

Privacy Vaults Online d/b/a PRIVO
17949 Main St., #1025
Dumfries, VA 22026-1025
www.privo.com
July 30th, 2025
VIA ELECTRONIC SUBMISSION: copc@oaic.gov.au

Re: PRIVO Comments:

Privacy Vaults Online, Inc. d/b/a/ PRIVO, an FTC approved Safe Harbor provider under the Children's Online Privacy Protection Act ("COPPA") submits its Comments in response to the OAIC Children's Online Privacy Code (consultation for industry, civil society, academia and other interested stakeholders). PRIVO is a leading authority in children's online privacy, age assurance and consent management. We support organizations and companies to navigate the online privacy landscape including COPPA, GDPR and existing Children Codes. PRIVO's cloud-based solutions include age assurance and parental consent, enabling online services to seamlessly engage with or block access to minors. PRIVO has been an FTC-approved COPPA Safe Harbor since 2004. <https://www.privo.com/>.

We welcome this opportunity to comment on such an important topic. Codes and standards need to keep pace with the rapidly changing online environment and emerging technologies. Children under 18 are developing an understanding of the world, and social media, games and online experiences are integral to that world. For far too long privacy and safety by design have not been considered by the majority of online services targeted at or likely to attract children resulting in well documented risks and harms to younger children and teens.

PRIVO works with hundreds of online services to support privacy and safety by design and compliance, from leading entertainment brands to small startups, ed tech providers and health care services. We have participated extensively in FTC proceedings addressing COPPA and in Safe Harbor roundtables, lending our extensive experience to help inform the Commission and industry on issues of children's privacy and developments in the marketplace. PRIVO has also been commented on and met with the UK ICO in relation to GDPR and the Children's Code and commented on and discussed the Irish DPC's Fundamentals for Child Oriented Data Processing¹. PRIVO has the first to market GDPRkids™ & Children's Code Privacy Assured Program. We also, via our work with the National Institute of Standards and Technology (NIST), co-authored the Minor's Trust Framework which facilitates ecosystem-wide compliance solutions for those participants adopting its principles for protection of child identity online.

The OAIC raised the question of age ranges and age-based guidance. It is important to take into account that children develop capacity at different ages and developmental stages as they start to recognize and understand content.² From ages 7 to 11 years old, as children enter the concrete operational stage, they can begin to form ideas and consider several attributes of the same property at the same time. They still lack the abstract thinking skills that define certain content as a larger concept but can start to recognize persuasive intent and advertisements with parental guidance³. The UK's Children's Code⁴ notes that children in this age range (6-9) are beginning to engage in online gaming, more often with parental involvement, beginning to experiment on social media and identifying online personalities (vloggers,

¹ [The Fundamentals for a Child-Oriented Approach to Data Processing](#)

² [Piaget's Stages: 4 Stages of Cognitive Development & Theory, Alicia Nortie, Ph.D.](#), May 3, 2021

³ [The CAP Code: Recognizing ads: Children](#)

⁴ [ICO Children's Code: Annex B: Age and developmental stages](#)

streamers, content creators) within their age range. At 12 years of age, as the child enters the formal operations stage⁵ and is capable of hypothetical deductive reasoning (i.e., testing a theory) they can begin to identify an ad and the advertiser's intent to change behavior.

The Children's Code⁶ notes that children ages 10-12 may be engaging with media to explore and develop their own self-identity, increasing their use of social media. Children exploring their identity may be more susceptible to peer pressure and value the opinions of their peers and by extension online influences over authority figures. The Children's Code⁷ also speaks to the developmental differences in teens ages 13-15 and 16-17. Children 13-15 are more independent in their online uses but still may seek to emulate online influencers. Children 16-17 years old may have fully developed their online skills and coping strategies but still lack the emotional and cognitive abilities to recognize potential long-term consequences of their online behavior when compared to an adult.

Knowing the age of your audience allows a service to treat them appropriately. Without guardrails in place for younger vulnerable users the risk of harms is apparent. Whistleblower Frances Haugen spoke in September 2021 at the US Senate hearing calling on "Facebook to disclose internal research on children's mental health"⁸. The hearing revealed that Meta was aware and actively exploiting internal research that suggested that Instagram made "body image worse for teenage girls", implicated social media in an epidemic of mental health amongst teens and linked the use of Instagram to suicidal thoughts⁹. The Wall Street Journal's investigation¹⁰ into the impact of social media on teen mental health showed evidence that when searching for fitness and workout content, the app's algorithms populated the user's feed with photos of how to lose weight, the "ideal" body type and what they should and shouldn't be eating. Haugen accused Facebook of "prioritize[ing] profit over the well-being of children and all users."¹¹

When considering which entities should be covered by the Code PRIVO agrees with those identified to date but suggests AI providers and deployers should be added. The already defined covered entities will implement or deploy AI providers in their services, ensuring privacy and safety by design is built into the AI will support to ensure children and vulnerable users are protected by the provider as well as the deployer. A provider of a designated internet service needs to be accountable. Platforms in the US are not responsible for the content users share, for example social media platforms are not responsible for the content a publisher/user uploads and shares with other users under Section 230 of the Communications Decency Act (CDA)¹². This is a US law that provides legal immunity to online platforms for content created by their users. It shields these platforms from liability for most user-generated content. This has resulted in serious harm to children, allowing for vast revenue to be generated from the content at the cost of vulnerable users not adequately protected by age assurance or verification to date.¹³

Likely to be accessed by a child is a standard that has caused consternation within industry along with the thresholds that need to be met to determine the standard. The threshold should not be based on

⁵ Piaget's Stages of development (n. 5)

⁶ ICO Children's Code (n. 7)

⁷ ICO Children's Code (n. 7)

⁸ [Blackburn & Blumenthal to Hold Hearing With Facebook Whistleblower, Sept 28, 2021](#)

⁹ [Facebook Aware of Instagram's harmful effect on Teenage Girls, Leak Reveals, The Guardian, Sept 14, 2021](#)

¹⁰ [Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show, Wall Street Journal, Sept 14, 2021](#)

¹¹ [Here are 4 key points from the Facebook whistleblower's testimony on Capitol Hill, NPR, October 5, 2021](#)

¹² [Section 230 of the Communications Act](#)

¹³ [It's Time to Update Section 230, Harvard Business News, Aug 12, 2021](#)

numbers but on several factors. Is it more probable that a child might access it than not? If the answer is yes, then include measures to protect the child in the service or prevent them from accessing if the service is not directed to them and content is not appropriate for them. Historically most online services have avoided the need to “know the audience” by relying on weak age gates to screen age, turning a blind eye to child users “gaming” the gate and therefore avoiding the need for appropriate privacy and safety features. The UK Children’s Code provides guidance to online services and entities assessing audiences to determine if it is likely to be accessed¹⁴. The US Children’s Online Privacy Protection Act¹⁵ also provides audience definitions that are helpful in determining the audience age range. The criteria for establishing a mixed audience definition are helpful. It’s also possible to look at the UK Online Safety Act¹⁶ which requires a child access assessment to be conducted.

The OAIC raises the question of age gates. Age gates are a first line of defense only. If the risk of harm is low (determined by a risk or access assessment) then an age gate may be an appropriate measure. Broken age gates, i.e. those that allow a child to back button, delete the app and then download again or simply change their date of birth, are not adequate to prevent a child from bypassing the gate to access content. Therefore, mapping a service’s data processing, features and functionality to risk determines if an age gate is appropriate. There is no silver bullet in age assurance, an age gate could be used as one control amongst others dependent on risk. For example, screening age and then using a form of age assurance (age estimation or verification) may be necessary. Some social media platforms have introduced AI to review content and infer age based on that content. This process raises concerns around profile building and misuse of the data that is collected by the platform, i.e. the use of the data for other secondary purposes. All users could be afforded the same protection until age is known i.e. implement age assurance measures at the point that the online service features and functionally pose a risk (based on a risk assessment).

When an online service targets users of all ages or is likely to attract children then knowing the age of the user or age range is necessary to ensure age-appropriate experiences are provided. If the risk is high to the child based on the risk assessment, then age assurance measures may be required. There should be no need to collect sensitive personal information from a child to verify age. Age verification measures should avoid collecting sensitive data such as biometrics, e.g. facial data points, digital fingerprints and so on and so forth from a child. Often a younger child will need parent consent to access a service, or certain features in which case the adult should be verified not the child. The adults should also be offered a choice of verification methods. A robust federated ID is key to ensuring that the parent only provides their personal data once and not repeatedly to different online services increasing the privacy and security risks to the data. An age-related token should be passed back to the online service by the provider and not the personal information of the user child or adult each time.

The OAIC asks if age-based guidance would be appropriate in tailoring protections and interfaces appropriately and effectively. The answer is yes, not least in relation to transparency principles. Privacy notices, just in time notices and safety features need to be written in a clear and accessible way for users of different age ranges. It is clear that privacy notices and terms are often incomprehensible to adults, not least due to the lengthy nature of some but also due to legalese and industry terms that an end user would not understand. Many of our members provide children’s privacy notices written for children. These explain and define privacy terms and are often written in bite size segments. Disclosures should be in the same format as the content to aid understanding i.e., if a video is delivered the

¹⁴ [ICO Children’s Code – Services Covered by this Code](#)

¹⁵ [Children’s Online Privacy Protection Rule](#)

¹⁶ [UK Online Safety Act 2023](#)

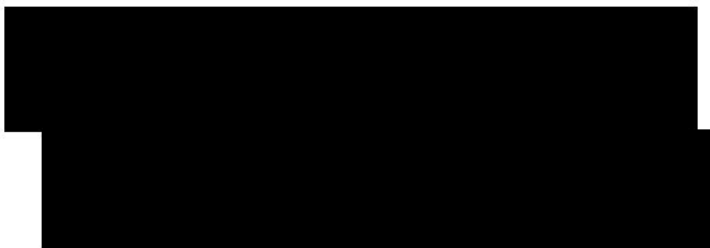
disclosure should be visual and if there is audio it could also be vocalized. It is a requirement of the GDPR¹⁷ and Children's Code¹⁸ for age-appropriate notices.

Mechanisms to action rights should be implemented including easy to access forms that do not request further unnecessary personal data and are not buried in a policy or terms but allow users easy access to the service to action rights. If a child is below the age of digital consent in the relevant jurisdiction or below 16 it may be appropriate to ask for parent contact details or legal guardian. Using a third-party dispute resolution process allows for a fair neutral complaint procedure.

In response to the points raised regarding direct marketing it is important to consider that this term encompasses several forms of marketing and could include targeted personalized interest-based ads which build a profile of the child. Recital 71 to the GDPR states that such automated decisions¹⁹ 'should not concern a child'. The EDPB guidelines on automated individual decision making and profiling states that organisations should, in general, avoid profiling children for marketing purposes, due to their vulnerability and susceptibility to behavioural advertising and the ICO's Children's Code speaks to the risks of profiling in relation to children. However, children do deserve relevance, and contextual and personalized advertising can provide this without profile building. Tailored communication makes for a better all-round experience for users of any age.

PRIVO is pleased to have had the opportunity to comment on these questions and looks forward to the outcome of the consultation.

Respectfully submitted,
PRIVACY VAULTS ONLINE, INC. d/b/a PRIVO
By:

A large black rectangular redaction box covering the signature and name of the representative of Privacy Vaults Online, Inc. d/b/a PRIVO.

¹⁷ Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject

¹⁸ [Age appropriate design: a code of practice for online services](#); 4. Transparency

¹⁹ [GDPR Recital 71: Profiling](#)