Meta

Submission on the Children’s Online Privacy Code Issues Paper

August 2025

Executive Summary

Meta welcomes the opportunity to make a submission in response to the Children's Online Privacy Code (**COPC**) Issues Paper released by the Office of the Australian Information Commissioner (**OAIC**). We fully support initiatives that promote a balanced approach to children's data protection in light of children's other fundamental rights and freedoms.

Meta's technologies connect people all around the world, creating opportunities and giving a voice to billions. For young people in particular, the digital world offers significant opportunities and we are committed to helping build safe, healthy and supportive online communities where they can participate in a way that suits them.

Since 2019, Meta has invested more than US$8 billion in building and continuing to evolve a rigorous privacy program that identifies and addresses privacy risks early and embeds privacy into our products from the start. We adopt a layered approach to privacy and provide multiple levels of user engagement and information dissemination to make our privacy practices more transparent, useful and understandable. We recognise that information about our products and services, and specifically how people's data is used, needs to meet the needs of a global population with varying digital and linguistic literacy. Our Privacy Policy has been written to make it easy to understand and clear about how we use user information. This includes using simple language, aiming for age 11-13 (middle school, 6-8 grade) level, determined by a Flesch-Kincaid reading score.

As the United Nations Convention on the Rights of the Child (**UNCRC**) General Comment on the Rights of the Child in the Digital Environment states, *"[t]he best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context"*.[1] In practice, it requires organisations to make an assessment based on the specific context in question and balance the young person's right to identity; freedom of association; freedom of expression, including the freedom to seek, receive and impart information; the right to education, and the right to play and take part in a wide range of activities - so that there are no unintended consequences for the young person. At Meta, we developed a process to help us translate this from policy into practice. We refer to this internally as the Meta Best Interests of the Child Framework which distils the best interests framework into six key considerations for product teams which we elaborate on below.

Applying this process, we have long developed additional protections for young people to protect their privacy and safety in an age-appropriate way. A recent example of this was our launch of Teen Accounts on Instagram in Australia in September 2024, to automatically provide teens with built-in protections and reassure parents that

[1] UN Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment', https://digitallibrary.un.org/record/3906061?ln=en&v=pdf, [12]

teens are having safe experiences.[2] We built Teen Accounts after conducting consultations with over 600 stakeholders, 300 teens and 270 parents from more than 351 countries to inform a number of the safety and privacy features of Meta technologies.[3] Now, there are at least 54 million active Teen Accounts globally, with 97% of teens ages 13-15 electing to remain in these protections.[4] We are now expanding Teen Accounts to Facebook and Messenger.[5]

With respect to the COPC, we welcome the recognition by the OAIC that *"[t]he aim of the Code is not to prevent children from engaging online, but to ensure their personal information is protected within that space."*[6] Achieving this aim requires a balanced approach to children's data protection in light of children's other fundamental rights and other regulatory objectives, such as safety and security. In turn, this includes a need for: a holistic view of the role of data in protecting young people and their rights; an understanding of age assurance as an ongoing process and not a one-time event; and, a recognition that multiple legal bases are needed to provide relevant, useful and safe online services. We also encourage the OAIC to shape the COPC mindful of the importance of a 'whole-of-ecosystem' approach to age assurance, which will be a best practice, data minimisation approach, and also mindful of the role of parents and guardians.

In developing the COPC, we encourage the OAIC to consider the following principles:

- **Best interests of the child** which should be applied holistically, balancing the right to privacy with young people's rights to identity, play, education and also freedom of expression and freedom of association, and to seek, receive and impart information.

- **Risk-based approach** which should be applied consistently across all provisions of the COPC, having regard to the other regulatory obligations protecting young people, especially online safety laws. This includes recognising the many individual benefits and safety and security measures that require ongoing personalisation and customisation of services.

[2] Meta, 'Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents', Newsroom, 17 September 2024, https://about.fb.com/news/2024/09/instagram-teen-accounts; Meta, 'Expanding Teen Account Protections and Child Safety Features', *Newsroom*, 23 July 2025, https://about.fb.com/news/2025/07/expanding-teen-account-protections-child-safety-features

[3] Meta, 'How research and consultation informed Instagram Teen Accounts: a new protected experience for teens, guided by parents', Trust, Transparency & Control Labs, 17 September 2024, https://www.ttclabs.net/site/assets/files/12047/how_research_consultation_informed_instagram_teen_accounts.pdf

[4] Meta, 'Working With Parents and New Technology to Enroll More Teens Into Teen Accounts', *Newsroom*, 21 April 2025, https://about.fb.com/news/2025/04/meta-parents-new-technology-enroll-teens-teen-accounts

[5] Meta, 'We're Introducing New Built-In Restrictions for Instagram Teen Accounts, and Expanding to Facebook and Messenger', *Newsroom*, 8 April 2025, https://about.fb.com/news/2025/04/introducing-new-built-in-restrictions-instagram-teen-accounts-expanding-facebook-messenger

[6] Office of the Australian Information Commissioner, 'OAIC Children's Online Privacy Code: Issues Paper', 12 June 2025, https://www.oaic.gov.au/__data/assets/pdf_file/0025/254662/Childrens-Online-Privacy-Code-Issues-Paper-2025-2-7-2025.pdf, p3

- **Age appropriate experiences require ongoing efforts** and are not a single tactic but rather part of a collection of ongoing efforts that work dynamically to provide effective solutions.

- **'Whole-of-ecosystem' solutions** minimise data collection, prioritise data privacy and security, and implement a privacy-preserving approach to age assurance.

- **Enabling parental/guardian support** because of the pivotal role they play in supporting the development of their children and determining what is best for them.

- **International harmonisation** as given the already strong international focus on youth safety online and age appropriate experiences, including the Age Appropriate Design Code in the United Kingdom (**AADC**)[7] and the Irish Fundamentals for a Child-Oriented Approach to Data Processing (**Fundamentals**)[8], and the global nature of the services that many young Australians use daily, it is helpful for the COPC to be developed consistent with existing and relevant international developments.

[7] UK Information Commissioner's Office, 'Age appropriate design: a code of practice for online services', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services

[8] Irish Data Protection Commission, 'The Fundamentals for a Child-Oriented Approach to Data Processing', https://www.dataprotection.ie/en/dpc-guidance/fundamentals-child-oriented-approach-data-processing

Overview of Meta's approach to privacy

Before turning to our specific comments on the COPC, we wanted to provide some background on Meta's approach to protecting privacy, to give context to our comments.

Overall, Meta's approach to protecting children's privacy forms part of our general, multilayered approach to protecting all users' privacy, which includes ensuring clear, accessible information and user control over personal information across all Meta platforms.

Protection of privacy and safety are closely entwined. Meta has designed its services to protect the privacy and safety of users by integrating a comprehensive suite of safeguards and controls. We have also implemented further safeguards in the best interests of young people, striking a balance between protecting them and facilitating their connection and development in the digital environment.

Since 2019, Meta has invested more than US$8 billion in building and continuing to evolve a rigorous privacy program that identifies and addresses privacy risks early and embeds privacy into our products from the start. For example, our privacy review process[9] is a central part of developing new and updated products, services, and practices at Meta. Through this process, we assess privacy risks that collecting, using, or sharing people's information may present, and to help determine what steps should be taken to mitigate any identified privacy risks, including through the development and use of AI models and tools.

Our layered approach to privacy is exemplified in our Privacy Centre, which we launched in 2022 as a centralised educational hub for users to learn about Meta's approach to privacy and how they can manage and control their privacy on Facebook, Instagram, Messenger and other Meta products.[10]

We provide multiple levels of user engagement and information dissemination to make our privacy practices more transparent, useful and understandable:

1. **Clear communication:** We recognise that information about our products and services, and specifically how people's data is used, needs to meet the needs of a global population with varying digital and linguistic literacy. For instance, in 2022, we rewrote and re-designed our Privacy Policy to make it easier to understand and clearer about how we use user information, and updated our Terms of Service to better explain what is expected from us and those who use our platforms.[11] This includes:

[9] Meta, 'Privacy progress update', https://about.meta.com/uk/privacy-progress

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

[11] Meta, 'Here's What You Need to Know About Our Updated Privacy Policy and Terms of Service', *Newsroom*, 26 May 2022, https://about.fb.com/news/2022/05/metas-updated-privacy-policy

a. using simple language, aiming for age 11-13 (middle school, 6-8 grade) level, determined by a Flesch-Kincaid reading score;

b. using relatable examples, storytelling, videos, illustrations and infographics where possible to effectively explain the data practice; and

c. making information findable - giving individuals access to our policy intuitively from our products, and making it easy for people to readily find the information they want within it (e.g. efficient navigation, meaningful sections and useful summaries).

We made these changes to the policy to facilitate more user engagement and promote greater understanding and control over personal information, to empower users to make informed decisions about their online experiences. We also continue to regularly review and update the policy for this and other purposes.

2. **Educational resources:** Our Privacy Centre includes modules on common privacy topics such as sharing, security, data collection, data use, AI and ads. These modules provide users with detailed information on how Meta handles their data and what controls are available to manage their privacy.[12]

   Teen-specific sections on our Privacy Centre provide teens with information about experiences across our platforms that are different for users under 18. Our 'Access support and resources for teens' page enables teens to learn more about our safeguards, link to additional resources, and review their settings.[13]

3. **Accessible controls:** We provide transparency measures and tools that give people greater insight and control over their experiences on Meta's apps and services. Our Privacy Centre provides direct links to privacy settings, allowing users to easily adjust their preferences and control how their information is used across Meta's apps and services, and limit who can see what they share.[14] Users are also empowered to review and update their settings at any time to change their choices.

As the UNCRC General Comment on the Rights of the Child in the Digital Environment states, an assessment of the *"best interests of the child ... requires an assessment appropriate to the specific context"*[15]. Centering the "best interests of the child" standard across all considerations requires an appropriate balance between protecting young people's privacy, safety, and wellbeing and empowering them with tools to

[12] Meta, *Privacy Centre*, https://www.facebook.com/privacy/center

[13] Meta, 'Access support and resources for teens', *Privacy Centre*, https://www.facebook.com/privacy/guide/teens

[14] Meta, *Privacy Centre*, https://www.facebook.com/privacy/center

[15] UN Convention on the Rights of the Child, 'General comment No. 25 (2021) on children's rights in relation to the digital environment', https://digitallibrary.un.org/record/3906061?ln=en&v=pdf, [12]

express themselves, access information, and build community online - so that there are no unintended consequences for the young person.

At Meta, we developed a process to help us translate this from policy into practice. We refer to this internally as the Meta Best Interests of the Child Framework which distils the best interests framework into six key considerations for product teams, and provides guidance on each, with context and examples on how to use them to make difficult decisions and tradeoffs:[16]

- Recognise and engage global youth and families using our products
- Create safe, age-appropriate environments for youth
- Promote youth autonomy while considering the role and duties of parents and guardians
- Prioritise youth well-being and safety over business goals and interests
- Support youth privacy in all product decisions
- Empower youth, parents and guardians to understand and exercise their data rights

Applying this process, we have long had additional protections for young people to protect their privacy and safety in an age-appropriate way. As a recent example, as mentioned above, we launched Teen Accounts on Instagram, and are now expanding this to Facebook and Messenger, to automatically place teens in built-in protections and reassure parents that teens are having safe experiences.[17] Teen Accounts was launched on Instagram in Australia in September 2024 and has now been rolled out globally. Now, there are at least 54 million active Teen Accounts globally.[18]

Informing our development of the features of Teen Accounts was considerable research and consultation with more than 600 stakeholders, 300 teens and 270 parents from more than 351 countries. This work confirmed that teenagehood is a transitional time when teens are learning how to express themselves and building community - whether online or offline - plays an important role in their development. Teens may use online spaces for connection and to discover new things, and we want to preserve these spaces for them when considering new, protected experiences. We

[16] Meta, 'Meta's Best Interests of the Child Framework', Trust, Transparency & Control Labs, https://www.ttclabs.net/news/metas-best-interests-of-the-child-framework

[17] Meta, 'Introducing Instagram Teen Accounts: Built-In Protections for Teens, Peace of Mind for Parents', *Newsroom*, 17 September 2024, https://about.fb.com/news/2024/09/instagram-teen-accounts; Meta, 'We're Introducing New Built-In Restrictions for Instagram Teen Accounts, and Expanding to Facebook and Messenger', *Newsroom*, 8 April 2025, https://about.fb.com/news/2025/04/introducing-new-built-in-restrictions-instagram-teen-accounts-expanding-facebook-messenger

[18] Meta, 'Working With Parents and New Technology to Enroll More Teens Into Teen Accounts', *Newsroom*, 21 April 2025, https://about.fb.com/news/2025/04/meta-parents-new-technology-enroll-teens-teen-accounts

also know that teens want their online experiences to be positive. We received feedback from teens that:

- They tend to look for continued support from social media apps, including tools that would address situations where they perceive they are wasting time, come across unappealing content or come in contact with people who make them uncomfortable.

- They are interested in ways that digital services might provide transparency and controls to help drive age-appropriate experiences.

- They see value in their parents having more insights at their disposal. Teens view supervision tools as useful since their changing patterns of behavior can be used as evidence to show their parents or caregivers that they are ready to handle greater responsibility, choice and control over time.[19]

Against this background, we developed the following features for Teen Accounts on Instagram:

- **Private accounts:** With default private accounts for new and existing teens, teens need to accept new followers and people who do not follow them cannot see their content or interact with them. This is the default setting for all new and existing teen accounts (13-17 years old), with the only exception being existing late teen accounts (16-17 year olds) who can retain their account privacy state and will not be switched to private if they have previously converted their account to public. This approach reflects the importance of ensuring the autonomy and independence of older teens in making privacy-related decisions, acknowledging that they are more capable of making informed choices about their online presence.

- **Messaging restrictions:** Teens are placed in the strictest messaging settings, so they can only be messaged by people they follow or are already connected to.

- **Sensitive content restrictions:** Teens are automatically placed into a strict setting of our 'sensitive content control', which limits the type of sensitive content (such as content that shows people fighting or promotes cosmetic procedures) teens see in places like Explore and Reels.[20] We continue to explore new ways to tailor teen content on our platform and provide more control for parents to shape their teen's content experience.

- **Limited interactions:** Teens can only be tagged or mentioned by people they follow. We also automatically turn on the most restrictive version of our

[19] Meta, 'How research and consultation informed Instagram Teen Accounts: a new protected experience for teens, guided by parents', Trust, Transparency & Control Labs, 17 September 2024, https://www.ttclabs.net/site/assets/files/12047/how_research_consultation_informed_instagram_teen_accounts.pdf
[20] See Meta, 'New Protections to Give Teens More Age-Appropriate Experiences on Our Apps', *Newsroom*, 9 January 2024, https://about.fb.com/news/2024/01/teen-protections-age-appropriate-experiences-on-our-apps

anti-bullying feature, Hidden Words, so that offensive words and phrases are filtered out of teens' comments and DM requests.

- **Time limit reminders:** Teens get notifications telling them to leave the app after 60 minutes of use each day.
- **Sleep mode enabled:** Sleep mode is turned on between 10pm and 7am, which mutes notifications overnight and sends auto-replies to DMs.

In July, we announced new safety features for Teen Accounts to protect teens from potentially unsafe and unwanted contact in DMs - giving teens more context about the accounts they are messaging (e.g. the month and year an account joined Instagram or if the account is overseas) and helping them spot potential scammers, and the ability to block and report DMs at the same time to make the reporting process easier.[21]

Teens under 16 and teens 16-17 years old in a supervision-relationship with their parent/guardian need a parent's permission to change any of these settings to be less strict. Unsupervised late teens (16-17 years old) can change settings themselves. Since making these changes, 97% of teens aged 13-15 have stayed in these built-in restrictions globally, which we believe offer the most age-appropriate experience for younger teens.[22]

Adopting an approach that is grounded in the global "best interests of the child" standard helps us build products for young people that support their well-being and rights while promoting consistency across different jurisdictions and product teams. We find that adopting a principles-based approach helps to promote consistency across jurisdictions and products, which is necessary to enable effective and scalable technology-driven solutions to protect young people online.

Important considerations for a balanced approach in the COPC

As the COPC is developed, we encourage the OAIC to take a holistic view of the role of data in protecting children and their rights. It is important that – as part of protecting young people's privacy and agency online – the COPC adopts a balanced approach and recognises that there are benefits as well as risks from the sharing and use of data online. There are multiple interaction points by young people and technology and it is important that the COPC takes an enabling role with respect to some of the

[21] Meta, 'Expanding Teen Account Protections and Child Safety Features', *Newsroom*, 23 July 2025, https://about.fb.com/news/2025/07/expanding-teen-account-protections-child-safety-features

[22] Meta, 'We're Introducing New Built-In Restrictions for Instagram Teen Accounts, and Expanding to Facebook and Messenger', *Newsroom*, 8 April 2025 https://about.fb.com/news/2025/04/introducing-new-built-in-restrictions-instagram-teen-accounts-expanding-facebook-messenger

productive and beneficial ways that data can provide safe and appropriate experiences online.

Additionally, as part of protecting and empowering young people online, we encourage the OAIC to recognise the importance of a ‘whole-of-ecosystem’ approach to online safety and privacy and its role in data minimisation and protecting children’s privacy. We also encourage consideration of the role of parents and guardians to guide young people through safe and empowered online experiences.

Providing safe and age appropriate experiences

At Meta, we invest in providing useful, relevant and age-appropriate experiences online. We have our Community Standards[23] that outline the content that can and cannot be shared on our services, our Recommendation Guidelines[24] that outline the content that we will and will not recommend to people, and we invest in our content governance and integrity systems to enforce these policies, with additional protections for teens.

These additional protections supplement those outlined above such as Teen Accounts. One part of these is age gating certain types of content that may otherwise be allowed on our services, but are not appropriate for young people. Recognising that some content may be appropriate for adults but too mature for teens under 18, we have worked with experts and conducted research across countries to understand what types of content are inappropriate for teens to see, and we hide this content from them.[25] For example, we hide most graphic and disturbing imagery from teens - such as a photo of a severely burned person - even if we would allow it behind a warning screen for adults.

As part of providing a personalised service, we can also help detect unusual behavior or signals that a child may be exposed to unsafe or unwanted interactions, enabling platforms to trigger protective actions like sharing a safety message or blocking harmful content. For instance:

- We show Safety Notices to remind people to be cautious in private messages and to block and report anything that makes them uncomfortable. In June alone, teens have blocked accounts 1 million times and reported another 1 million after seeing a Safety Notice on Instagram.[26]

[23] Meta, ‘Community Standards’, *Transparency Centre*, https://transparency.meta.com/en-gb/policies/community-standards

[24] See Facebook, ‘About recommendations on Facebook’, *Facebook Help Centre*, https://www.facebook.com/help/1257205004624246; Instagram, ‘Recommendations on Instagram’, *Instagram Help Centre*, https://help.instagram.com/313829416281232

[25] Meta, ‘Helping Teens See Age-Appropriate Content’, *Transparency Centre*, https://transparency.meta.com/policies/age-appropriate-content

[26] Meta, ‘ Expanding Teen Account Protections and Child Safety Features’, *Newsroom*, 23 July 2025, https://about.fb.com/news/2025/07/expanding-teen-account-protections-child-safety-features

- We show Location Notices to let people know when they are chatting with someone who may be in a different country, which is designed to help protect people from potential sextortion scammers who often misrepresent where they live. In June, teens and young adults saw our Location Notice on Instagram 1 million times, with 1 in 10 tapping on the notice to learn more about the steps they could take.[27]

And finally, the nature of many online services – including those provided by Meta – are personalised to provide appropriate, relevant and useful information to young people. Subject to our Community Standards and Recommendation Guidelines, this can include analysing and adapting content recommendations to fit a child's age and maturity level.

To achieve all of this, we employ a range of signals to assess users' ages, including self-declared age information, behavioral patterns, and device and account data. These signals collectively enable us to tailor content, features, and privacy settings that align with the developmental needs and protections for children.

Importantly, age assurance is typically not a one-time event but an ongoing process, as children grow and their online interactions evolve. Continuous age assurance and adaptive measures ensure that protections remain effective over time, addressing challenges such as account sharing, changes in user behavior, and emerging risks. This dynamic approach supports a safer digital environment that respects children's rights while enabling them to benefit from age-appropriate online experiences.

For example, to develop our adult classifier,[28] we first train an AI model on signals such as profile information, like when a person's account was created and interactions with other profiles and content. From those signals, the model learns to make calculations about whether someone is an adult or a teen.

To evaluate the performance of the model, we develop an "evaluation dataset." That dataset is created by having teams manually review certain data points that we believe to be strong signals of age, such as birthday posts. Identifying details are removed before these posts are shared with the team to make a determination about the age of the person who posted it. Once the team has made that determination, they label the data with a note indicating whether the post was made by an adult or a teen. These labeled data points then make up our evaluation dataset.

We then evaluate our classifier on a country-by-country basis. Before applying the classifier to a new country, we look at its performance across several criteria, including overall accuracy and accuracy across different groups of people. For example, since we

[27] Meta, ' Expanding Teen Account Protections and Child Safety Features', *Newsroom*, 23 July 2025, 'https://about.fb.com/news/2025/07/expanding-teen-account-protections-child-safety-features

[28] Meta, 'How Meta uses AI to better understand people's ages on our platforms', Tech at Meta, 22 June 2022, https://tech.facebook.com/artificial-intelligence/2022/6/adult-classifier

use interactions with content as a signal, we look at how our model performs for people who have not been on our platform for very long. But the work is not done once the classifier is up and running. To check that our determinations are up-to-date, we regularly rerun the classifier to include the latest information.

As the OAIC develops relevant obligations for the COPC, we encourage the OAIC to harmonise with international standards, including those that permit personalisation if a company has reasonable measures in place to protect the child from any harmful effects, which takes into account the balance of factors relevant to personalisation, including the benefits to young people. This could then be supported by regulatory guidance on how to identify harmful effects in practice.

The COPC should recognise that consent is often not an appropriate legal basis

It is of the utmost importance that young people understand when their personal information is being collected and how it is used, as well as their options to control and delete their personal information. This is why we have a layered approach to our Privacy Policy using simple language aimed for 11-13 year olds (determined by a Flesch-Kincaid reading score), and we provide privacy settings and controls that are easy to use and have educational resources such as our Privacy Centre. That said, it can be challenging and inappropriate in many instances for the legal concept of 'consent' to be the primary or only legal basis for data collection and processing.

Firstly, from a user perspective, an over-reliance on consent could lead to "consent fatigue" - where individuals become overwhelmed by frequent consent requests and may no longer engage meaningfully with them - resulting in user frustration and disengagement.

Secondly, from a safety and integrity perspective, online service providers need to collect and use personal information in order to provide a safe and age appropriate service and in these circumstances it is not workable to seek consent, which is also withdrawable.

The limitations of consent as a primary legal basis for processing personal information has been recognised in other jurisdictions. For example, the General Data Protection Regulation (**GDPR**) in the European Union (**EU**) (and associated youth guidance, i.e., the UK's AADC and Irish Fundamentals) permits multiple legal bases for data processing other than consent, and each basis is equally valid, including 'contractual necessity' and 'legitimate interests'. It is up to services to decide which lawful basis for processing is most appropriate to the processing.

We encourage the OAIC to give consideration to the practical challenges that overly broad consent requirements can create, particularly if they may inadvertently compromise essential data processing such as the provision of safety and integrity measures or providing age-appropriate experiences for younger users.

Age assurance and data minimisation

We encourage the COPC to be developed recognising the different roles that different providers have in the ecosystem, and the differing regulatory frameworks that are being developed.

Understanding a user's real age is key to all of the efforts by policymakers and online services to promote a more age appropriate experience online. We are seeing the introduction of age assurance obligations under multiple regulatory regimes in Australia (as well as overseas) which is leading to an increasingly fragmented and potentially overlapping approach to the collection and use of personal information by a growing range of services. For example, the *Online Safety Amendment (Social Media Minimum Age) Act 2024* imposes age assurance obligations on in-scope social media services. At the time of writing, the eSafety Commissioner has accepted for registration three Phase 2 Codes developed under the *Online Safety Act 2021*, which include age assurance requirements for internet search engines[29], and is considering proposed age assurance measures at other levels of the technology stack. This is in addition to the development of the COPC.

Age assurance obligations are therefore being developed under multiple regulatory regimes without a holistic view of how they interact, or a practical view of how children and parents use online services or how industry conducts age assurance, potentially leading to increased data collection, and safety and security risks.

To minimise the collection and processing of children's data for age assurance purposes, we support the leveraging of existing data collection points - and information that is already being collected today - at the app store and OS provider levels, to implement a privacy-preserving approach to age assurance.

This is a 'whole-of-ecosystem' approach that prioritises data privacy and security, as it means that parents and teens would not have to give their government IDs or other personally identifiable information to each and every app or service out there to verify their age or their child's age. Under this approach - which has gained traction in other jurisdictions - app store and OS providers would share age bands APIs with app providers and websites.

Teens and parents already provide companies like Apple and Google with this information and these companies have already built systems for parental notification, review, and approval into their app stores. Meta's investment in User Age Group APIs in the Meta Quest Store, which are designed to help developers understand how old their users are, is an example of how this can be achieved in a privacy-preserving way. When someone launches an app on the Meta Quest platform, these APIs allow Meta

[29] Internet Search Engine Services Online Safety Code (Class 1C and Class 2 Material) https://onlinesafety.org.au/wp-content/uploads/2025/07/Schedule-3-Internet-Search-Engine-Services-Online-Safety-Code-Class-1C-and-Class-2-Material.pdf

to share whether the app is used by a preteen, teen or adult account. The app is then able to use this information to tailor a more age-appropriate experience and to properly protect young people's data.[30]

We do not recommend this approach in order to divest Meta of our responsibility to ensure safe and age appropriate experiences for teens on our services. Rather, it recognises the practical reality of how young people use apps and services - for example, the average teenager uses dozens of applications on their phone, all with different and constantly changing standards and features - and the broader regulatory context relating to age assurance. App store/OS level age verification is the most efficient, consistent and sustainable solution. Meta will continue to do our part by continuing to act responsibly and build and invest in new tools to ensure children have age appropriate online experiences.

We support an industry-wide solution where all apps are held to the same, consistent standard which provides the necessary consistency to most effectively protect young people. The alternative - which is the current trajectory - is a fragmented and siloed app-by-app, service provider-by-service provider approach, which increases the opportunity for identity theft or other misuse of identity data. This is contrary to both data privacy and security; we should minimise the number of times and places where parents and teens should have to prove their age.

The role of parents and guardians

Another benefit of age assurance at the app store and OS levels is that it provides parents with oversight and control of their children's downloads and online activities - including the personal information their children provide.

Parents play a pivotal role in supporting the development of their children and determining what is best for them. Article 5 of the UNCRC emphasises the need to respect the responsibilities, rights and duties of parents, extended family members or legal guardians to provide the appropriate direction and guidance in the exercise by the child of the rights recognised in the UNCRC. It is therefore essential that the COPC fully accounts for the role of parents who are primarily responsible for empowering and supporting their children.

The app store/OS level age assurance approach leverages not only existing data collection points and data collection, but also the 'golden moment' when a parent or guardian gives their child a device - at that moment, parents are well placed to verify their child's age when setting up their phone and app stores can then apply that age to any apps young people want to download. This solution makes it easy on parents; gives parents control; and does so in a privacy-protective way.

[30] Meta, Introducing Age Group Self-Certification & Get Age Category API for All Developers, 23 July 2024, https://developers.meta.com/horizon/blog/age-group-self-certification-apis-meta-quest-developers

Detailed comments

Against the backdrop of these important considerations to inform a balanced approach in the COPC, we make the following comments on some key issues in response to the Issues Paper.

Scope of services

Given young people use a wide range of online services, the COPC should apply to all entities regulated by the Privacy Act that are likely to be accessed by children. This is consistent with equivalent codes in the UK and Ireland, and allows the COPC to support broader data minimisation solutions as part of an app store/OS 'whole-of-ecosystem' approach to age assurance (discussed above).

When and how the COPC should apply to organisations subject to the Australian Privacy Principles (APPs)

Meta supports taking an approach consistent with the UK AADC when considering what factors should be taken into account to determine whether a service is considered likely to be accessed by children. In addition to this approach taking into account factors such as the nature and content of the service, and the way in which the service is accessed and any measures put in place to prevent children gaining access, taking this approach would provide consistency for service offerings available both in UK and Australia (and other countries that take a similar approach in the future).

Approaches taken by services to age-gate or prevent access by children should be proportionate to the risk faced by children on those particular services. This should also be balanced with data minimisation principles - entities should not be encouraged or required to collect additional data unless for age-gating or verification purposes if it is not proportional to the risk to children on those particular services.

Age range specific guidance

Meta recognises the importance of age-appropriate experiences for children that are adapted to their developmental needs. This is reflected through our product offerings like Teen Accounts on Instagram. For example, teens under the age of 18 will be automatically placed into Teen Accounts, and teens under 16 (as well as teens aged between 16-17 years old in a supervised experience) will need a parent's permission to change these built-in protections to be less strict.

All teens will be automatically placed into defaults, for example, a private account, messaging restrictions, a strict setting of our Sensitive Content Control, a daily limit reminder after 60 minutes of use, and no notifications from 10pm to 7am. If an early teen (13-15) wishes to change to a less protective setting, they will need to set up a supervision relationship with their parent/guardian and seek parental permission to make that change. Supervised late teens also require parental permission to change to less restrictive settings.

Setting up parental supervision provides parents with numerous insights into their teen's online activity to help them support their teen (for example, the ability to see who their teen follows and who follows their teen and with whom their teen has been recently messaging) and enables the parent to set a daily time limit on the app that logs the teen out and to turn the app off altogether at night via sleep mode. Unsupervised late teens (aged 16-17) will be placed into the same defaults, but will not require parental permission to change the default settings, recognising the evolving capacity and autonomy of teens as they grow older.

The reason we designed these age bands and differences in the parental supervision tools into Teen Accounts is because our research[31] showed that younger and older teens should have different online experiences based on their maturity and stage of development because the path to digital independence is not linear. There are many different family realities where teens are in a state of flux and parent rules change over time. Settings and tools should provide flexible solutions for parents and teens in any stage of development, with later teens graduating toward greater forms of self-supervision. In general, our research showed that younger teens benefit from guidance and supervision to stay safe online and older teens seek more autonomy and self-expression, but still benefit from support and guidance.

Providing different age-related experiences is also reflected in our age-based restrictions on advertising categories and harmful content. We restrict certain advertising topics for teens in Australia. Ads related to sensitive subjects such as alcohol, financial products, and weight loss products and services are prohibited from being shown to people under 18. Teens can also manage the types of ads they see on Facebook and Instagram with Ad Topic Controls.[32]

We support the OAIC providing age-based guidance and suggest that the OAIC consider adopting the approach taken by the UK in the AADC, including the importance of ensuring the autonomy and independence for older teens in making privacy-related decisions, acknowledging that they are more capable of making informed choices about their online presence.

[31] Meta, 'How research and consultation informed Instagram Teen Accounts: a new protected experience for teens, guided by parents', Trust, Transparency & Control Labs, 17 September 2024, https://www.ttclabs.net/site/assets/files/12047/how_research_consultation_informed_instagram_teen_accounts.pdf

[32] Facebook, 'Your ad preferences and how you can adjust them on Facebook', *Facebook Help Centre*, https://www.facebook.com/help/247395082112892; Instagram, 'Control which ads show on your Instagram account', *Instagram Help Centre*, https://help.instagram.com/911879456838933

Comments in relation to specific APPs

With respect to the OAIC's questions on specific APPs, we relevantly note:

- **APP 1 - Transparency:** Meta understands the importance and challenge of making privacy policies and other key information accessible and understandable to users of all ages and abilities. In order to address this challenge, Meta has taken steps to make our Privacy Policy easier to understand through clear language, taking a layered-approach and providing examples. This approach lowered the comprehension level of the Meta Privacy Policy from college-age to 9th grade on the Flesch-Kincaid scale. In addition, we introduced Privacy Centre as a place where people can learn more about Meta's approach to privacy across our apps and technologies.

  As mentioned above, our Privacy Centre also provides teen-specific access support and resources, enabling them to learn more about our safeguards, additional resources, and to review their settings.[33]

  We acknowledge that providing transparency and accessibility needs to be an ongoing journey. Whilst we consider that our existing, holistic approach to transparency is sufficient, we would welcome guidance on best-practice evidence-based approaches to ensuring important information is communicated to users of all ages and abilities.

- **APP 2 - Anonymity and pseudonymity:** Without commenting on the merit of whether anonymity and pseudonymity are appropriate in any or all circumstances for children, Meta notes that providing high-fidelity age-assurance or verification may not be practical in the context of maintaining anonymity or pseudonymity with respect to a platform or service providers' knowledge of the user (i.e. as opposed to other users on the platform).

- **APP 3 - Collection of personal information:** The criteria for determining what is "reasonably necessary" should be proportional to both the age and relative capacity of the child (i.e. different ages having different levels of development and therefore capacity) and what is necessary for the provision of the service.

  An important qualification is that there are many instances in which it is not appropriate to rely on the consent of an individual for personal information processing, regardless of the individual's age. For example, where data processing is necessary for the integrity of a platform or service or for the safety and security of other users. This is acknowledged in the UK AADC and EU GDPR which have multiple, non-heirarchical legal bases available for the processing of personal information in addition to consent.

[33] Meta, 'Access support and resources for teens', *Privacy Centre*, https://www.facebook.com/privacy/guide/teens

- **APP 5 - Notification:** We refer to our comments on APP 1 with respect to the challenge of making information clear, understandable and comprehensive. In addition to welcoming further guidance in this area, we recommend caution in guidance that would require or encourage the collection of sensitive information, including information about disabilities. Rather than requiring services to be responsive to the ages and abilities of specific individuals (potentially requiring collection of sensitive personal information), guidance that points to standards, principles, style guides and examples that services can rely on when creating transparency materials for users of various ages and abilities would be more practical and preferred from a data minimisation perspective.

- **APP 6 - Use and disclosure:** Meta recognises the importance of providing clear and understandable transparency for all users, including children. In addition, as explained above, we note that consent is not an appropriate legal basis in many circumstances. Notwithstanding this, in appropriate circumstances we consider that consent can be obtainable from children depending on their relative age and capacity when the transparency associated with the consent is understandable by them. However, for some ages there should be the ability for parents to be in-the-loop and able to supervise child accounts (we have built controls to enable this). As children grow and develop, the importance of individual agency and autonomy over their online presence increases.

- **APP 12 - Access and parental support:** Meta recommends that OAIC consider the UK AADC approach to parental controls and access to children's personal information. That includes taking a considered approach balancing the relative age of different children, the rights of parents, and the rights of children to autonomy and self-determination.