

[22] Meta, 'Submission to the Australian Privacy Act Issues Paper', *Attorney General Website,* https://www.ag.gov.au/integrity/publications/submissions-received-review-privacy-act-1988-issues-paper

identifiability, Recital 26 provides "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."[23]

A similarly balanced approach is recommended by draft guidance produced by the Information Commissioner's Office in the UK, which indicates on this topic that *"even where you use anonymisation techniques, a level of inherent identification risk may still exist. However, this residual risk does not mean that particular technique is ineffective. Nor does it mean that the resulting data is not effectively anonymised for the purposes of data protection law when you consider the context. Also, data protection law does not require anonymisation to be completely risk-free. You must be able to mitigate the risk of re-identification until it is sufficiently remote that the information is 'effectively anonymised'."*[24]

The draft guidance also indicates that the standard of anonymisation must be assessed by reference to the capabilities of the particular organisations concerned: "*In the ICO's view, the same information can be personal data to one organisation, but anonymous information in the hands of another organisation. Its status depends greatly on its circumstances, both from your perspective and in the context of its disclosure. You need to take into account all the means reasonably likely to be used, by yourself or a third party, to identify an individual that the information relates to. This will determine whether the data is anonymous information. We refer to this as the 'reasonably likely' test.*"[25]

Australian law should take a similar approach. Setting a higher bar in Australia would not add meaningfully to the level of privacy protection that Australians enjoy, but would put Australian companies at a disadvantage compared to their international counterparts who have greater flexibility to use appropriately anonymised information to conduct research and development or to develop innovative new service offerings.

2.6 Re-introduce the Privacy Amendment (Re-identification) Offence Bill 2016 with appropriate amendments.

We support this proposal.

---

[23] See General Data Protection Regulation, *Recital 26: Not applicable to anonymous data*, https://gdpr-info.eu/recitals/no-26/

[24] See Information Commissioner's Office, *'Introduction to anonymisation',* May 2021, https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf

[25] Ibid.

3. Flexibility of the APPs

3.1 Amend the Act to allow the IC to make an APP code on the direction or approval of the Attorney-General:

- **where it is in the public interest to do so without first having to seek an industry code developer, and**
- **where there is unlikely to be an appropriate industry representative to develop the code**

We believe that industry should be given the first chance to develop any industry codes under privacy legislation. Where industry-specific dynamics require an industry-specific regulatory response, we consider that it is important to first provide industry with an appropriate opportunity to develop that response in a way that properly takes into account the unique features of that industry before inviting further direct intervention by the Information Commissioner. We recognise that the code-making powers of the Information Commissioner needs to reflect practical realities, and we support the principle of ensuring codes can be developed even if there is no appropriate industry representative.

However, we have concerns that granting the Information Commissioner broad, subjective discretionary powers in determining the "public interest" and developing a code without other checks and balances. This power essentially allows the Information Commissioner to develop binding new regulatory rules, without requiring prior Parliamentary approval, and without any requirement to follow due process in allowing industry a first chance to develop the code.

Firstly, although the Information Commissioner has claimed that this new power is necessary because of the online industry, this industry already has an emerging track record of working together to effectively deliver regulatory codes, for example, in the development of the Australian Code of Practice on Disinformation and Misinformation.[26] This Code commits a diverse set of technology companies to reducing the risk of online misinformation causing harm to Australians.

Secondly, similar legislation with code-making powers, the Online Safety Act, does not contain these requirements. The online industry is already well-advanced in preparing an industry code under the Online Safety Act. Given that the Government has not considered it necessary to grant the eSafety Commissioner powers to develop their own code without industry consultation in "the public interest", there is no justification for granting a power such as this to the IC.

Given that undertaking appropriate stakeholder consultation (including with end-users) and achieving cross-industry alignment will likely require significant time and effort, it will also be important for industry to be given an appropriate period of time to develop any industry code that may be required. We would suggest that a minimum of 12 months be allowed for the development of any new industry code, before the Information Commissioner would be able to intervene.

3.2 Amend the Act to allow the IC to issue a temporary APP code on the direction or approval of the Attorney-General if it is urgently required and where it is in the public interest to do so.

---

[26] J Machin, 'Facebook's response to Australia's disinformation and misinformation industry code', *Facebook Australia Blog*, 21 May 2021, https://australia.fb.com/post/facebooks-response-to-australias-disinformation-and-misinformation-industry-code/,

We support this proposal in principle. However, in line with our response in 3.1, we believe it is important that industry is provided with the opportunity to comment on a Code before it is put in place. We appreciate that in this instance there may be a need to develop a Code urgently, in which case we believe it would be efficacious to offer an expedited consultation timeline. This would give industry the opportunity to (1) provide input on the Code and its practicalities, and (2) begin to prepare for the Code's implementation.

3.3 Amend Part VIA of the Act to allow Emergency Declarations to be more targeted by prescribing their application in relation to:

- **entities, or classes of entity**
- **classes of personal information, and**
- **acts and practices, or types of acts and practices.**

We support this proposal.

3.4 Amend the Act to permit organisations to disclose personal information to state and territory authorities when an Emergency Declaration is in force.

We support this proposal.

4-7. Small business, employee records, political and journalism exemptions

Meta has no comments in relation to the exceptions for small business, journalism, political parties or employee records.

8. Notice of collection of personal information

8.1 Introduce an express requirement in APP 5 that privacy notices must be clear, current and understandable.

We support this proposal.

At Meta, we are committed to upholding people's basic rights to be informed about how their information is collected and processed. Without this crucial information, people cannot make choices about what digital services to use and how to engage with controls offered by companies for limiting and exercising their rights. But we're also aware that while people need to be informed, it doesn't help just to give people more information. People have to be meaningfully informed, in a way that empowers them to make choices about how they participate online and share their data. This means that privacy notices have to be relevant to people's needs and expectations, understandable, accessible, and simple. Over the past few decades, we have worked to make privacy notices more user-friendly by adopting practices like layered privacy policies, just-in-time notices, and in-context notifications. We embrace our responsibility to help people become informed - and stay informed - about how and when their data is collected, shared, and used. As we look to improve our own approaches, we want to work with policymakers, academics, and other companies to find new solutions.

In 2020, we published a White Paper titled "Communicating About Privacy: Towards People-Centred and Accountable Design" where we shared our views on ways to improve privacy notices.[27] Because we know that this isn't an issue that can be solved by a single company, we welcome the opportunity to work with others. For instance, in 2017, we launched "Trust, Transparency and Control Labs," or TTC Labs, to bring together those who work on privacy in government, industry, academia, the design community, and civil society to devise solutions for improving transparency and control across digital services. In Singapore, TTC Labs worked with the Infocomm Media Development Authority to create the "Facebook Accelerator", a startup programme that included a regulatory sandbox. This initiative enabled startups to find new ways to increase the reach of their businesses while maintaining people' s trust and giving them control over their data. Through intensive collaboration efforts like Design Jams, 35 startups in the Accelerator received ongoing compliance guidance and support from regulators, and regulators could better understand startups' business models and design approaches. These Design Jams identified several new design prototypes that are explored in more depth in the TTC Labs report titled, "People-Centric Approaches to Notice, Consent and Disclosure."[28]

8.2 APP 5 notices limited to the following matters under APP 5.2:

- **the identity and contact details of the entity collecting the personal information**
- **the types of personal information collected**
- **the purpose(s) for which the entity is collecting and may use or disclose the personal information**
- **the types of third parties to whom the entity may disclose the personal information**

---

[27] E Egan, 'Communicating About Privacy: Towards People-Centred and Accountable Design', white paper, https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf
[28] Trust, Transparency and Control Labs, 'People-centric approaches to notice and consent disclosure', *TTC Labs*, https://www.ttclabs.net/insight/people-centric-approaches-to-notice-consent-and-disclosure

- **if the collection occurred via a third party, the entity from which the personal information was received and the circumstances of that collection**
- **the fact that the individual may complain or lodge a privacy request (access, correction, objection or erasure), and**
- **the location of the entity's privacy policy which sets out further information.**

We support this proposal.

8.3 Standardised privacy notices could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording and icons. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised notices.

While we support the principle that notices should be clear and transparent, we do not believe standardising privacy notices is an effective mechanism and is more likely to lead to consumer confusion and unintended consequences. The policy objective is better achieved by introducing an express requirement that privacy notices must be clear, current and understandable.

As we noted in our submission on the issues paper, the perceived benefits that may be afforded by standardised notices will come at a price.[29] Standardisation may make everyone's data handling practices look largely the same, when in reality there are important differences that could influence consumer choices. Put simply, every business is unique. Businesses that rely upon consumer data – including banks, telcos, retailers, insurers, and social media service providers – come in all different shapes and sizes and operate according to different business models. It would not be helpful to consumers to force all of these different businesses to attempt to describe their different data management practices using the same limited vocabulary of words and symbols. Rather, the focus should be on each business explaining its own unique approach in a way that is straightforward and easily digestible for their audience.

The limitations of an overreliance on standardised disclosure requirements was recently explored in the context of financial services in a joint report by the Australian Securities and Investments Commission and the Dutch Authority for the Financial Markets.[30] This report explored several reasons why standardised, mandatory disclosures often do not lead to improvements in consumer understanding nor increase the rationality of choices made by consumers. Some of these reasons the report identifies include:

- inherent complexity in products and factual contexts cannot always be solved through simplified disclosure materials. In this regard, the report quotes research by Professors Omri Ben-Shahar and Carl E Schneider on the failure of mandated disclosure, who argue that 'the complex is not simple and cannot easily be made so';[31]
- simplification often amounts to simplification of language, rather than of concepts or issues. In other words, introducing a taxonomy of simplified icons does not address the underlying complexity inherent in explaining how data is collected and processed;
- standardised disclosures cannot overcome critical differences in contexts, such differences in the products or services to which the disclosures relate. As the report put

[29] Meta, 'Submission to the Australian Privacy Act Issues Paper', *Attorney General Website,* https://www.ag.gov.au/integrity/publications/submissions-received-review-privacy-act-1988-issues-paper
[30] ASIC and AFM, '*Disclosure: Why it shouldn't be the default',* 2019, https://download.asic.gov.au/media/5303322/rep632-published-14-october-2019.pdf
[31] See O Ben-Shahar & CE Schneider, 'More than you wanted to know: The failure of mandated disclosure', *University of Pennsylvania Law Review*, vol. 159, 2011, pp 647- 749

it, 'one size disclosures do not fit all,' because the effects of disclosure are different person to person and situation to situation; and

- lastly, mandatory disclosures can have unintended negative impacts, such as reducing the amount of independent research consumers do in relation to the risks associated with a product when a standardised warning is included in advertisements.

Standardisation may also have the effect of stifling innovation. Prescriptive requirements around the display of icons, or use of particular words, may not necessarily be well suited to new types of services or new forms of communications over time. For example, a requirement to use a particular layout or form of words may presuppose that notices will always be presented in the format of a linear written document, which may not translate well into an immersive virtual world, such as the metaverse. Standardisation is not always in the interests of consumers, especially not when it may block future innovations and developments that could enable even more effective and convenient ways of communicating in different contexts.

In addition, prescriptive requirements regarding use of specific words or icons in Australian privacy notices may also make it more challenging for companies with a global operating footprint to use consistent notices across jurisdictions. This may result in inefficiency, without necessarily delivering material benefits for Australian consumers.

8.4 Strengthen the requirement for when an APP 5 collection notice is required – that is, 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*.**

In principle, we support strong privacy notice requirements. However, we have a couple of concerns in relation to this specific proposal.

Firstly, the proposed "impossibility" standard sets a remarkably high bar and may drive undesirable outcomes, as in almost every case there will be some method by which it would be theoretically possible to provide a collection notice, even though it may impose a significant burden on the organisation giving the notice and result in a highly disruptive and inconvenient user experience for the individual concerned. We consider that a more balanced position should apply where any privacy benefits derived from the collection notice need to be weighed against the costs of providing the notice and any negative impacts on the relevant individual's user experience. It would also help to address a number of the concerns flagged in the discussion paper about the negative consequences of more frequent notifications, including the risk of notice fatigue. Indeed, the discussion paper itself identifies a number of situations where there should be greater flexibility not to provide a separate collection notice. A more balanced approach could be achieved simply by providing further guidance as to how the existing "reasonable steps" standard should be applied in practice.

Secondly, there should be an express acknowledgement that a separate collection notice is not required where personal information is collected by a third party service provider solely in order to process that information on behalf of one of the service provider's customers (e.g. in the context of an outsourcing arrangement). As long as the information is only being processed within the scope of the customer's directions, there should be no need to provide a separate collection notice for the third party service provider as the purposes for which the information may be used and disclosed will remain restricted by the collection notice that the customer itself should have already provided. If the service provider is obliged to issue its own separate collection notice in this scenario, then consumers may soon be flooded with notices from service providers that they have no direct contact with and that play no meaningful role in

determining how their information is processed.

9. Consent to the collection, use and disclosure of personal information

9.1 Consent to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.

We support this proposal in principle, provided that the role of consent remains as it currently is under the APPs. In particular, valid consent should continue to be either express or implied, and the definition of 'current' should not be drafted so as to necessitate renewal where there has been no change to the scope of using the information.

We suggested in our submission to the Issues Paper[32] that one of the key risks of some reform proposals would be over-emphasising consent to the extent it becomes a nuisance for individuals. Many submissions made the point that overreliance on consent leads to 'consent fatigue,' where people no longer meaningfully engage with consents, treat them as an inconvenience and blindly accept them. To the credit of the Department, the discussion paper does recognise that "while consent is necessary in some cases, it should be relied upon as rarely as possible given limits to individuals' time and energy." Eighty-two per cent of Australians believe they have already experienced consent fatigue while using online products and services. A soon to be released report by Accenture on consent requests found that future privacy laws should not encourage overreliance on consent - the average person currently receives over 7 consent requests a day, equating to approximately 1 hour and 13 minutes per day to read requests and notices. When asked how they respond to consents, 69 per cent of people said they generally don't read the details of consent requests.

Further, it is essential that the Privacy Act continue to specify that valid consent may be either express or implied. This has important advantages as it provides flexibility to cater for different circumstances in which consent may be required. The availability of implied consent allows consent to be established in different ways as the context requires (for example, taking into account the nature of the interaction with the individual, the communication methods being used and any pre-existing relationships between the parties). A requirement for express consent in every situation would lead to individuals being asked to provide express consent in circumstances where their implicit consent has already been provided, which may disengage individuals from the consent process and lead to consent fatigue. For organisations, such a requirement may lead to less meaningful consideration of whether consent has been provided, taking all of the circumstances into account, and encourage thinking of compliance as more of a box ticking exercise. Importantly, the discussion paper does not set out any arguments to support the removal of implied consent from the Privacy Act.

Lastly, we ask for further guidance on the proposed requirement for consent to be "current". Consents should not need to be periodically "renewed" or "refreshed" as long as there is no change to the scope of purposes for which the relevant information may be used or disclosed. It may be intrusive and annoying for consumers to be repeatedly asked to confirm their consent choices, and doing so will not provide any material privacy benefit where consumers already have the ability to update their consent settings, including by withdrawing consent, of their own volition and time of choosing. Any requirement to renew or refresh consents should be considered against the risk of inducing consent fatigue among consumers, who may have a reasonable expectation that their consent should only be sought again where a change to the purposes for which their information is being used or disclosed is proposed. It should also be considered in the context of proposal 14.1, which would give consumers' a new right to withdraw their consent at any time.

---

[32] Meta, 'Submission to the Australian Privacy Act Issues Paper', *Attorney General Website,* https://www.ag.gov.au/integrity/publications/submissions-received-review-privacy-act-1988-issues-paper

9.2 Standardised consents could be considered in the development of an APP code, such as the OP code, including standardised layouts, wording, icons or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consents.

See our comments in relation to proposal 8.3.

10. Additional protections for collection, use and disclosure of personal information

10.1 A collection, use or disclosure of personal information under APP 3 and APP 6 must be fair and reasonable in the circumstances.

We support this proposal.

10.2 Legislated factors relevant to whether a collection, use or disclosure of personal information is fair and reasonable in the circumstances could include:

- **Whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances**
- **The sensitivity and amount of personal information being collected, used or disclosed**
- **Whether an individual is at foreseeable risk of unjustified adverse impacts or harm as a result of the collection, use or disclosure of their personal information**
- **Whether the collection, use or disclosure is reasonably necessary to achieve the functions and activities of the entity**
- **Whether the individual's loss of privacy is proportionate to the benefits**
- **The transparency of the collection, use or disclosure of the personal information, and**
- **If the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child.**

We support this proposal.

However, in implementing these changes, and articulating the factors to be taken into account, it will be important to ensure that there is no unnecessary duplication or "doubling-up" of compliance obligations under the APPs in a way that could lead to uncertainty or inconsistency in the way different APPs are applied in practice.

In particular, many of the proposed factors to be taken into account when assessing whether or not a particular act of collection, use or disclosure is "fair and reasonable" will already be taken into account in the context of other APPs. To take a few examples: transparency concerns are addressed by APP 1 and APP 5; an individual's reasonable expectations will be relevant to whether a particular use or disclosure of their information is permitted under APP 6; and the "sensitivity and amount" of personal information being collected, used or disclosed will be relevant to the steps that must be taken to protect that information under APP 11. In principle, we consider that more specific compliance obligations, as set out in these other APPs, should prevail to the extent that there is any cross-over with more general requirements. Otherwise, organisations may never know whether they have done enough to satisfy these obligations, with the resultant lack of regulatory certainty potentially having a chilling effect on innovation.

10.3 Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3.

Commissioner-issued guidelines could provide examples of reasonable steps that could be taken, including making reasonable enquiries regarding the collecting entities' notice and consent procedures or seeking contractual warranties that the information was collected in accordance with APP 3.

We support this proposal in principle, subject to seeing the further guidance that is contemplated as to how the "reasonable steps" standard will be applied in practice. We consider that in almost all cases this standard should be satisfied by obtaining a suitable contractual warranty or other written assurance from the third party in question that it has satisfied relevant compliance requirements relating to the original collection of the information. Requiring further steps, such as active due diligence or assessment of specific information collection practices followed by individual organisations would be intrusive, as it may require sharing of commercially sensitive information, and would add significant friction to commercial dealings as different organisations may have different (though equally valid) views as to how to satisfy their respective compliance procedures. It would also be economically inefficient to require organisations to continually reassess these matters before each new commercial dealing that may involve an exchange of information. Ultimately, each organisation should be responsible for its own compliance with the APPs, with the OAIC, and ultimately the courts, acting as the arbiter as to whether or not any given organisation has met the required standard.

10.4 Define a 'primary purpose' as the purpose for the original collection, as notified to the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.

We support this proposal on the basis that organisations will have flexibility to clearly define the relevant primary purposes for which they collect personal information within their privacy notices (consistent with the comment in the discussion paper that entities should be encouraged to classify a greater range of uses and disclosures as primary purposes) and that no artificial constraints will be applied in that regard. Otherwise, the effect of narrowing the range of permitted "secondary purposes" will be to force organisations to rely more heavily upon consent as a basis for justifying the use and disclosure of personal information, with the various negative outcomes that may entail. In this regard, we endorse the following observations made by the OAIC in its submission to the Issues Paper on the limitations of the notice and consent framework: *"consent is only required under the Privacy Act for higher risk information handling activities. This is why there is a high threshold for valid consent. If consent became the primary basis for personal information handling, this high threshold would place an unnecessary compliance burden on entities for much of their information handling across the online and offline environment."*

11. Restricted and prohibited acts and practices

11.1 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:

- **Direct marketing, including online targeted advertising on a large scale**
- **The collection, use or disclosure of sensitive information on a large scale**
- **The collection, use or disclosure of children's personal information on a large scale**
- **The collection, use or disclosure of location data on a large scale**
- **The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software**
- **The sale of personal information on a large scale**
- **The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale**
- **The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or**
- **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 (see Chapter 14), or by ensuring that explicit notice for restricted practices is mandatory.

We support the proposal in Option 1, which broadly aligns with obligations that apply under the GDPR as well as the way that we understand the OAIC is currently applying existing general compliance obligations under APP 1.2 in practice. It is also consistent with the existing privacy compliance processes that we follow in relation to our business. Under our current processes, any new or updated projects, products or features that store, process or share customer data must go through a formal privacy review before they can launch. This process is designed to help identify and mitigate potential privacy risks. However, it does not necessarily involve the preparation of a specific privacy impact assessment for each individual jurisdiction where we offer our services. Taking that approach could result in a lot of duplicative effort for little net benefit from a user perspective. Therefore, in implementing the proposal in Option 1, we urge the Government to ensure that any specific Australian requirements or guidance in relation to privacy impact assessments should align broadly with international standards, including those set under the GDPR. This would avoid wasted effort in undertaking duplicative work and would make it easier for multinational businesses to roll out their service offerings in Australia.

12. Pro-privacy default settings

12.1 Introduce pro-privacy defaults on a sectoral or other specified basis.

- **Option 1 – Pro-privacy settings enabled by default: Where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.**

- **Option 2 – Require easily accessible privacy settings: Entities must provide individuals with an obvious and clear way to set all privacy controls to the most restrictive, such as through a single click mechanism.**

In our experience, it is important that defaults are flexible to the nature of the audience and service being provided, while still representing pro-privacy default settings. For this reason, we support Option 2 as a pro-privacy approach. This option provides businesses with the flexibility to offer differing privacy defaults depending on the nature of the service and the age of the user, and also provides users with the control to choose privacy settings that best suit their individual wishes.

We want to ensure that when a user signs up to our services, the privacy defaults reflect the service's engagement model, and what is appropriate for the user's age. For example, Facebook was built to bring people together and build relationships, it is a 'friends-based' model that enables interactions between a user, and the people and groups they care about. For this reason, when new people join Facebook, the default audience is set to "Friends" only (ie. not public) so that their posts can only be seen by people they have expressly 'friended' on Facebook.[33] Alternatively, Instagram has a 'follower' model, which is based on people being able to find and follow their friends, interests and public figures to stay up to date with the latest trends. The nature of Instagram can mean that the 'public' audience is most appropriate for most uses of the platform. However, it is especially important that young people on Instagram can have a safe and private experience that still allows them to connect with their friends. For this reason, we default all new Instagram users who are under the age of 16 in Australia into a private account, and we show notifications to current Instagram users highlighting the benefits of a private account and how to change their privacy settings.[34]

Meta supplements this approach by providing users with the control to change their privacy settings at any time. We clearly outline in our Help Centre how a user can adjust their settings from 'public' to 'private' on Instagram. We also offer a number of additional privacy settings on Facebook, where users can choose if they want their posts to be seen by 'specific friends' or 'only me'. By extension, we believe consumers should have meaningful transparency around how their data is used. As described in the 'Privacy at Meta' section, we have worked to make privacy notices more user-friendly by adopting practices like layered privacy policies, just-in-time notices, and in-context notifications.[35] These controls help to empower users to make choices about their privacy settings, and the information they want to see and share.

We believe this approach, in line with Option 2, provides users with an experience that reflects the nature of the service and the way it enables interactions. Option 1 on the other hand, sets out a "one size fits all" approach that may not be practicable or in the interests of the user. For

[33] Meta, 'Making it easier to share with who you want', *Meta Newsroom*, 22 May 2014, https://about.fb.com/news/2014/05/making-it-easier-to-share-with-who-you-want/
[34] Meta, 'Giving young people a safer, more private experience on Instagram', *Meta Newsroom,* 27 July 2021, https://about.fb.com/news/2021/07/instagram-safe-and-private-for-young-people/
[35] E Egan, Communicating About Privacy: Towards People-Centred and Accountable Design, white paper, https://about.fb.com/wp-content/uploads/2020/07/Privacy-Transparency-White-Paper.pdf

example, the highest privacy setting on Facebook is to share posts with 'only me'. This means that only the user would see their posts, and it would not be shared with the friends they have connected to. By requiring pro-privacy defaults to be set to the 'highest possible' or 'most restrictive' settings, it may discourage companies from building stronger protections that are designed for niche uses or particular cohorts but are unsuitable for the bulk of users.

However, even with the proposal in Option 2, care must be taken to avoid overly rigid and inflexible compliance requirements. We suggest that a requirement to provide 'simple and easy to use' privacy controls would be more appropriate than to mandate a 'single click' mechanism that may not be practical to apply for complex services where individual users may legitimately wish to select a range of different privacy settings. It also assumes that a 'click' will always be the most common or appropriate way to interact with digital services. In a technology landscape which will have increasingly virtual and immersive spaces there should be flexibility for a wide variety of user interfaces and ways of communicating, so as not to allow present day thinking to artificially constrain future innovation. Applying a more rigid approach where everything must always be reduced to a single action such as a 'click' would also make it more difficult to roll out new service features, which would not necessarily be in the interests of Australian consumers as it means they may miss out on new features where the cost of inter-linking all relevant privacy controls cannot be justified.

In any event, whichever Option is preferred for this proposal, it should be applied on an economy-wide basis rather than as a targeted measure that is limited to certain industry sectors. The discussion paper does not present any compelling justification for discriminating between industries in this regard and we consider that consumers would reasonably expect to be provided with a consistent level of control over their privacy no matter what industry they are dealing with.

13. Children and vulnerable individuals

13.1 Amend the Act to require consent to be provided by a parent or guardian where a child is under the age of 16. The Review is seeking additional feedback on whether APP entities should be permitted to assess capacity on an individualised basis where it is practical to do so. The Review is also seeking feedback on the circumstances in which parent or guardian consent must be obtained:

- **Option 1 - Parent or guardian consent to be required before collecting, using or disclosing personal information of the child under the age of 16.**
- **Option 2 - In situations where the Act currently requires consent, including before the collection of sensitive information or as an available mechanism to undertake a secondary use or disclosure of personal information.**

The assumed age of capacity would also determine when a child may exercise privacy requests independently of their parents, including access, correction or erasure requests.

We recommend that any changes to the Act in this regard should be aligned with the equivalent rules within the Online Privacy Bill and Online Privacy Code.

It is important that children and other vulnerable individuals have a consistent level of protection no matter what company or industry they are dealing with. For this reason, the Act and the Online Privacy Code's requirements around parental consent should be consistent, so as not to confuse consumers over the different protections and safeguards that would apply across different industries. Applying a differentiated approach would also drive unnecessary complexity for service providers who operate across different industry sectors.

Meta has provided commentary on the Online Privacy Code's parental consent requirements in our submission in response to the Online Privacy Bill. We work hard to proactively offer products, tools and controls that give young people age-appropriate and privacy protective experiences.

Meta recognises that regulation has an important role to play in ensuring that young people have safe and age-appropriate experiences online. For this reason, Meta has supported the Government's enhancement of online safety laws via the Online Safety Act, and has been working constructively with the Government on the Draft Restricted Access System Declaration, as well as the Australian eSafety Commissioner's Age Verification Roadmap.

Globally, the UK's Age Appropriate Design Code has set a benchmark for regulation in this space and we commend it as a good starting point for regulators in Australia considering new requirements for protecting the data of young people.

When considering the role of parental consent, it is important that the following principles are applied, to ensure the 'best interests' of the child are taken into account:

- **Privacy-preserving.** Regulation should respect the data protection principle of data minimisation, and should not require collection of additional data.
- **Age-appropriate safeguards.** Younger users require additional safeguards for their safety, privacy, and wellbeing, whereas older teens may require fewer safeguards. Rather than impose blanket requirements for all young users, regulation should allow for a range of age-appropriate safeguards.
- **Youth empowerment.** Young people use online services to express themselves, to keep up with their families and best friends, and to find new passions and interests. Likewise,

teens can organise around things they care about, support underrepresented voices and push for societal change. Regulation should support the responsible empowerment of young people rather than removing their choice or agency.

- **Innovation**. Industry is moving quickly and there are a lot of developments in the area of age-appropriate experiences internationally. Good regulation should encourage innovation by industry to develop age-appropriate experiences rather than prescribing particular technologies or processes (which may quickly become outdated).

Policymakers should not assume that requiring parental consent is the sole solution for ensuring age-appropriate experiences online. Many providers - including Meta - also provide significant controls for parents. Controls provide more meaningful oversight and transparency for parents around how a teen is using a service, while still empowering them to engage in online social interactions.

Controls also provide a more flexible approach, allowing parents to review what is most appropriate for their child at different points in time, and make adjustments based on changes in a young person's age, interests, and interactions with the service. By contrast, parental consent has a stronger focus on requiring a parent to engage with privacy settings when the user first signs up, and can lead to a 'set and forget' approach which is not later revisited and reviewed.

Nevertheless, while controls may provide a more meaningful approach, we see a role for balanced requirements around parental consent.

The following considerations should be kept in mind when determining the role of parental consent, and how this provision would supplement requirements in the Online Platform Code:

- **The risk of overloading parents with potentially excessive requests.** The proposal for parental consent should be read in the context of the other provisions of the Online Privacy Code, which may potentially expand the current role of consent.[36] These requirements create ambiguity about the role of consent.

  If the online privacy code requires online operators to seek consent more often and at a more granular level, it risks over-emphasising consent to the extent it becomes a nuisance for individuals. As outlined in our submission to the issues paper[37] and many other submissions, overreliance on consent leads to 'consent fatigue,' where people no longer meaningfully engage with consents, treat them as an inconvenience and blindly accept them. Overloading parents with potentially excessive requests for them to consent to every action of their child is more likely to overwhelm parents than provide meaningful confidence in the safety or privacy of their child. It also shifts the burden onto the parents to understand every request at a granular level of detail.

---

[36] In particular:
- section 26KC(2)(d) requires that the online privacy code set out how relevant organisations are to "comply with Australian Privacy Principles 3 and 6 in ensuring that an individual has provided consent for the collection, use or disclosure of personal information". ;
- section 26KC(e)(ii) requires that the online privacy code make provision for how consents are to be required, including by requiring consent for collection of sensitive information to be renewed "periodically" or when circumstances change; and
- section 26KC(5)(b) requires that the online privacy code make provision for consent to be provided by a parent or guardian on behalf of a child or other person who is unable to give consent on their own.

[37] Meta, 'Submission to the Australian Privacy Act Issues Paper', *Attorney General Website,* https://www.ag.gov.au/integrity/publications/submissions-received-review-privacy-act-1988-issues-paper

- **Relying solely on consents – rather than a mix of consents and controls – risks an overly rigid approach.** Many teens in Australia may not have easy access to official identity documents (for example, teens in remote communities or from refugee backgrounds) and/or be in a situation to seek parental approval (for example, children in a family violence situation). Establishing overly strict requirements risks disenfranchising these groups of teens by denying them social connection from the internet altogether.
- **There are technical drafting issues which make the obligation unworkable for service providers.** Option 1 above, as well as the Online Platform Code's exposure draft, requires a service provider to seek parental consent prior to obtaining any data relating to a child; however, service providers will need to collect at least some data to know whether a user is a child (and hence needs further parental consent). Under section 26KC(2)(6)(b) of the Code, a social media service provider will have to obtain consent from a parent or guardian before collecting information about a child. However, the service provider will need to collect some information from the child in order, first, to verify their age and then, second, in order to be able to identify their parent/guardian. It is not clear how the service provider would do that if it is in fact prohibited from collecting information from the child to begin with.

To address these considerations, Meta has recommended in our submission on the Online Privacy Code that the exposure draft be amended so that service providers would be required to "undertake reasonable steps to seek parental consent" rather than "undertake all reasonable steps". We also recommend including in the explanatory material for the legislation that the provision should not be read as an obligation for service providers to prove parental or guardianship status, to avoid establishing a mass collection of new data that would be a significant impost on the time of parents.

We recommend that the Privacy Act is drafted in line with these considerations, and ultimately consistent with the parental consent provisions in the Online Privacy Code.

13.2 Require APP 5 notices to be clear, current and understandable, *in particular for any information addressed specifically to a child.*

We support this proposal.

14. Right to object and portability

14.1 An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information.

On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection.

This proposal would require companies to take reasonable steps to cease use or disclosure of an individual's personal information on request. This proposed right is significantly broader than the equivalent right under GDPR, which is limited to situations where the legal basis for processing is public interest or legitimate interests.

While we broadly support this proposal in principle, it is critical that allowance is made for continued collection, use or disclosure in appropriate circumstances. We consider that these circumstances must include where the collection, use or disclosure is necessary:

- for the purpose of complying with the individual's objection request
- to complete a transaction or give effect to a contract
- to provide a service or product the individual has requested
- for legal purposes
- due to a permitted general or health situation
- for safety, security and integrity purposes or
- to process data in order to understand if a user should have their data processed (e.g. to understand if the data does not belong to a user).

Some of these circumstances were already contemplated in the discussion paper, while others are essential additions. In particular, an entity should not be required to fundamentally alter its business model in order to comply with the right to object, and that a service provider should be able to deny access to a service if an individual objects to a collection, use or disclosure of information that is reasonably necessary for the provision of that service according to the service provider's chosen business model.

As set out in our Online Privacy Bill submission, we strongly support arming consumers with rights to opt out of direct marketing services such as an email marketing newsletter, but submit that it may be helpful to consider how the right to object applies to advertising-supported services, where advertising is an intrinsic part of the service. Australians benefit from being able to access free digital services, funded by personalised advertising that is relevant and useful. Ad-supported business models help to ensure that digital tools and services are free and easily accessible to all consumers - including those who are disadvantaged or otherwise may not be able to afford to pay.

According to a 2020 survey in the US, people place a value of more than US$1,400 per year on the array of free digital content, services, and mobile apps that are currently funded by advertising.[38] When asked whether they prefer an ad-supported internet where most services are free or an ad-free internet where everything costs money, 84.1 per cent of respondents indicated they would prefer an ad-supported internet.

[38] Digital Advertising Alliance, 'Americans value free ad-supported online services at $1,400 a year', *Digital Advertising Alliance Website*, September 2020, https://digitaladvertisingalliance.org/press-release/americans-value-free-ad-supported-online-services-1400year-annual-value-jumps-more-200

Without the ability to personalise, the ad-supported internet would revert to an annoying and intrusive experience, and an increasing number of internet experiences would live behind paywalls, available to the privileged few who could afford them. Non-personalised ads, which defined the early internet, were annoying to people and unhelpful to businesses. Websites in the 1990s resorted to flashing, spammy pop-up ads to catch peoples' attention for otherwise irrelevant messages. This degraded the user experience. In a report conducted by Infogroup, roughly 90 per cent of people said that messages from companies that are not personally relevant to them are "annoying." Of those irritating messages, 53 per cent said advertising for an irrelevant product tops their list of messaging annoyances.[39]

The personalised ads-supported internet directly benefits small businesses. A recent report by Deloitte looks at how small business growth and innovation has been driven by the personalised economy.[40] It finds that social media and digital technologies are enabling small and medium-sized businesses to enhance the personalisation of their products, services and customer experiences. 82 per cent of Australian small businesses reported using Facebook apps to help them start their business, and 64 per cent reported that Facebook apps were important for obtaining feedback, which in turn helped improve their product or service. It also finds that 71 per cent of Australian small businesses that use personalised advertising reported that it is important for the success of their business. Particularly over the past 2 years, personalised advertising has helped businesses target new customers as they pivot away from bricks-and-mortar operations for the purposes of public health.

Personalised ads are the most cost-effective way for small businesses, particularly less-advantaged groups, to reach new customers and grow. Businesses of all sizes see improved return-on-investment from personalised ads – a BCG study found 80 per cent of marketers reported an increased ROI over the past three years, in particular from improvements in technology that enables the personalisation of advertising.[41]

By helping businesses grow, personalised ads contribute to economic growth and job creation.

Given the significant economic benefits of personalised advertising, any reforms to the Privacy Act should not fundamentally undermine the ability for companies to offer services underpinned by ad-supported business models.

It would be very concerning if the right to object was read as requiring an ad-supported service to continue providing the same service without ads, if a consumer objects to their personal information being used for advertising. An organisation should not have to fundamentally change its business model (which in turn affects the business models of its advertising customers) in order to respond to a consumer objection. If the consumer objects to the business model, then they are able to cease using the services. Given the wide array of ways that Australians can communicate with each other online and the fierce competition for services attracting the time and attention of users, there are ample other options if consumers object to using an advertising-supported service.

The right should also be limited to information provided by the user that the company controls. If a person posts or shares the name of an objecting person on a platform, then the platform should be able to process that data in accordance with the original person's expectations.

---

[39] Infogroup, The Power of Personalization, May 2019, https://www.emarketer.com/chart/228797/attitudes-toward-personalization-among-us-internet-users-jan-2019-of-respondents

[40] Deloitte, 'Dynamic Markets Report: Australia - unlocking small business innovation and growth through the personalised economy', *Meta Australia blog*, October 2021, https://australia.fb.com/economic-empowerment/

[41] A Schwabe et al. 'Getting the most from Europe's marketing ecosystem', *BCG,* May 2020, https://www.bcg.com/publications/2020/leveraging-european-marketing-ecosystem

15. Right to erasure of personal information

15.1 An individual may only request erasure of personal information where one of the following grounds applies, and subject to exceptions:

- **the personal information must be destroyed or de-identified under APP 11.2**
- **the personal information is sensitive information**
- **an individual has successfully objected to personal information handling through the right to object (see Chapter 14)**
- **the personal information has been collected, used or disclosed unlawfully**
- **the entity is required by or under an Australian law, or a court/tribunal order, to destroy the information, and**
- **the personal information relates to a child and erasure is requested by a child, parent or authorised guardian.**

We support this proposal.

15.2 Provide for exceptions to an individual's right to erasure of personal information. An APP entity could refuse a request to erase personal information to the extent that an exception applied to either *all or some* of the personal information held by an APP entity.

We support this proposal and consider that, if a right to erasure is introduced, it should be subject to appropriate exceptions equivalent to those that apply under Article 17 of the GDPR at a minimum. This would necessitate providing exceptions where the retention of the personal information is required for freedom of expression, for a public interest purpose, for complying with a legal obligation, or for establishing or defending a legal claim.

Further, we support the analysis set out in the discussion paper indicating that the following exceptions should be included:

- where personal information is necessary to complete a transaction or for performance of a contract;
- where erasure is technically impractical or would constitute an unreasonable burden; and
- where erasure would have an unreasonable impact on the personal information of another person.

Lastly, as highlighted above in our discussion of proposal 2.4, it is critical that entities are able to refuse a request to erase personal information to the extent the information is necessary for safety, security and integrity purposes.

15.3 An APP entity must respond to an erasure request within a reasonable period. If an APP entity refuses to erase the personal information because an exception applies, the APP entity must give the individual a written notice that sets out the reasons for refusal and mechanisms available to complain about the refusal, unless unreasonable to do so.

We support this proposal.

16. Direct marketing, targeted advertising and profiling

16.1 The right to object, discussed at Chapter 14, would include an unqualified right to object to any collection, use or disclosure of personal information by an organisation for the purpose of direct marketing. An individual could still request not to receive direct marketing communications from an organisation. If an organisation provides marketing materials to an individual, it must notify the individual of their right to object in relation to each marketing product provided.

On receiving notice of an objection, an entity must stop collecting, using or disclosing the individual's personal information for the purpose of direct marketing and must inform the individual of the consequences of the objection.

As outlined above in relation to proposal 14.1 and in our submission on the Online Privacy Bill, we consider that ad-supported services provide significant value to Australian users and businesses alike.

It would be very concerning if the right to object was read as requiring an ad-supported service to continue providing that service without ads, or at least without personalised ads, if a consumer objects to their data being used for advertising. An organisation should not have to fundamentally change its business model (and, potentially, indirectly impact the business models of its business partners, such as advertisers) in order to respond to a consumer objection – if the consumer objects to the business model, including any ad-supported features, then the appropriate outcome is for the consumer to cease using the services offered by that organisation.

Consistent with our comments on proposal 14.1 above, in order to avoid any potential confusion in this regard, if a right to object is introduced as contemplated by this proposal, then we consider it should be expressly stated that a service provider may deny access to an ad-supported service if an individual user objects to the collection, use or disclosure of their personal information for the purposes of providing personalised ads on that service. That way, the user will be able to make an appropriately informed decision as to whether the value they derive from the service outweighs any actual or perceived cost to their privacy from accepting personalised ads. It will also allow the market to determine whether ad-supported or user-pays business models should be preferred or, indeed, whether there is scope for the market to support both business models for different user cohorts. Any other outcome, where a service provider may be constrained from adopting a particular business model, will necessarily result in market distortions and loss of economic efficiency.

16.2 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.

We have concerns about the effects of this proposal. While we support transparency for consumers in how their data is used, it is not clear (1) why this proposal takes such a narrowly defined view of "influence" or (2) why other proposed legislative changes would not already address any policy concerns here.

This proposal in the discussion paper is based on the assumption that all entities involved in the delivery of personalised ads or other targeted content are uniquely doing so for the purposes of influencing an individual's behaviour or decisions.

Of course, all advertising is, to some degree, an attempt to influence consumer behaviour. But any link it has to influencing consumers' behaviour is similar to other uses of data: for example, collection of health data may influence consumers to exercise more or eat better, or collection of electricity consumption data may influence consumers to moderate their usage. For these

reasons, it would not be equitable to suggest online advertising represents influencing consumers' behaviour but other forms of data collection do not represent 'influence'.

It is also not clear that specifically prescribing use of the terminology "influencing their behaviour" will increase Australians' meaningful understanding of or engagement with their own privacy settings. Consumers already understand that advertising services are intended to raise awareness about products, services, events or causes that they may not have previously been aware of. If cross-economy privacy reform compels notices and consents to be clear, current and understandable, regulated entities will already be expected to clearly set out for consumers when their data may be used for advertising purposes

The potential impact or influence of online advertising will also depend more on the advertiser, rather than the entity that delivers the advertising. To use an analogy, where an ad is broadcast on TV it is the advertiser and not the TV broadcaster that is hoping to influence the audience watching that broadcast. It would not be accurate or appropriate to compel the broadcaster to present itself as somehow being in the business of influencing its viewing audience to purchase the goods and services offered by advertisers, when really its business is simply about attracting an audience by providing engaging content and then charging a fee to deliver ads to that audience.

We have absolutely no qualms about being fully transparent with our users about how we use their information to personalise their experience of our services. This includes being fully transparent about how we use information to show them personalised ads. For example, in our Data Policy we expressly state "*We use the information we have about you – including information about your interests, actions and connections – to select and personalise ads, offers and other sponsored content that we show you.*"

This is also why we offer tools to our users that enable them to control how their information is used. For example, we've built Off-Facebook Activity, which lets people see a summary of the information other apps and websites send to Facebook, and gives them the option to disconnect it from their account.[42] We also give users access to the "Why am I seeing this ad?" tool, which enables users to see how factors like basic demographic details, interests and website visits contribute to the ads in News Feed. In 2019, we expanded the tool to include additional details about ads when information on an advertiser's list matches a user's Facebook profile.[43] "Why am I seeing this ad?" also now provides details such as when the advertiser uploaded the information or if the advertiser worked with another marketing partner to run the ad.

While we share the policy objective of requiring transparency in how any online service uses ads or personalises the experience of consumers, we believe that working with industry on promoting best-practice transparency tools (combined with the legislative reform contemplated in other proposals) is more likely to be effective.

16.3 APP entities would be required to include the following additional information in their privacy policy:

- **whether the entity is likely to use personal information, alone or in combination with any other information, for the purpose of influencing an individual's behaviour or decisions and if so, the types of information that will be used, generated or inferred to influence the individual, and**

[42] M Zuckerberg, 'Starting the Decade By Giving You More Control Over Your Privacy', *Meta Newsroom*, 28 January 2020, https://about.fb.com/news/2020/01/data-privacy-day-2020/
[43] S Thulasi, 'Understand Why You're Seeing Certain Ads And How You Can Adjust Your Ads Experience', *Meta Newsroom*, 11 July 2019, https://about.fb.com/news/2019/07/understand-why-youre-seeing-ads/

- **whether the entity uses third parties in the provision of online marketing materials and if so, the details of those parties and information regarding the appropriate method of opting-out of those materials.**

Please refer to our comments in response to proposal 16.2 above.

16.4 Repeal APP 7 in light of existing protections in the Act and other proposals for reform.

We support this proposal.

17. Automated decision-making

17.1 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.

We support this proposal.

18. Accessing and correcting personal information

18.1 An organisation must identify the source of personal information that it has collected indirectly, on request by the individual, unless it is impossible or would involve disproportionate effort.

We broadly support this proposal but suggest that any amendment should require organisations to provide 'any available information' as to the source of personal information. This would achieve closer alignment with the requirement under Article 15 of the GDPR.

18.2 Introduce the following additional ground on which an APP organisation may refuse a request for access to personal information:

- **the information requested relates to external dispute resolution services involving the individual, where giving access would prejudice the dispute resolution process.**

We support this proposal.

18.3 Clarify the existing access request process in APP 12 to the effect that:

- **an APP entity may consult with the individual to provide access to the requested information in an alternative manner, such as a general summary or explanation of personal information held, particularly where an access request would require the provision of personal information that is highly technical or voluminous in nature; and**
- **where personal information is not readily understandable to an ordinary reader, an APP entity must provide an explanation of the personal information by way of a general summary of the information on request by an individual.**

We support this proposal.

More generally, we consider there would be value in aligning access rights, and associated exceptions, with international standards in order to help standardise compliance processes and better manage situations where overlapping rights may apply under different laws. For example, in relation to access rights, we consider that it would be appropriate to include an express right to refuse an access request that is "manifestly unfounded or excessive" as currently reflected in Article 12(5) of the GDPR. This would help prevent attempts at leveraging these types of rights for ulterior purposes rather than to protect genuine privacy concerns.

19. Security and destruction of personal information

19.1 Amend APP 11.1 to state that 'reasonable steps' includes technical and organisational measures.

We support this proposal.

19.2 Include a list of factors that indicate what reasonable steps may be required.

We support this proposal.

19.3 Amend APP 11.2 to require 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.

We support this proposal, subject to our comments on proposal 2.5 above.

20. Organisational accountability

20.1 Introduce further organisational accountability requirements into the Act, targeting measures to where there is the greatest privacy risk:

- **Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.**

We do not object to this proposal, though we query whether it would add meaningfully to the level of privacy protection that individuals would enjoy under the Act, particularly taking into account other protections contemplated within the discussion paper.

Nonetheless, if this proposal is pursued, it would be useful to clarify that it would only apply on the first occasion that the relevant information is used for the relevant secondary purpose. That is, where information is to be used for a purpose that may be repeated over time, it should not be necessary to create a separate record on each occasion that the information is used for that purpose – that would clearly be excessive and of no practical value from a privacy compliance perspective.

We support the proposition in the discussion paper that there should be no need to expressly require entities to determine, at or before the time of collecting personal information each of the purposes for which the collected information is to be used or disclosed. While it is appropriate to require an entity to clearly state its primary purposes of collection at the relevant time, consistent with proposal 10.4, it is possible that secondary purposes will evolve over time and may not always be possible to anticipate or identify with specificity at the time of collection. It would not be appropriate to artificially constrain an entity's ability to make use of information it has collected by requiring all possible secondary purposes to be identified and defined in advance.

22. Overseas data flows

22.1 Amend the Act to introduce a mechanism to prescribe countries and certification schemes under APP 8.2(a).

We support this proposal.

22.2 Standard Contractual Clauses for transferring personal information overseas be made available to APP entities to facilitate overseas disclosures of personal information.

We support this proposal.

22.3 Remove the informed consent exception in APP 8.2(b).

We support this proposal.

22.4 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 entity's up-to-date APP privacy policy required to be kept under APP 1.3.

We support this proposal.

22.5 Introduce a definition of 'disclosure' that is consistent with the current definition in the APP Guidelines.

We support this proposal.

22.6 Amend the Act to clarify what circumstances are relevant to determining what 'reasonable steps' are for the purpose of APP 8.1.

We support this proposal.

23. Cross Border Privacy Rules and domestic certification

23.1 Continue to progress implementation of the CBPR system.

We strongly support this proposal.

23.2 Introduce a voluntary domestic privacy certification scheme that is based on, and works alongside CBPR.

We support this proposal.

24. Enforcement

24.1 Create tiers of civil penalty provisions to give the OAIC more options so they can better target regulatory responses including:

- **A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy.**
- **A series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.**

We have no comments on this proposal.

24.2 Clarify what is a 'serious' or 'repeated' interference with privacy.

This proposal relates to s 13G of the Privacy Act, which is a civil penalty provision that applies in two circumstances:

- where there is serious interference with an individual's privacy; or
- where there are acts or practices that are repeated interferences with the privacy of one or more individuals.

While we support clarification on the list of factors to be considered in determining whether or not a breach is captured by s 13G, the relevant test should always be whether or not the breach was "serious" or "repeated", especially given the substantial penalties associated with s 13G. In explaining this proposal, the discussion paper argues that "the threshold [under s 13G] could more clearly express that breaches affecting a large number of individuals without affecting any one individual seriously can be subject to this civil penalty provision". We respectfully disagree that clarification of this sort is appropriate. Naturally the number of individuals who are affected by an act or practice may be a relevant factor in determining whether there has been a 'serious' or 'repeated' interference with privacy. However, in isolation, the number of individuals who are affected should not be determinative. This is recognised by the OAIC's current guidance in relation to s 13G which says, "an act or practice that simultaneously results in the interference with privacy of several individuals – such as a mail merge error leading to the personal information of multiple individuals being disclosed to third parties – will not in itself constitute a 'repeated' interference with privacy. Similarly, a single act which results in the breach of multiple APPs will not in itself be a 'repeated' privacy interference."

24.3 The powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act) would apply to investigations of civil penalty provisions in addition to the IC's current investigation powers.

We have no comments on this proposal.

24.4 Amend the Act to provide the IC the power to undertake public inquiries and reviews into specified matters.

We have no comments on this proposal.

24.5 Amend paragraph 52(1)(b)(ii) and 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined:

- **a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals.**

We have no comments on this proposal.

24.6 Give the Federal Court the power to make any order it sees fit after a section 13G civil penalty provision has been established.

We support this proposal. However, in order to avoid risk of overlapping or inconsistent orders, it should be made clear that where the Court finds that there has been a serious breach and makes orders under section 13G, the Information Commissioner should not be allowed to separately issue a determination on the same matter under section 52.

24.7 Introduce an industry funding model similar to ASIC's incorporating two different levies:

- **A cost recovery levy to help fund the OAIC's provision of guidance, advice and assessments, and**
- **A statutory levy to fund the OAIC's investigation and prosecution of entities which operate in a high privacy risk environment.**

We agree in principle that the OAIC should have sufficient resourcing to implement its duties. We have no objections to a cost recovery approach for provision of guidance, advice and assessments that are initiated by industry.

However, we have concerns that the statutory levy as proposed is too narrow, arbitrary and inequitable.

In determining the scope of companies to pay the statutory levy, the discussion paper does not provide any indication as to how relevant high risk privacy environments would be identified. However, it asserts without rationale that social media companies would qualify and should be expected to make this industry contribution. Given the levy appears to be intended to fund the investigation and prosecution of breaches, a logical place to start would be to look for those industry sectors that are responsible for the majority of privacy complaints. Of the three most recent annual reports that were available at the time of writing this submission, the OAIC identified the top sectors by privacy complaints received as follows:

- **2020-2021:** (1) Finance; (2) Australian Government; (3) Health Service Providers; (4) Retail; and (5) Online Services[44]
- **2019-2020:** (1) Australian Government; (2) Finance; (3) Health Service Providers; (4) Retail; and (5) Telecommunications
- **2018-2019:** (1) Finance; (2) Australian Government; (3) Health Service Providers; (4) Telecommunications; and (5) Retail

It would seem logical then for the sectors that have featured consistently in this list to be identified as the "high risk privacy environments" against whom the statutory level should be

[44] The number of complaints received in relation to the Online Services sector (152) was less than half those received in relation to the Finance sector (327).

applied. However, they are not mentioned in the discussion paper. In any event, these statistics indicate that it would be inequitable to apply the statutory levy to a narrow selection of companies.

Any industry contributions should be much more broad-based than is contemplated in the discussion paper.

24.8 Amend the annual reporting requirements in the AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground.

We have no comments on this proposal.

24.9 Alternative regulatory models

- **Option 1 – Encourage greater recognition and use of 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.**
- **Option 3 – Establish a Deputy Information Commissioner – Enforcement within the OAIC.**

We do not have any comments on this proposal.

25. A direct right of action

25.1 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 FPO) and have their complaint assessed for conciliation either by the OAIC or a recognised EDR 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.**

For reasons previously set out in our submission on the Issues Paper, we have concerns with the introduction of a direct right of action and instead recommend that the introduction of a statutory tort of privacy would sufficiently achieve the underlying policy objectives here. We consider that the OAIC remains best placed to resolve privacy complaints and the OAIC's track record shows that it is capable of doing this efficiently and effectively. It is not in the best interests of individuals to encourage them to seek recourse through the far more costly and time consuming Court process. It may also take up scarce Court resources on relatively low level complaints that have limited precedential value.

Nonetheless, if the Government is determined to introduce such a right, we suggest that the OAIC should play an important gatekeeper role in ensuring that only appropriate matters make their way through to the Courts. In particular, we still consider that Court action should only become an option if the OAIC confirms that:

- the plaintiff has made a genuine attempt to conciliate but that the conciliation process has nonetheless not resulted in a successful resolution to the matter – that is, the plaintiff must take the conciliation process seriously and not simply treat it as a box that must be ticked in order to gain entry to the Court system. Entities should not be drawn into potentially costly litigation in relation to matters that should have been possible to resolve at an earlier stage if the plaintiff had adopted a reasonable attitude; and
- that the plaintiff's complaint relates to an interference with privacy that, if established, would in the OAIC's opinion constitute a serious interference – that is, the Court's resources should not be unnecessarily wasted on matters that may, compared to other matters routinely considered by the Courts, be relatively trivial. For example, in the OAIC's annual report for 2020-2021 (the most recent report available at the time of writing this submission), the OAIC indicated that it had closed 71 privacy complaints that involved payment of monetary compensation as a remedy. In only 11 of those 71 complaints was the amount of compensation more than $10,000. In our view, it would not be in the public interest to take up the Court's resources with matters of that magnitude.

26. A statutory tort of privacy

26.1 Option 1: Introduce a statutory tort for invasion of privacy as recommended by the ALRC Report 123.

26.2 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.

26.3 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.

26.4 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.

Consistent with our previous submission on the issues paper, we support the introduction of a statutory tort for invasion of privacy that follows the model recommended in ALRC Report 123. It follows that we support Option 1 over the other Options contemplated in the discussion paper. In any event, care should be taken to avoid unnecessary overlap between any direct right of action under the Act and any statutory tort. The regulatory landscape is already complex and the objective should be to avoid duplicative measures that will risk causing more confusion for both consumers and businesses.

27. Notifiable Data Breaches scheme

27.1 Amend subsections 26WK(3) and 26WR(4) to the effect that a 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.

We broadly support this proposal.

However, it would be helpful to expressly clarify that there will be no requirement to include any confidential information in the notice, or anything else that may compromise any information security procedures that the reporting entity may have in place. It would clearly be counterproductive for reporting entities to be compelled to provide information that could give hackers and other bad actors insights that they may then exploit in future attacks.

In addition, we support suggestions noted in the discussion paper that, to the extent practicable, it would be sensible to align the Australian notifiable data breaches scheme with international equivalents in order to streamline and simplify the breach assessment and reporting process for organisations that operate across multiple jurisdictions.

28. Interactions with other schemes

28.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.

28.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.

28.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

We strongly support any attempts to harmonise privacy rules and regulations, both in line with domestic regulatory reforms, and global frameworks. This will reduce the risk of overlap, duplication or inconsistency across different laws, both domestically or internationally, which could result in an inconsistent or confusing experience for users, and a high compliance burden for businesses.

The regulatory landscape is becoming ever more complex with a wide range of privacy rules and regulations for businesses and consumers to navigate. In addition to the Privacy Act and the Online Privacy Code, there are: State-based privacy laws; industry-specific laws such as under Part 13 of the Telco Act and State-based laws dealing with health records; information-specific laws that apply to things such as healthcare identifiers, tax file numbers, information that is subject to the Consumer Data Right regime, and identity information that will be the subject of the proposed new Trusted Digital Identity Bill; and potential protections that may apply at common law for serious invasions of privacy. This is not to mention other laws such as the Australian Consumer Law and State-based fair trading laws, that are also subject to certain privacy practices. Generally speaking, we consider there is value in seeking alignment and consistency across all of these initiatives wherever possible in order to avoid creating an unmanageable compliance burden.

It is also important that policy areas pursued in the Privacy Act review and the Online Privacy Bill are in alignment with other reforms being pursued by the Government. For example, the Government is pursuing multiple different regulations in relation to age verification that contain slightly similar but differing objectives.

The possibility of age restrictions for social media was introduced in the Online Safety Act, which received Royal Assent in July 2021. As part of that requirement, eSafety released a draft declaration for a Restricted Access System Declaration with greater detail on age restrictions in August 2021. This is due to take effect in January 2022.

Simultaneously, eSafety began consultation on steps taken to verify the ages of users as part of an Age Verification roadmap in August 2021. This is due to be completed in December 2022.

Also underpinning the Online Safety Act are the online safety industry codes and the Basic Online Safety Expectations, both of which began consultation in September 2021 and October 2021, respectively. Each of these regulatory mechanisms also include requirements for industry to introduce age-dependent restrictions for certain content, and age verifications.

At the end of 2021, the draft legislation for the Online Privacy Code was released that went further and included mandatory requirements for social media companies to verify the age of all Australian users. The Privacy Act discussion paper also introduces options for parental consent based on a young person's age, which would require service providers to verify the young person's age, prior to seeking consent.

The Government has also signaled that it is working towards expectations about identity verification (which would go even further again to verify not just a user's age, but their legal name and identity).

The final result could be more than five separate regulations, all with slightly differing requirements around age restrictions and verification.

Whilst well-intended in terms of the outcomes being pursued, the potential for regulatory uncertainty and inconsistency that not only confuses industry but also consumers is significant. Time and care should be taken to ensure requirements are carefully designed, allow companies sufficient time to build for compliance, and be compatible with existing rules.

We would also encourage that any reforms of the Privacy Act are considered within the context of a global contest of competing visions of the internet.[45] The democratic values that underpin the open internet, such as free expression, transparency, accountability and the encouragement of innovation and entrepreneurship, cannot be taken for granted. In 2019, analysis by Bain & Company, Google and Temasek found that south-east Asia's digital economy was worth more than $US100 billion a year. Before COVID-19 hit, it was on track to treble to over $US300 billion by 2025. The open, global internet has allowed for this growth, particularly for small and medium-sized businesses.[46]

Other countries look to Australia, and it is important to consider whether Australian regulation sets an example which encourages a liberal, open and democratic approach to the internet, or an internet that is more closed, tightly controlled and fragmented. We encourage countries like Australia to pursue privacy and data protection regulation that is as consistent as possible to the best practice privacy frameworks of leading digital economies in the world, like the GDPR. As the OECD and others have stated, ensuring alignment with global norms enhances Australia's global competitiveness and this type of regulatory harmonisation reduces unnecessary compliance costs and leads to increases in productivity.[47] Crucially, a globally harmonised privacy and data protection framework will ensure that Australians, and people around the world, can continue to benefit from the opportunities afforded by access to an internet which is not fragmented by localised regulatory barriers.

---

[45] N Clegg, a bretton Woods for the digital age can save the open internet', *Australian Financial Review*, 16 November 2021, https://www.afr.com/technology/a-bretton-woods-for-the-digital-age-can-save-the-open-internet-20211115-p5994h

[46] Google, Temasek and Bain & Company, 'e-conomy SEA 2020- resilient and racing ahead: Southeast Asian at full velocity', *Bain & Company website*, 10 November 2020, https://www.bain.com/insights/e-conomy-sea-2020/

[47] OECD, *OECD Privacy Framework*, https://www.oecd.org/sti/ieconomy/oecd privacy framework.pdf.