

Snap Inc. Submission to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts

Thank you for the opportunity to provide a submission responding to the statutory review (the Review) into the operation of the *Online Safety Act 2021* (the Act).

Snap strongly supports both the Act and the current review into its operation and effectiveness. We thank Ms Delia Rickard PSM and the Department for providing us with the opportunity to contribute and for preparing a detailed Issues Paper. In our submission, we have responded to many of the discussion questions in the Issues Paper. We also take the opportunity to demonstrate Snap's commitment to the safety of all our users, including Australians.

We hope this submission assists Ms Rickard in conducting the Review, and would be happy to answer any further questions or provide any further information that may assist her team.

Introduction to Snap and Snapchat

As a brief introduction, Snap is a technology company. The company's three core products are Snapchat, a visual messaging app that enhances people's relationships with friends, family, and the world; Lens Studio, an augmented reality (AR) platform that powers AR across Snapchat and other services; and the company's AR glasses, Spectacles. We are proud to say that 422 million people globally now use Snapchat every day to express themselves and learn about the world.

Snapchat is designed very differently to traditional social media platforms: in fact, Snapchat has been designed as the antidote to such platforms. Unlike traditional social media, Snapchat does not apply an algorithm to a feed of unvetted or unmoderated content where unvetted publishers or individuals have an opportunity to broadcast hate, misinformation, or violent content. There is no "rabbit hole" of potentially harmful content.

Rather, Snapchat is at heart a visual messaging application, designed for private communications (either 1:1 or in limited-size groups), with the aim of encouraging users to interact creatively with their real friends, not strangers. The app serves primarily as a personal messaging service for connecting with friends, rather than a means to meet new people or broadcast information to large audiences.

Our approach to safety on Snapchat

Privacy and safety by design is a cornerstone of Snap's approach to designing and launching its products, and is built into Snap's compliance program. Members from Snap's product, policy,

Snap Inc.

legal, and engineering teams are involved in the product development lifecycle of all new Snapchat features, from conception to release.

We work hard to help keep Snapchatters safe, and continue to invest in our teams that respond to safety issues and support local law enforcement agencies. We're proud to have on-the-ground Trust & Safety and Law Enforcement Operations teams in Australia, based in our Sydney office.

Over the years, we've made a wide range of intentional design decisions that have had a powerful positive impact on the safety and privacy of our users, including:

- **Focus on creativity rather than consumption:** The app opens directly into the camera, rather than to a scrolling feed, creating a dynamic and immediate way to share visual experiences with friends and family.
- **Communication between real friends:** We intentionally make it harder to find and talk to strangers on Snapchat. For example there are no public profile photos and no public friend lists. Snapchatters also cannot receive a message from anyone whom they have not accepted as a friend on Snapchat or who is not a contact in their phone book.
- **Private by default for all:** Settings for all Snapchatters, including those under 18, are set to private by default. Contact settings are set to friends and phone contacts only by default, and cannot be expanded to strangers.
- **Location sharing off by default:** If Snapchatters decide to use the location-sharing feature on our Snap Map, they have to "opt in" and can only share their location with people they are already friends with.
- **No Comparison Metrics:** Unlike many platforms, Snapchat eschews public social comparison metrics such as public 'likes' or public friend counts, which may increase social pressure.
- **Algorithmic Design and Content Moderation:** Both of our primary public content platforms where we use algorithms to rank content, Spotlight and Discover, are subject to unique safeguards to limit the reach of potentially harmful content.
 - On Spotlight, our primary broadcast platform for user-generated content, content is moderated before it reaches a large audience.
 - Discover, Snapchat's other large-scale broadcast content platform, is a closed content platform, which only features content from select publishers and creators.

Snap Inc.

- **Reporting tools:** All content on Snapchat must adhere to our [Community Guidelines](#). Snapchat and our support site have reporting mechanisms that make reporting content, accounts and chats for violations of these Guidelines easy. Last year we rolled out in-chat reporting, enabling users to quickly report specific chat messages for human review.
- **Global and local Trust & Safety team:** Our global Trust & Safety team, which includes team members embedded in our Sydney office, works 24/7 to review user reports and take appropriate action.
- **Transparency reports:** We are committed to transparency and openness with what is happening on Snapchat and how we respond to it. Our bi-annual [transparency reports](#) details our response to illegal and harmful content on Snapchat, including a [dedicated Australia-specific breakdown](#) of content reported and enforced for Australia.

While we prioritise creating a safe and positive experience for Snapchatters of all ages, given Snapchat's popularity among teenagers we have dedicated significant time and resources to help ensure that younger people have a safe experience when using the app. For example:

- **Mutual friend requirement:** While we already intentionally make it harder to find others on Snapchat compared to other platforms, it is even harder to find Snapchatters who are not adults. Teen Snapchat users (aged 13-17) are not recommended to another person unless they have multiple mutual friends on the platform, meaning they are likely to know them in real life.
- **Public profiles:** By default, teens cannot create public profiles, barring them from creating a public My Story. Only users with a declared age of 18 or older can have a Public Profile and Public Story. If a user lowers their birthday to an age under 18, we delete their Public Profile and Public Stories.
- **In-app warnings to teens:** We also show warnings to teens if someone with whom they do not share minimum mutual friends tries to chat with them. Teens will now also see a warning message if they receive a chat from someone who has been blocked or reported by others, or is from a region where the teen's network isn't typically located.
- **Family Centre parental tool:** Parents can link their account with their teens using Family Centre where they can see who their teens have been chatting to recently on Snapchat, their teens' friends' list and new friends their teens have added, as well as a complete list of group members for the group chats in which their teens have been active over the last week. It also allows parents to review privacy settings and set content controls that filter out suggestive or sensitive content. Parents can also confidentially report accounts they may have concerns about directly to our Trust & Safety team.

Summary of recommendations

Overview

Snap supports effective online safety regulation based on broad principles that provide clear expectations to industry, while also providing flexibility. This flexibility is vital so that digital platform providers can implement measures that are appropriate and proportionate to their products, taking into account their size, service models and risk levels.

We believe that the OSA has been working well since coming into effect in January 2022. It provides effective, multi-layered regulation, including a principles-based Basic Online Safety Expectations (BOSE) framework that sets clear expectations and has already driven meaningful transparency across the industry. Meanwhile, while the Act's online safety industry code framework is still in development, several codes have already come into effect and are guiding platform responses to online harms.

Snap also supports an effective independent online safety regulator with necessary and appropriate powers to take action to protect Australian end-users. The Australian eSafety Commissioner (the Commissioner) is arguably the world's most respected and expert online safety regulator, and has been backed up by a broad range of content takedown, investigation, information gathering and enforcement powers that are matched by strong penalties for non-compliance.

In response to the questions in the Issues Paper, we have outlined a range of recommendations in support of online safety regulation that is effective but also flexible and proportionate in how they apply to platforms, and encourages innovation rather than being overly complex or prescriptive.

List of recommendations

Snap recommendation (Q1): We support the current objects of the Act and recommend that they be maintained.

Snap recommendation (Q4): We support the BOSE framework and recommend that it continue in its current form.

Snap recommendation (Q5): We recommend the Act be amended to make it explicitly clear that a platform shall only be required to comply with one industry code or standard.

Snap recommendation (Q6): We support amending the Act to require online platforms to have community guidelines and terms of use or service.

Snap Inc.

Snap recommendation (Q7): We recommend that determination of risk should not be based solely on simplistic metrics like the number of users, but take into account design choices including whether a user has been permitted by the platform to:

- openly communicate with users they do not know
- access an open, unmoderated public feed
- post unmoderated content to all users of a platform or to the public
- allow for publicly viewable comments to be made on their posts
- forward or share user-generated content to a mass audience.

Snap recommendation (Q9): We support the complaint schemes and recommend that they continue in their current form.

Snap recommendation (Q16): We recommend that the Commissioner continue to be given the responsibility and resources to undertake its valuable research, educational and awareness raising work, and to partner with industry to achieve our shared goals of supporting end-users.

Snap recommendations (Q21):

- We support a duty of care that is flexible, principles-based and proportionate, with enforcement prioritising rectification and undertakings over penalties.
- We support the best interests of the child principle and believe that it has already been implemented through the BOSE.
- While it is a matter for Government and Parliament as to whether stronger enforcement powers are necessary, we recommend practical consideration of whether existing laws are already sufficient.
- On transparency and data access, we recommend implementing baseline industry transparency requirements and stronger coordination between global regulators rather than burdensome assessment and reporting requirements.

Snap recommendation (Q23-24): We recommend that the Act include a requirement for platforms to provide at least annual transparency reports, including Australia-specific data.

Snap recommendation (Q28): We encourage the Act to continue taking a flexible, principles-based approach to regulation rather than to adopt granular requirements that may not only fall out of date more quickly and but may also discourage innovative safety and privacy measures.

Snap recommendation (Q29): We recommend that the Act remain technology-neutral.

Snap response to the proposed amendments

For the remainder of this submission, we have provided responses to a range of questions set out in the Issues Paper.

Part 2 – Australia’s regulatory approach to online services, systems and processes

1. Are the current objects of the Act to improve and promote online safety for Australians sufficient or should they be expanded?

We support the current objects of the Act, being to improve online safety for Australia and to promote online safety for Australians. These objects are comprehensive, effective and broad, encompassing a wide range of online harms. We are not aware of any specific online safety technologies, emerging practices or harms that would not be covered by these objects.

Snap recommendation: We support the current objects of the Act and recommend that they be maintained.

4. Should the Act have strengthened and enforceable Basic Online Safety Expectations?

We take the BOSE very seriously and believe that they have been highly effective. The BOSE provide a practical and efficient mechanism for the Government to set out its online safety expectations across the online industry, while the Commissioner’s reporting notices have already proved to be an effective tool for improving industry transparency. Since the BOSE are determined by legislative instrument, they are by design able to be updated and strengthened easily as technology evolves (for example, the most recent updates to the BOSE to respond to recent advancements in generative AI technology). There are significant financial penalties for failure to comply with the reporting notices, while the Commissioner’s powers to issue provider notifications have a powerful reputational effect. We are of the view that the current form of the BOSE strike an adequate balance between regulatory “bite” and the need for flexibility in response to the rapid pace of technological advancements.

Snap recommendation: We support the BOSE framework and recommend that it continue in its current form.

5. Should the Act provide greater flexibility around industry codes, including who can draft codes and the harms that can be addressed? How can the codes drafting process be improved?

We are supporters of the online safety industry codes and contributed, through the working groups established by the industry associations drafting the codes, to the development of the social media services industry code that Snapchat falls under.

While the codes that have been registered have only been in place for less than a year, we believe that they are working well. One recommendation that we make is that the Act should make it explicitly clear that a platform should only be required to comply with one industry code or standard, which we understand to be the intention of the Act and the way that the Commissioner intends to enforce them. For example, a social media service should only be required to comply with the code covering social media services and not the code or standard for any other section. Given that some platforms may potentially fall within the definitions of more than one section of the online industry, this change will help to remove the risk of regulatory uncertainty and overlap. The Commissioner's office has provided us with multiple assurances on this point, but we think it would be helpful for this to be codified in legislation, if the Act is amended.

Snap recommendation: We recommend the Act be amended to make it explicitly clear that a platform shall only be required to comply with one industry code or standard.

6. To what extent should online safety be managed through a service provider's terms of use?

Snap strongly supports terms of use. All content on Snapchat must adhere to our [Community Guidelines and Terms of Service](#), which provide strict rules about what can be posted or amplified on Snapchat. These apply to all content and user behaviour on Snapchat and we take strong measures to ensure that they are effectively and consistently applied and enforced.

Snap recommendation: We support amending the Act to require online platforms to have community guidelines and terms of use or service.

7. Should regulatory obligations depend on a service provider's risk or reach?

We recognise that in some overseas jurisdictions, certain regulatory obligations may depend on a digital platform's metrics including size and reach. We also note that some of the existing online safety industry codes that have been registered, including the social media services code that Snapchat falls under, have adopted a risk-based tiering system for determining the obligations that apply to platforms.

While we do not disagree with the principle of basing at least some regulatory obligations for platforms on whether certain risk elements have been met, we believe that 'risk' should be measured in a comprehensive and holistic way to gauge a platform's genuine risk level rather than relying solely on more simplistic measures such as 'reach'.

For example, while Snapchat may share a similar reach to other large platforms that offer a public content feed, the design of the public content areas of our app, Spotlight and Discover,

Snap Inc.

has been designed very differently to other platforms. Unlike traditional social media, as we have mentioned, Snapchat does not apply an algorithm to a feed of unvetted or unmoderated content and there is no “rabbit hole” of potentially harmful content.

Similarly, while Snapchat and other messaging apps (as well as SMS and email) allow users to text each other, unlike many other apps we have taken the step of only allowing messaging between users who are already friends on Snapchat or who are existing phone contacts. Also unlike some other platforms, we do not have publicly viewable friends lists, and our users can easily report content and accounts through our app.

We believe that platforms’ design choices should be taken into account in any consideration of a platform’s level of risk, and have provided some suggestions below on how to achieve this.

Snap recommendation: We recommend that determination of risk should not be based solely on simplistic metrics like the number of users, but take into account design choices including whether a user has been permitted by the platform to:

- openly communicate with users they do not know
- access an open, unmoderated public feed
- post unmoderated content to all users of a platform or to the public
- allow for publicly viewable comments to be made on their posts
- forward or share user-generated content to a mass audience.

Part 3 – Protecting those who have experienced or encountered online harms

9. Are the complaints schemes accessible, easy to understand and effective for complainants?

We support the existing complaints schemes under the Act and believe that they have been working well. These reporting schemes provide tangible support for people who are struggling with harmful content online. We have a strong and positive relationship with the Commissioner and any complaints that they receive related to Snapchat are prioritised.

It is appropriate and beneficial that digital platforms are the first avenue for users to seek the removal of content. It is also appropriate for platforms to have the primary responsibility for upholding the safety and wellbeing of their users. On Snapchat, our users can quickly and easily report content through our in-app reporting tool as well as our support website. As discussed, we release transparency reports twice a year, including Australia-specific data, on our response to illegal and harmful content.

We also note that it is common practice for the Commissioner to pass on complaints to platforms informally, rather than through formal content removal notices, as it will generally lead to faster outcomes for end-users.

Snap recommendation: We support the complaint schemes and recommend that they continue in their current form.

16. What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?

In addition to its regulatory functions, we strongly support the crucial research, educational and awareness-raising work of the Commissioner.

We thoroughly assess all relevant research published by the Commissioner, and the information that it provides to industry, to inform our own response to harmful content and activity. The Commissioner's education resources, including material on its website such as its eSafety Guide for popular services including Snapchat, also provide crucial public resources. The Commissioner should continue to be given the responsibility and resources to continue this invaluable work.

Looking forward, we believe that awareness raising with parents and teachers around the apps that their teens use, ways to talk to teens about staying safe online, and how to use parental tools such as Snapchat's Family Centre will be particularly crucial. There are opportunities for us and the industry to partner with the Commissioner around these important goals and we look forward to exploring this work.

Snap recommendation: We recommend that the Commissioner continue to be given the responsibility and resources to undertake its valuable research, educational and awareness raising work, and to partner with industry to achieve our shared goals of supporting end-users.

Part 4 – Penalties, and investigation and information gathering powers

18. Are Australia's penalties adequate and if not, what forms should they take?

While it is a matter for the Government and Parliament to determine the appropriate penalties in the Act, Snap takes compliance with all requirements of the Act very seriously.

Part 5 – International approaches to address online harms

21. Should the Act incorporate any of the international approaches identified above? If so, what should this look like?

As we've set out, Snap is supportive of principles-based regulation that provides clear expectations to industry while also ensuring flexibility. As such, we would support the

introduction of a flexible and outcomes-focussed duty of care on industry to take responsibility for the safety of their users, as we have seen in the UK Online Safety Act.

Importantly, an effective duty of care should not impose a single “one-size-fits-all” standard, but instead recognise that there will be significant differences between platforms in terms of size, core design, user demographic, service model, resources and overall level of risk - all of which will be relevant to whether a platform has satisfied its duty of care. For example, while the UK Online Safety Act imposes a duty on regulated user-to-user service providers to take proportionate measures to prevent individuals from encountering priority illegal content through the service, it gives service providers the discretion to determine how to discharge these duties based on their service’s unique size and capacity and the levels of risk posed by the platform.

As opposed to a ruled-based approach focused on specific pieces of content, a systems-based duty of care approach also provides flexibility for service providers to keep pace with technological and online behavioural developments on social media. Similarly, a duty of care should be sufficiently flexible to enable platforms to implement diverse and innovative measures, recognising that not all measures will be appropriate, proportionate or possible for all platforms. While platforms should rightly provide transparency on their compliance with the duty, this should not be dependent on burdensome compliance reporting requirements. As a flexible principle, the duty of care is most effective as a tool for guiding platforms towards ensuring they have the right systems and processes, and enforcement should prioritise platforms committing to rectification and undertakings rather than proceeding straight to penalties.

Finally, as noted in the Issues Paper, the duties under the UK Online Safety Act do not create a private right of claim for end-users. We would encourage any Australian duty of care to take a similar approach, recognising that the Commissioner is best placed to pursue corrective action, including in response to reports from the public, and to mitigate the risk of frivolous claims.

We support the adoption of a best interests of the child principle, as exemplified in the UK and California Age Appropriate Design Codes (AADCs). We note this principle has already been implemented through a recent addition in the BOSE requiring providers to “take reasonable steps to ensure that the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children”, which we welcome. We also note that the Australian Government has committed to develop its own version of the AADC in its response to the Review of the Privacy Act.

On enforcement powers, while it is a matter for Government and Parliament as to whether stronger powers are required, we recommend practical consideration of whether existing laws are already sufficient. In relation to the example given in the Issues Paper of powers to seek service restriction or access restriction orders in the UK Online Safety Act, we note that the Act already provides the Commissioner with similar significant powers, including for hosting services

Snap Inc.

to cease hosting certain material, for ISPs to cease providing a link to certain material, and for app distribution services to cease enabling end-users to download an app.

On transparency and data access, we are strong supporters of industry transparency but caution against burdensome risk assessments and compliance reporting. The Commissioner's powers to issue BOSE reporting notices, in addition to other investigative and information-gathering powers provided to the Commissioner under OSA, already provide powerful tools to obtain and access information from industry. There is a risk that the increasing burden of multiple, comprehensive assessment and reporting requirements in Australia and around the world may impact on frontline and safety-focused teams.

Instead, we support an expectation of regular transparency reporting by industry. For example, as we have mentioned, Snap publishes bi-annual transparency reports detailing our response to illegal and harmful content on Snapchat, and is currently one of, if not the only major platform to provide country-specific information including in Australia about reports received and our responses to these. We also support stronger coordination between global regulators, including through the Global Online Safety Regulators Network, to align respective compliance and reporting requirements.

Snap recommendations:

- We support a duty of care that is flexible, principles-based and proportionate, with enforcement prioritising rectification and undertakings over penalties.
- We support the best interests of the child principle and believe that it has already been implemented through the BOSE.
- While it is a matter for Government and Parliament as to whether stronger enforcement powers are necessary, we recommend practical consideration of whether existing laws are already sufficient.
- On transparency and data access, we recommend implementing baseline industry transparency requirements and stronger coordination between global regulators rather than burdensome assessment and reporting requirements.

23. Is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?

24. Should there be a mechanism in place to provide researchers and eSafety with access to data? Are there other things they should be allowed access to?

As we have mentioned above, we are committed to transparency and openness with what is happening on Snapchat and how we respond to it. Our bi-annual transparency reports detail our response to illegal and harmful content on Snapchat, including a dedicated Australia-specific breakdown of content reported and enforced for Australia.

Through the Commissioner's powers to issue BOSE reporting notices and its other information gathering powers under the Act, we believe the Government already has the necessary tools to drive transparency within industry. This could be further strengthened through an additional requirement for platform providers to publish at least annual transparency reports. In our submission to the Department's consultation on the most recent BOSE amendments, we supported the inclusion of a new additional expectation for annual transparency reports.

On the question of access to data, we believe that the most effective way to ensure researchers, governments, other third parties and the community have fair, equitable and open access to data is also through a requirement for platforms to release transparency reports.

Snap recommendation: We recommend that the Act include a requirement for platforms to provide at least annual transparency reports, including Australia-specific data.

25. To what extent do industry's current dispute resolution processes support Australians to have a safe online experience? Is an alternative dispute resolution mechanism such as an Ombuds scheme required? If so, how should the roles of the Ombuds and Commissioner interact?

While these are matters for the Government to consider, we currently provide all of our users, including Australians, with the ability to appeal decisions that we have taken to remove or restrict content that they have posted or distributed in certain parts of Snapchat in response to violations of our Community Guidelines. Accounts locked by our safety team for violations of our Community Guidelines can also be appealed. In both cases, we will always email the user to let them know the outcome of their appeal.

Part 6 – Regulating the online environment, technology and environmental changes

27. Should the Commissioner have powers to act against content targeting groups as well as individuals? What type of content would be regulated and how would this interact with the adult cyber-abuse and cyberbullying schemes?

While these are matters for the Government and Parliament to consider, under our Community Guidelines, hate speech or content that demeans, defames, or promotes discrimination or violence on the basis of race, colour, caste, ethnicity, national origin, religion, sexual orientation, gender, gender identity, disability, or veteran status, immigration status, socio-economic status, age, weight or pregnancy status is already prohibited.

Our in-app reporting tool allows users to directly report hateful content or activities that support terrorism or violent extremism. On our public content platforms, we take a proactive approach to moderating any content that may violate these rules. In the [most recent monitoring round](#) of the EU Code of Conduct on countering illegal hate speech online, which involved 36 organisations

from 21 Member States sending notifications to Code participants during the period 28 March to 13 May 2022, Snapchat did not receive any notifications for hate speech.

28. What considerations are important in balancing innovation, privacy, security, and safety?

In our view, innovation, privacy, security and safety often go hand-in-hand. Safety by Design means putting user safety and user security at the heart of the design and development of our products and features, while privacy by design means minimising the collection and processing of user data. These goals can be achieved without sacrificing innovation - and in fact innovation can be key drivers of privacy and safety by design.

There are also opportunities for the Government to encourage privacy, security, and safety through innovation in the Act. Through the existing BOSE framework and the minimum requirements for industry codes set out in the Act, the Government has been able to set out high level principles-based online safety expectations to industry, while giving flexibility to platforms on the way that these expectations can be achieved. This encourages platforms to invest in innovative solutions to achieve privacy and safety by design in line with these principles, rather than to adopt specific measures that may not necessarily be suitable for them nor allow them to nimbly adapt to evolving technologies and threats.

Snap recommendation: We encourage the Act to continue taking a flexible, principles-based approach to regulation rather than to adopt granular requirements that may not only fall out of date more quickly and but may also discourage innovative safety and privacy measures.

29. Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?

We believe that remaining technology-neutral will enable the Act to flexibly adapt to changes in the online environment, including to new threats as they emerge. A technology-neutral approach will help to prevent the Act from losing relevance or becoming out of date. We also note that the BOSE already provide an efficient mechanism for the Government to address new technologies quickly, as demonstrated by the specific new expectations that have recently been added to the BOSE to address generative AI and recommender systems.

Snap recommendation: We recommend that the Act remain technology-neutral.

30. To what extent is the Act achieving its object of improving and promoting online safety for Australians?

31. What features of the Act are working well, or should be expanded?

Snap Inc.

We believe that the Act has been working well. The Act provides for a broad and multilayered set of regulations and powers that, through its coverage of social media services, relevant electronic services and designated internet services in particular, extend to all corners of the online sector in Australia and around the world.

In the two and a half years that the Act has been operating, we believe that it has already had a material positive impact on the online safety of Australia. For example, the BOSE and the online safety industry codes have undoubtedly led to platforms making changes to their product and to further embed Safety by Design into their product and policy development processes.

Conclusion

We again thank the Department for the opportunity to provide a response to the Review. We strongly support the Act and the aims of the Review to ensure that it operates effectively. We stand ready to continue to support the Review and look forward to its outcomes.