Meta

Response to the Australian online privacy code exposure draft

DECEMBER 2021

Executive summary

Meta welcomes the opportunity to respond to the exposure draft legislation for an online privacy code.[1] We believe it is essential to set the right framework for privacy and data protection to give Australians confidence about the digital economy. This legislation - combined with cross-economy reform under consideration by the Government - will significantly alter how personal information is managed within Australia.

Privacy and protection of people's data are fundamental to our business, and we have put consumer rights and strong safeguards at the heart of our approach to privacy.

We have also long supported stronger privacy protections for consumers. Since 2019, we have been calling for new rules to govern the internet[2] - including in relation to privacy - and we have consistently supported reform to the Australian Privacy Act since it was suggested by the ACCC in the Digital Platforms Inquiry.

There are some key elements of the draft legislation that we support and that will provide the basis for a strong privacy code.

- First, an online privacy code developed under this legislation would require companies to make more information available about data practices. Greater transparency for consumers is something Meta has long supported and sought to provide.[3]
- Second, we support the principle underpinning the draft legislation that industry should be given the first opportunity to develop sector specific rules (with oversight by the Office of the Australian Information Commissioner [OAIC]), to ensure they are workable and effective.
- Third, we support the inclusion of "large online platforms" within the scope of the draft legislation, to give consumers confidence that all major online operators who use data in similar ways will be held to the same high standards.

The Australian Government has determined that digital platforms should be subject to stronger privacy rules *first*, in advance of broader cross-economy reform which is being

[1] The Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021
[2] 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.
[3] 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.

contemplated via a separate consultation process about the same issues.[4] However, this staged approach to updating privacy regulation will lead to inconsistent rules across the economy. This is because nearly every company uses data to provide their services - not just large online platforms. Indeed, privacy and data obligations are just as important for e-commerce providers as they are for health services or insurance companies. But the staged approach could mean that similar data practices will be governed differently depending on whether the business is a social media company, a large online platform, a large business that is not an online platform, or a small business. (This is on top of bespoke privacy rules for entities that interact with government agencies, or participate in the Consumer Data Right or COVID-19 tracing app, among other programs.)

As a result, rather than ensuring that consumers have privacy protections that are as clear, consistent and applied as broadly as possible, it will be more confusing and challenging for consumers to understand and assert their privacy rights.

It is surely more appropriate for online platform-specific rules to be developed *after* cross-economy reform rather than before. However, if the Government proceeds with an online privacy code first, we urge the Government to (1) minimise the risks of misalignment between the online privacy code and future cross-economy reform; and (2) ensure that an appropriately broad cross-section of the online industry is captured by the online privacy code, so that consumers have confidence that they will receive a consistent level of protection when they are online. The risk of misalignment can be reduced by taking a less prescriptive approach to some provisions of the draft legislation (in particular, relating to notice and consent, and the right to object), and by providing a longer timeframe for code development (say, 24 months), which would allow for the code to reflect developments in the broader cross-economy reform process.

There are two other critical areas where we encourage further consideration by the Government.

Firstly, the draft legislation establishes new requirements around young people's data and age verification. Protecting our users - particularly young people - is of paramount importance to Meta. Ensuring age-appropriate experiences and robust privacy settings for young users is imperative. We recognise the role that proportionate and risk-based age assurance regulation (in addition to other safety and privacy safeguards) can play in

[4] The Privacy Act Review Discussion Paper, released in October 2021, https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review---discussion-paper.pdf

helping to ensure that young people have an age-appropriate experience online, and we have previously commended the UK's Age Appropriate Design Code as a good starting point for Australian policymakers.

However, we are concerned that the draft legislation could compel companies to collect significantly more data about *all* Australian users, and an even greater level of data about teens and their family. In addition, an overly-rigid approach to parental consent risks overloading parents with consent requests, without leading to meaningful improvements in privacy.

Secondly, the draft legislation establishes a 'right to object' (requirements to cease using or disclosing consumers' data on request) and the explanatory memorandum specifically indicates this right is intended to be applied 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 advertising-supported services by impeding 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. 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 in a recent survey indicated they would prefer an ad-supported internet.[5]
- 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 Facebook apps to help them start their business.[6] 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

[5] Digital Advertising Alliance, 'Americans value free ad-supported online services at $1,400 a year', *Digital Advertising Alliance Website,* https://digitaladvertisingalliance.org/press-release/americans-value-free-ad-supported-online-services-1400year-annual-value-jumps-more-200, September 2020.
[6] Deloitte, 'Dynamic Markets Report: Australia - unlocking small business innovation and growth through the personalised economy', *Meta Australia blog*, https://australia.fb.com/economic-empowerment/, October 2021.

helped businesses target new customers as they have needed to pivot away from bricks-and-mortar operations during the pandemic.

A right to object would be best considered in the context of cross-economy reforms to privacy legislation. However, if the Government retains this requirement for the online privacy code we recommend clarifying that companies can 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) (which appears to be the Government's intention as per the discussion paper for broader privacy reform).

There are also a number of areas where the drafting of the legislation appears to go further than the Government's intention. For example, once a component of a company's business qualifies as a social media service, *all* components of that business are subject to the online privacy code (even if they would not otherwise qualify as social media or an online platform and are unrelated to those services). Similarly, the draft legislation seeks to make Australian privacy law extraterritorial by removing the need for any "Australian link". Consequently, if a company has a service available in Australia, it would mean Australian privacy law would apply to personal information collected from *all* individuals - even those who are not in Australia. These requirements are plainly not proportionate, and our submission makes some drafting suggestions that aim to bring the scope back in line with our understanding of the Government's intent.

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

Recommendations

We make the following suggestions about amendments to the draft legislation for an online privacy code. This will ensure the legislation enables industry to deliver a workable code.

1. If the Government proceeds with an online privacy code prior to cross-economy reform, we urge the Government to minimise the risks of misalignment between the online privacy code and future cross-economy reform. This can be achieved by removing some of the more-prescriptive language (specifically, around notice and consent, and the right to object), and by allowing a longer timeframe for the code to be developed (say, 24 months from the date of the Privacy Reform for the code to be finalised to avoid inconsistencies).

2. If they are retained in the online privacy code legislation, the requirements relating to notice and consent contained in sections 26KC(2)(e) and (g) of the current draft legislation should be clarified to indicate that they will apply at a principle level and will not require relevant organisations to follow specifically prescribed notice and consent practices. It is important for different businesses to retain the flexibility to design notice and consent practices that are most suitable for their particular context.

3. The requirement that organisations must take reasonable steps not to use or disclose personal information upon request by an individual (s 26KC(2(h)) should be removed and instead be addressed in the broader cross-economy reforms. In the event the Government retains these requirements in the online privacy code, it should be amended to expressly state that the requirement to take reasonable steps to stop using or disclosing personal information on request will still allow for continued use or disclosure where required:
    - to complete a transaction or give effect to a contract
    - 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).

4. The government should retain and not narrow the currently proposed definition for large online platforms, to give consumers confidence that all major online operators who use data in similar ways will be held to the same high standards.

5. We recommend that two amendments should be made to the children's data and age verification requirements: (1) the requirement should be for companies to undertake age *assurance* rather than age *verification*, drawing from the work in the UK that has found a bundle of age assurance measures may be more effective and proportionate at determining age than verification alone; and (2) the law should require platforms to take 'reasonable steps' rather than '*all* reasonable steps'. These changes would ensure companies are able to take a balanced approach that does not result in overburdening parents with excessive consent requests.

6. The definition of social media services in this legislation should be amended to ensure it is interpreted in the same way as the definition of 'social media services' under the Online Safety Act.

7. To avoid confusion, the legislation should clarify (s26KC(6)) that the additional compliance obligations intended for social media services are limited to those services and should not extend to any other unrelated service offerings, even if provided by the same organisation. It could be amended by adding words to the effect of those shown in bold here: "the OP code must require OP organisations of a kind covered by subsection 6W(1) to do the following **in relation to social media services they provide**".

8. In relation to new powers to share information in the public interest, we suggest the Information Commissioner should be required to consult with any potentially affected parties. Affected parties should be provided with the opportunity to submit why information should not be disclosed and to seek review of the Information Commissioner's decision if necessary.

9. For the new criminal offence where there is a failure by a body corporate to comply with information requests on multiple occasions in a way that constitutes a system of conduct or pattern of behaviour, we recommend the requirement could be clarified and should include some of the requirements currently set out in APP 12.

10. The extra-territoriality provision should be amended so that Australian privacy law does not apply to instances where both the user and service provider are outside Australia.

Table of contents

Privacy at Meta

Meta provides people with a unique and relevant experience by personalising the content they see. Personalisation presents benefits for users and for businesses. It allows users to see content and advertising that they care about, instead of things that don't interest them. It also allows us to provide content which is most appropriate for a user, taking into consideration their age, location and preferences. Personalisation also allows businesses to connect with customers who are most interested in their products and services.

Personalisation is particularly important for Australian small businesses who often may not have a large enough advertising budget to spend on other forms of advertising. A recent report by Deloitte found that 71 per cent of Australian small businesses who use personalised advertising reported that it is important for the success of their business. Personalised advertising has become even more important over the past two years as businesses have needed to pivot away from bricks-and-mortar operations.

While personalisation relies on the collection and sharing of data, it does not, and should not, come at the expense of a user's privacy. Privacy and protection of people's data are fundamental to our business.

We believe consumers should have meaningful transparency and control over how their data is used. Further, consumers need to be informed in a way that empowers them to make privacy choices that are meaningful for them; privacy policies cannot be the only ways that companies communicate with people about their information.

We've worked with policymakers, regulators, academics, civil society, businesses and other stakeholders over the years to build industry-leading tools that show users how their information is used, and to allow them to manage it.[7] Our products aim to be transparent and informative so that people can easily access specific information about how we collect, use and share their personal information. 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.[8] This tool was unprecedented when it was launched, and we believe it remains unmatched today. We also offer the 'Why am I Seeing This?' feature on any ad in News

[7] 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
[8] 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/

Feed to help users control what they see going forward.[9] For a detailed overview of industry-leading products, tools and policies we offer that enable people to take control of their data, please see our submission in response to the Review of the Privacy Act 1988 issues paper.[10]

We continue to invest in research and development of privacy-enhancing technologies so that we can offer better and more innovative services, while protecting the privacy of our users and giving them flexibility and control over their personal information.

Ensuring age-appropriate experiences

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:

- **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.

- **Limiting advertisers' ability to reach young people:** We now only allow advertisers to target ads to people under 18 in Australia based on their age, gender and location. This means that previously available targeting options, like those based on interests or on their activity on other apps and websites, will no longer be available to advertisers.

[9] 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/.
[10] Meta, 'Submission to the Australian Privacy Act Review Paper, *Attorney General Website,* https://www.ag.gov.au/sites/default/files/2021-02/facebook.PDF, 6 December 2021.

This is in addition to age-gating controls made available for those advertisers who publish age-sensitive ads or content (such as related to gambling).

Through our controls in ad settings, we give people ways to tell us that they would rather not see ads based on their interests or on their activities on other websites and apps. But we've heard from youth advocates that young people may not be well equipped to make these decisions. For this reason, we are taking a more precautionary approach in how advertisers can reach young people with ads.

- **Restricting adults from privately messaging young people:** Since 2020, we have sent safety notices to users in Messenger, and subsequently Instagram, if we believe an adult could be pursuing a potentially inappropriate private interaction with a teen. These notices are designed to discourage inappropriate interactions with children and to limit the potential for grooming to occur via Messenger and Instagram.[11] These are over and above restrictions in place on Messenger and Instagram preventing an adult from privately messaging an unconnected young person.

- **Making it more difficult for adults to find and follow teens:** We've developed new technology that will allow us to find accounts that have shown potentially suspicious behaviour, such as accounts that have been blocked or reported by a young person, and stop those accounts from interacting with young people's accounts.

  Using this technology, we won't show young people's accounts in Explore, Reels, 'People You May Know' or 'Accounts Suggested For You' to these adults. If they find young people's accounts by searching for their usernames, they won't be able to follow them. They also won't be able to see comments from young people on other people's posts, nor will they be able to leave comments on young people's posts. We'll continue to look for additional opportunities to apply this technology to protect young people from unwanted contact.

- **Implementing stricter controls for sensitive content:** We recently announced a Sensitive Content Control on Instagram. We recognise that people have different preferences when it comes to sensitive content which does not break our rules but could be potentially upsetting (such as sexually suggestive or violent

[11] J Sullivan, 'Preventing unwanted contacts and scams in Messenger', *Messenger News*, 21 May 2020, https://messengernews.fb.com/2020/05/21/preventing-unwanted-contacts-and-scams-in-messenger/.

content). This new tool provides users with the control to adjust their preferences to see either more or less sensitive content. We default users who are under the age of 18 on Facebook and Instagram into being unable to see sensitive content; however, this tool also allows them and their parents the option of removing even more potentially sensitive content for an even safer viewing experience.[12]

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 have even greater controls for a service where we allow users under the age of 13. The parental controls that are appropriate for a 12-year-old are very different to those appropriate for a 17-year-old.

In 2020, in response to the COVID-19 pandemic and to ensure that families could stay in touch while isolating or in lockdown, we accelerated the launch in Australia of a product called Messenger Kids. This is a new messaging product for users who are not yet 13, and provides them with much greater privacy and security controls than regular Messenger. Parental control is at the heart of Messenger Kids. Parents manage who their child interacts with and can monitor their child's activity in the app through the Parent Dashboard, where they can also download their child's information at any time.

The design of Messenger Kids, and the control measures, have been developed after extensive consultation with a team of experts in online safety, child development and media, as well as parents. We continue to update our controls, and our privacy notices and disclosures, to reflect feedback from these consultations.

By working with parents and other experts, we aim to continue providing controls that ensure age-appropriate experiences for young people.

[12] Meta, 'Introducing sensitive content control', *Meta Newsroom*, 20 July 2021, https://about.instagram.com/blog/announcements/introducing-sensitive-content-control

Overarching comments on the exposure draft legislation

One of the most important considerations relating to the draft online privacy code legislation is the intersection between a code and the broader review of the Privacy Act. The Government's Privacy Act Review Discussion Paper proposes cross-economy reforms that cover many of the same areas as the draft legislation, including on fundamental concepts such as notice and consent, the right to object, and a right to object specifically for direct marketing. The Government has set a timeframe that will see the online privacy code developed and finalised first, before any cross-economy reforms.

While we understand the Government is committed to proceeding with online-specific privacy reform first, this timeframe means it will be very challenging to develop an online privacy code that will remain fit-for-purpose in the long term. The online privacy code would need to be developed in reference to the current APPs, which may be soon out of date. The current draft sets very prescriptive requirements that specifically reference compliance with the APPs: for example, the draft legislation proposes that the online privacy code will set out how relevant organisations are to comply with APPs 1.4(c), 3, 5 and 6. At the same time, the Privacy Act discussion paper proposes amendments to those APPs. This provides a high level of uncertainty throughout the drafting of the online privacy code, because industry could develop a code that is workable in relation to the current APPs, but is misaligned with future amendments to the APPs and will become immediately outdated once those amendments take effect.

If the Government's intention is to deliver cross-economy privacy reform that is aligned with the online privacy code, we would raise concerns that an important piece of legislation, which will set the standard for cross-economy reform, is being drafted within a very short period of time.

The Privacy Act Discussion Paper proposes a number of general amendments that would duplicate provisions contemplated for the online privacy code. A clear example of this is the proposal to introduce a requirement that organisations subject to the code be required to take reasonable steps not to use or disclose the personal information of an individual on request by the individual. A similar "right to object" is also proposed in the Privacy Act Discussion Paper. If the proposal in the Discussion Paper were adopted and the Privacy Act amended to introduce a right to object in respect of all entities that are subject to the Privacy Act, it would lead to this aspect of the online privacy code either being redundant (if the right to object was drafted in the same way), or being inconsistent with the Privacy Act (if the right was formulated in a different way).

If the online privacy code falls out of step with future changes to the Privacy Act, then it would be necessary to update the online privacy code, which would at that stage be the third major change in privacy regulation in a short period. Regularly-changing privacy requirements will lead to complexity and confusion for consumers (not to mention disproportionate and unnecessary regulatory compliance costs).

Consumers are best served by clear and consistent privacy protections. Consumers should have the same fundamental rights and protections no matter what type of business they are dealing with. Deviations should be limited wherever possible, as they only make it more difficult for consumers to understand their legal rights. Deviations also introduce complexity for businesses, particularly those that work across different industries and so may be exposed to different rules for different parts of their operations and also those that work both with some businesses that are captured under the online privacy code and some that are not.

For this reason, any sector-specific rules should be tightly focused and should be reserved for matters that are truly unique to the industry in question. The need for such rules can only be properly assessed once there is a stable baseline. Accordingly, as a matter of policy, we strongly believe that any online privacy code should only be considered after the Government has finalised cross-economy privacy reforms.

However, if the Government believes it is necessary to progress the online privacy code before proper consideration and consultation on cross-economy reform, the risk of misalignment could be significantly reduced by allowing greater flexibility as to what should be covered under the online privacy code, and allowing a slightly longer timeframe for its development such as 24 months instead of 12 months. This should not delay other reforms contemplated under the draft legislation, such as changes to penalties and changes to the extra-territorial application of the Privacy Act. However, it would help to ensure that any online privacy code that is developed is durable and workable in practice.

There is a significant amount of prescription set out in the legislation, which will provide a rigid framework that cannot be easily adapted in response to changes in technology. This level of legislative prescription has not been necessary for other recent online platforms codes in Australia, such as the voluntary industry code on disinformation and misinformation, or the codes being developed under the Online Safety Act. Given the OAIC also intends to issue an additional position paper to set out their expectations about the detail of the online privacy code, it is not necessary to include this level of prescription in legislation (for example, by setting particular definitions of notice or consent that must be used in the online privacy code).

The most prescriptive aspects of the draft legislation that we recommend adjusting include:

- Clarifying that requirements relating to notice and consent contained in sections 26KC(2)(e) and (g) of the current draft legislation will apply at a principle level and will not require relevant organisations to follow specifically prescribed notice and consent practices. It is important for different businesses to retain the flexibility to design notice and consent practices that are most suitable for their particular context;
- Removing the requirement that organisations must take reasonable steps not to use or disclose personal information upon request by an individual (s 26KC(2(h)) so this can be addressed in the broader cross-economy reforms. Although, in the event the Government retains these requirements in the online privacy code, we have provided suggestions below.

Specific comments on the exposure draft legislation

Scope of organisations covered

The categorisation of online messaging services and online interactive gaming services under the draft online privacy code legislation should be clarified as online platforms rather than social media services.

In other legislation in Australia, the definition between social media and other services is more clearly defined. For example, the Online Safety Act 2021 distinguishes between 'social media services' and 'relevant electronic services' (defined as a service that enables end-users to communicate with other end-users by email; instant messaging; short message service (SMS); multimedia message service (MMS); or a chat service or a service that enables end-users to play online games with other end-users). Under the Online Safety Act, a messaging platform, such as WhatsApp, or an interactive gaming service will be regulated as a relevant electronic service rather than as a social media service.

The position under the online privacy code exposure draft legislation is less clear. The exposure draft has taken the definition of 'social media service' from the Online Safety Act, but not included the concept of 'relevant electronic service'. The Explanatory Paper for the draft legislation indicates that online messaging platforms, like WhatsApp, as well as interactive gaming services *will be* social media services under the online privacy

code. This means that, although the defined term ‘social media service’ is the same across the two pieces of legislation, their interpretation would be different.

For consistency with the Online Safety Act and to avoid confusion, we suggest that online messaging services like WhatsApp, as well as interactive gaming services, should not be treated as social media services under the online privacy code (noting they would still fall under the definition of large online platforms, which attracts different requirements). This approach reflects the fundamental differences in the nature of these services and social media services.

The Explanatory Paper for the draft online privacy code legislation argues that social media platforms pose a higher risk to children than other large online platforms due to “the nature of the interactions that can occur via social media platforms, and the wide range and volume of personal information that social media platforms handle.” While we do not accept that this assertion is correct, the same rationale clearly does not apply to messaging services such as WhatsApp. WhatsApp collects an extremely limited set of personal information from each user at sign up (a name and a telephone number). The content of messages sent on WhatsApp are end-to-end encrypted, which means that WhatsApp cannot see the contents of messages sent on the platform. This means that WhatsApp actually collects significantly less personal information than a number of other organisations that are likely to be large online platforms.

Further, the nature of a messaging platform or an online gaming service significantly differs from a social media platform in that messaging and gaming generally involve an individual communicating one-on-one or with a limited group of their choosing and does not involve personalisation in the same way as social media. For these reasons, the definition of social media services in this legislation should be interpreted in the same way as the definition of social media services in the Online Safety Act.

Scope of social media organisations

The draft legislation applies at the organisation level, rather than the service level. This appears to be inconsistent with the principle underpinning the code, which is that certain services are higher risk than others.

The current drafting in the legislation suggests that, if an organisation provides a social media service, a data brokerage service or a service that brings it within scope of the definition of ‘large online platform’, that organisation would need to comply with the online privacy code in respect of *all* of its products or services, regardless of whether

they would have otherwise met the criteria specified in s 6W. For example, if an organisation provides a social media service but also provides a completely unrelated enterprise service, that service would be captured by the online privacy code, even if the enterprise service would not have otherwise been captured.

This puts the separate services of a large online platform at a potential significantly different compliance requirement, compared to other competitors within Australia. It is also not consistent with the rationale for the online privacy code, which is focused on the nature of the services provided by an organisation, rather than the organisation itself.

To avoid confusion, it should be clear that the additional compliance obligations intended for social media services are limited to those services and should not extend to any other service offerings, even if provided by the same organisation. To achieve this, s 26KC(6) should be amended by adding words to the effect of those shown in bold here: "the OP code must require OP organisations of a kind covered by subsection 6W(1) to do the following **in relation to social media services they provide:**"

So that the draft online privacy code legislation contains a formal defined term for social media services, s 6W(1) should also be amended in the following manner: "provides an electronic service that satisfies each of the following conditions **(a social media service)**:"

Right to object

The draft legislation proposes that the online privacy code 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.

The explanatory paper to the draft legislation indicates one of the priorities of a right to object relates to direct marketing, and enabling people to object to their data being used for direct marketing purposes.

While we strongly support arming consumers with rights to opt out of direct marketing services such as an email marketing newsletter, 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.[13] 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.

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,[14] 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.

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.[15] 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

[13] Digital Advertising Alliance, 'Americans value free ad-supported online services at $1,400 a year', *Digital Advertising Alliance Website,* https://digitaladvertisingalliance.org/press-release/americans-value-free-ad-supported-online-services-1400year-annual-value-jumps-more-200, September 2020.
[14] Infogroup, *The Power of Personalization,* https://www.emarketer.com/chart/228797/attitudes-toward-personalization-among-us-internet-users-jan-2019-of-respondents, May 2019.
[15] Deloitte, 'Dynamic Markets Report: Australia - unlocking small business innovation and growth through the personalised economy', *Meta Australia blog*, https://australia.fb.com/economic-empowerment/, October 2021.

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.[16]

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

Given the significant economic benefits of personalised advertising, the online privacy code legislation 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 services 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 in the market for social media services, there are ample other options if consumers object to using an advertising-supported service.

We understand that it is not the Government's intention to force ad-supported businesses to change their business model. The Privacy Act Discussion Paper, which deals with this same issue, suggests that there should be a right to object to the use of personal information for direct marketing, but also contemplates that in this instance one consequence may be that a service provider will no longer be able to provide relevant services to the objecting user (see pages 113 and 132 of the Privacy Act Discussion Paper).

Ideally, a proportionate and carefully-tailored right to object would be established in cross-economy legislation, rather than a sector-specific code. It would be a critical, new

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

consumer right that should be applied across all businesses subject to the APPs, in order to ensure consistently high privacy standards across the economy.

However, if the Government retains a right to object in the online privacy code, to avoid confusion, we suggest that the draft legislation be amended to reflect the intention set out in the cross-economy reform discussion paper and ensure that ad-supported business models are not fundamentally undermined. We recommend that the legislation clarify that companies may cease to provide a service to an individual who requests the organisation to no longer use their personal information to the extent such use is necessary to provide the service.

A blanket right to object is not practical. The legislation should also clarify that companies may need to retain and handle personal information for the purpose of complying with the individual's objection request, and limited to reasonable archival storage. 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. Consistent with the discussion paper on cross-economy reform, we also recommend that the draft legislation expressly state that the requirement to take reasonable steps to stop using or disclosing personal information on request will still allow for continued use or disclosure where required:

- to complete a transaction or give effect to a contract
- 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).

Children's data and age verification

Protecting our users - particularly young people - is of paramount importance. As outlined above, 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, 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.

We suggest that any regulation relating to protecting young people's data be developed in recognition of the following principles, to ensure that 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).

While we support in principle new regulation in Australia relating to age assurance and ensuring age appropriate experiences online, we have some specific comments and concerns about the proposal. The following sections provide comments on age verification and parental consent.

Meta's views are informed by our ongoing, global consultation with experts, parents and teens themselves.

Age verification

Although there is a growing consensus globally that companies should provide age-appropriate experiences for young users, there is ongoing debate and discussion around the world about the best way to do that. Understanding the ages of people on the internet is a complex and industry-wide challenge, with many competing goals at play.

We are concerned that the current age verification proposal would compel social media services to collect significantly more data about all Australian users, and an even greater level of data about teens and their families. Collecting such data is at odds with the principle of data minimisation (as referred to in the Privacy Act Discussion Paper).

Industry is developing promising ways to offer multi-faceted age assurance solutions. These solutions aim to address privacy concerns by taking a proportionate approach to understanding a user's age, without requiring the collection of additional personal information about a user.

We have outlined below Meta's layered approach to age assurance on Facebook and Instagram. We aim to strike a balance between protecting people's privacy, wellbeing, and freedom of expression, while taking into account technical and operational constraints involved in verifying ages.

First, Facebook and Instagram require everyone in Australia to be at least 13 years old before they can create an account. We require users to provide their date of birth into an "age screen" when they register. The age screen is neutral (i.e. does not assume that someone is old enough to use our service), and we restrict people who repeatedly try to enter different birthdays into the age screen.

But we also recognise that some people may misrepresent their age online. For that reason, we have been developing artificial intelligence tools to better understand someone's real age. This technology allows us to estimate people's ages -- i.e, if someone is below or above 18. We train the technology using multiple signals. We look at things like the age written in "happy birthday" posts: for example, "Happy 21st Birthday!". We also look at the age users have shared across apps: for example, if a user has shared their birthday on Facebook, we'll use the same for linked accounts on Instagram.

We're focused on using existing data to inform our artificial intelligence technology. Where we do feel we need more information, we're developing a menu of options to allow people to prove their age.

We're also in discussions with the wider technology industry on how we can work together to share information in privacy-preserving ways to establish whether people are over a specific age. One area we believe has real promise is working with operating system providers, internet browsers and other providers so they can share information to help apps establish whether someone is of an appropriate age.

This would have the dual benefit of helping developers keep underage people off their apps while removing the need to go through differing and potentially cumbersome age verification processes across multiple apps and services. While we are confident in the effectiveness of our approach to understanding user age, these measures should not end with an individual app or website. Collaboration with operating system providers, internet browsers and others can help protect users upstream as one component of an ongoing multilayered approach.

Technology like this is new, evolving, and it isn't perfect. It also may not always be the most appropriate measure for all use cases. Inaccurate AI predictions could undermine people's ability to use services, for example, by incorrectly blocking them from an app or feature based on false information. There is no single, fail-safe solution to age assurance and, hence, technology such as this should be used in conjunction with other age assurance measures -- such as age collection at registration and community reporting tools.

The use of identification documents to verify age, however, raises significant privacy, wellbeing and access concerns. Good regulation should not depend on the collection of young people's ID documents, such as driver's licenses. There are significant limitations to relying on ID collection. Lack of ID access disproportionately impacts disadvantaged communities in Australia. Even if they did have an ID, some young people may be uncomfortable sharing it. For example, perhaps they're a young member of the LGBTQIA+ community and they worry about having their identity attached to an account engaged as part of that community.

Requiring companies to collect IDs from people may also be inconsistent with the core data protection principle of data minimisation. It is important that any requirement to verify a user's age balances these considerations with the intended policy goal.

We would suggest that future regulation recognises the complexities of determining a user's age online, and the inherent trade offs when requiring the collection of ID and age verification data.

While we acknowledge the Government's intention to include requirements in the online privacy code around age-appropriate experiences, the current drafting of the draft legislation risks diverging from international best practices around age assurance. drafting means the Australian legislation would go well beyond similar requirements in the UK. These requirements would apply to *all* Australian users, not only to accounts that we suspect are maintained by children. Depending on the method of verification used, this could involve collection of new types of information about users on a mass scale. (This seems to be confirmed by the Regulatory Impact Statement, which estimates that the compliance cost for social media platforms would be >$500 million.) If a user is clearly over 18, we do not believe there is a clear policy justification for why a social media operator should have to verify their specific age. It should not make a difference if the user is 18 or 28 or 38; if they are 48 and want to present their online identity as 38, that should be a matter for them.

To ensure a more proportionate requirement that aligns with current international best practice, we recommend making the following two amendments to the drafting:

1. The exposure draft currently requires social media platforms to take *all* reasonable steps to verify the age of all individual users. Use of the word 'all' does not allow companies to develop their own, most appropriate approach to understanding someone's age; it would compel them to use every possible age verification measure, even if it is not suitable for their services. Each company should have the flexibility to determine their approach to understanding a user's age based on their policies, tools, and technical and operational capabilities. We recommend removing the word 'all' and requiring companies to take 'reasonable steps'.
2. The legislation requires age *verification*. This would go beyond requirements in the Online Safety Act and associated supplementary regulations. We do not agree that requiring more data collection from digital platforms (including platforms based in countries with data access regimes with far fewer checks and balances than in Australia) for all users is a good outcome from a privacy perspective. We recommend replacing the term verification with age *assurance*, which requires companies to provide age-appropriate experiences but without compelling additional data collection.

Parental consent

The draft online privacy code legislation requires that a social media service provider must obtain consent from a parent or guardian before it collects, uses or discloses the personal information of a child who is under the age of 16, and that the service provider must take all reasonable steps to verify the consent.

Policymakers should not assume that requiring parental consent is the ultimate 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.

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

However, as currently drafted, the provisions around parental consent in the draft legislation would represent an unworkable and disproportionate obligation for service providers, and could also be an overwhelming or ineffective experience for parents. We believe it requires redrafting for the following reasons:

- **The legislation risks 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.[17] 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[18] 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. To the credit of the Government, the discussion paper on cross-economy reform recognises that "while consent is

[17] 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". It is not clear whether this is intended to elevate the role of consent by requiring consent to be obtained in circumstances where it is not currently required under APPs 3 and 6;
- 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.

[18] Meta, 'Submission to the Australian Privacy Act Review Paper, *Attorney General Website,* https://www.ag.gov.au/sites/default/files/2021-02/facebook.PDF, 6 December 2021.

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. Research 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.

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.

- **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**. The legislation 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), 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 risks, we recommend that the Government amend the legislation 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.

Information sharing

The draft online privacy code legislation will give the Information Commissioner the ability to disclose information acquired in the course of exercising their powers or performing their functions or duties where they are satisfied that it is in the public interest to do so. We suggest that before exercising the right to share information in the public interest, the Information Commissioner should consult with any potentially affected parties and allow them to make submissions as to why all or some of the information should not be disclosed and to seek review of the Information Commissioner's decision if necessary. Without this type of protection it will be much harder for regulated entities to be comfortable sharing information with the Information Commissioner on a voluntary basis, as there would be a heightened underlying risk of that information being shared outside an entity's control.

Information requests

The draft online privacy code legislation introduces a separate criminal offence where there is a failure by a body corporate to comply with information requests on multiple occasions in a way that constitutes a system of conduct or pattern of behaviour.

As the draft online privacy code legislation is currently drafted, it is unclear when the criminal penalties could be triggered; it is unclear when an entity's actions would be considered to constitute a "system of conduct" or "pattern of behaviour". There is also uncertainty as to the scope of the "reasonable excuse" exception that currently applies under section 66(1B) of the Privacy Act where an entity is unable to respond to a requirement to provide information.

Given the serious implications of applying a criminal penalty, we suggest that this requirement be further clarified. In addition to the general "reasonable excuse" exception there should be an express statement that an entity is not required to provide information that does not exist or that is not reasonably accessible by the entity, along with carefully-tailored requirements to (1) ensure that a reasonable time period be allowed to respond to requests for information; (2) protect trade secrets; and (3) exempt data that could adversely affect the rights and freedoms of others. This is particularly pertinent to situations where a requirement may relate to highly technical or voluminous information. The Privacy Act Discussion Paper engages with these issues in

the context of individual information access rights under APP 12 and proposes a number of alternatives, including that entities may, as a substitute for providing access to the information itself, provide a general summary or explanation of information that is highly technical or voluminous in nature or may otherwise not be readily understood (see Proposal 18.3). A similar approach should apply for requirements to produce information to the Information Commissioner.

Extra-territoriality

While we are generally supportive of changes to clarify the extra-territorial operation of the Privacy Act, the proposed change to the "Australian link" test means that any foreign corporation that carries on business in Australia will be bound to comply with the Australian Privacy Act even in relation to personal information that they collect from individuals who are not in Australia.

For example, if a US corporation carries on business in Australia through providing services to Australian end users, then the updated "Australian link" test would mean that the Privacy Act would also apply to that corporation's handling of information about users in the US or in any other jurisdiction where that corporation makes its services available. This appears to be an unintentional consequence of the proposed drafting changes. In principle, we see no reason for Australian laws to seek to regulate management of personal information that has no direct connection with Australia or with Australians.