Snap Inc.

8 August 2025

Snap Inc. Submission to the Office of the Australian Information Commissioner

Thank you for the opportunity to provide this submission responding to the initial consultation on the Children's Online Privacy Code (the Code). We are pleased to share our early views through this submission and through the OAIC Industry Roundtable that we attended in July 2025. We commend the OAIC for the consultative approach that it has taken, including the release of an Issues Paper, and we welcome the opportunity for continued engagement on this important work and look forward to reviewing a draft Code in 2026.

We welcomed the proposal to develop the Code in our submission to the Government's Privacy Act Review report in 2023, and we strongly support the OAIC's development of the Code. At Snap, we have a longstanding commitment to privacy and data minimisation, and we fully support the objectives of the Australian Government to better protect the privacy and security of Australians, including younger Australians, and their personal data online.

In summary, we recommend that:

- the Code align closely with the UK's Age Appropriate Design Code (AADC) to the extent possible.
- the Code embed a risk-based and proportionate approach to regulation, taking into account the different risk profiles of entities, activities and personal information.
- the Code adopt the same standard as the AADC for "likely to be accessed by children" and recognise that platforms subject to an age-gate should not be considered to be likely to be accessed by children under the minimum age for that age-gate.
- The Code should "deem" a platform to be in compliance with their APP obligations if they implement key, specific data protection or data-minimising measures for children.

Our approach to privacy on Snapchat

Privacy is central to Snapchat's values. When we first created Snapchat, we decided to prioritise privacy-by-design and data minimisation.

- **Privacy-by-design**: We develop our products through rigorous safety and privacy processes, which can slow how quickly we release features, but is the right thing for our community.
- **Data minimisation**: We believe the best way to protect data is to never have it in the first place, which is why we minimise the data we collect.

Most messages sent over Snapchat will be automatically deleted once they've been viewed on the Snapchat mobile or web app or have expired, which sets us apart from other platforms. We're deliberate about not keeping a permanent record of most messages you say or share.

Further, while most other platforms have friend or follower lists that are public by default or provide an option to share friend lists publicly, friend lists or even the number of friends are kept private on Snapchat. Geolocation sharing on Snapchat is also off by default.

We're private by default while also offering extra privacy and safety protections to children including:

- We make it difficult for strangers to find teens on Snapchat by limiting ways for teens to show up in search results, such as if they have several mutual friends or contacts in common, or are existing phone contacts.
- Snapchat sends teens an in-app warning if someone tries to contact them who does not share mutual friends with them or is not in their contacts, or is from a region where the teen's network isn't typically located.
- By default, children under 16 cannot create public profiles, barring them from creating a Public Story. Only users with a declared age of 16 or older can have a Public Profile and Public Story.
- When children post to Snap Map, their profile details are anonymised as an extra precaution.

Alignment with the UK's Age Appropriate Design Code (AADC)

In response to Question 2.2 of the Issues Paper, Snap recommends that the Code align closely with the AADC to the extent possible. As we outlined in our 2023 submission to the Attorney-General's Department consultation on its review of the Privacy Act 1988, the AADC provides a commendable example of proportionate, risk-based international regulation. We consider it to be best practice regulation which has already driven significant changes across online platforms.

The AADC sets a clear objective for online platforms to be designed with the best interests of children in mind while not being overly prescriptive, and is intended to give platforms the flexibility to implement its strong standards in ways which are appropriate for their service model. Importantly, alignment with the AADC will also support greater global harmonisation of international privacy standards, which will provide clarity and consistency for entities, and support more effective compliance and enforcement.

Embedding a risk-based and proportionate approach to regulation

In response to Questions 2.6 and 2.7, we recommend that the Code adopt a risk-based model, providing for flexible and proportionate regulation that takes into account the different risk profiles of entities, activities or information, similar to the approach adopted by the AADC. Consistent with this approach, whether and what expectations will apply under the Code should depend on factors such as how likely an entity's service (or relevant part of the service) will be accessed by children and their age, the level of sensitivity around how a child's information is being held or used, and the kind of information involved.

Not all data processing involving children presents the same level of risk, and it is vital that the Code takes this into account. For example, a platform that is commonly used by children under the age of 10 presents a different risk profile to one that only allows users aged 13+. Age data that is used to ensure that a child is restricted from inappropriate ads or to facilitate parental controls should be treated differently to age data that is collected for another purpose.

Age-gating and "likely to be accessed by children"

We support the Code adopting the same standard as the AADC for "likely to be accessed by children", for the reasons outlined above, in its guidance to assist entities to determine whether a platform is likely to be accessed by children. We also support the Code adopting a flexible approach for determining when the Code applies to platforms, and to accommodate different expectations for different classes of entities, personal information and activities of entities, as already flagged in the Issues Paper.

Specifically in response to Questions 2.3 and 2.4 of the Issues Paper, we support the view that if a service takes reasonable steps to implement an age-gate, that platform should not be considered to be likely to be accessed by children under the minimum age for the age-gate. Further, if a platform implements an age-gate for certain features or parts of the platform, those features or parts should also not be considered to be likely to be accessed by children under the minimum age for the age-gate.

This approach is aligned with the AADC, where the way in which a service is accessed and any measures that are put in place to prevent children gaining access is a relevant factor for determining whether a service is likely to be accessed by children.

Implementing best practice safety measures

In response to Question 2.5 of the Issues Paper, we are of the view that there are effective alternatives to age gating or age verification that can help APP entities meet their obligations under the Code, without unduly limiting children's access to digital services. Specifically, we propose the following approaches:

- **Parental controls and consent:** Offering robust parental controls and consent mechanisms allows parents to manage their children's access to services. This empowers parents to make informed decisions about their children's online activities.
- **Highest privacy settings by default for children:** Ensuring that children benefit from the most protective privacy settings by default (e.g. having geolocation tracking turned

off by default, limiting public profiles for children) aligns with the principle of the best interests of the child and limits data collection and sharing without hindering access.

- **Privacy by design and default**: Offering robust, intuitive parental tools enables parents or guardians to guide and manage their child's experience, which supports a co-regulatory model of child safety and privacy protection.

These approaches balance children's access to key digital services while ensuring child privacy.

Finally, and notwithstanding the need for flexibility, we believe that the Code should "deem" a platform to be in compliance with their APP obligations if they implement key data protection or data-minimising measures for children. The Code could provide best practice guidance or standards including, for instance, the measures set out above. We note that this approach is consistent with the recommendation made by the Australian Government's Productivity Commission in its August 2025 *Harnessing data and digital technology* Interim report for the Government to provide an alternative method for entities to fulfil their privacy obligations by meeting certain compliance criteria, in addition to a more flexible outcomes-based pathway.

Conclusion

We again thank the OAIC for the opportunity to contribute our early views, and we reiterate our strong support for the Code and look forward to continued engagement on its development.