18 August 2023

Snap Inc. Submission on the Exposure Draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023

Thank you for the opportunity to make a submission on the Exposure Draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023 ("the Bill").

Snap shares the Government's objectives of preventing harmful online misinformation and disinformation. We take these issues very seriously at Snap and have designed a platform which intentionally minimises the spread of fake news or misinformation.

There are elements of the Bill which are to be commended. We support the Bill's focus on the systems and processes which digital platforms have in place to address misinformation and disinformation on their services, rather than on directly regulating individual pieces of content. Such an approach is in keeping with a principles-based approach to online regulation, which is now widely considered as international regulatory best practice. We support the proposed graduated application of enforcement powers of the Australian Communications and Media Authority (ACMA), with the most severe penalties only considered after formal warnings, infringement notices and remedial directions are issued. This is a coherent model which encourages companies facing systemic challenges with misinformation and disinformation to put remedial steps in place. We also welcome the exemption of private messages from the scope of the ACMA's new powers, although we note that the definition of private communication could be expressed more clearly. Our other suggested amendments are largely geared towards ensuring safeguards in the application of the proposed new powers for the ACMA, to enable clear and effective regulation which minimises unnecessary regulatory burden for industry participants, which will enable innovative challenger companies to continue to grow and thrive in Australia.

Summary of key recommendations

- The Government should amend the Bill to broaden its definition of private message to "private communication," including both messages and online content that is only observable to end-users of the service selected by the sender.

- The Government should amend the Bill to include requirements for the ACMA to:

    - have due regard to proportionality when considering the application of its new regulatory powers; and to ensure that powers are applied in a risk-based way.

    - consider existing efforts made by providers of digital platform services to provide transparency information, before exercising its new powers related to information-gathering or code development.

  - consider measures taken by providers of digital platform services to comply with requirements in existing regulatory codes, before requesting the development of new codes for misinformation and disinformation.

- The Department of Infrastructure, Transport, Regional Development, Communications and the Arts should conduct a review of the Australian online regulatory framework, as first recommended by the House of Representatives Select Committee on Social Media and Online Safety in March 2022, with a view to simplifying regulatory arrangements while also ensuring the safety and security of Australian citizens online.

Introduction to Snap and Snapchat

As a brief introduction, Snap Inc. 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. While Snap is still a significantly smaller company than the established tech giants that have dominated online media for the past decade, we are growing, with 397 million people globally now using Snapchat every day, and we reach a community of over 7.5 million Australians.

Snapchat has intentionally been designed very differently to traditional social media. At a high level, we use two principles to help guide our design process: **safety by design**, which is about prioritising the safety of our community, and **privacy by design**, which focuses on data minimisation and protecting user data. Product, Policy, Legal and Engineering colleagues are fully involved in the product and feature development lifecycle, from conception to release.

This up-front focus on safety and privacy by design is reflected in the build of Snapchat. Unlike traditional social media, Snapchat does not offer an open news feed where unvetted publishers or individuals have an opportunity to broadcast hate, misinformation, or violent content, nor do we permit public comments that may amplify harmful behaviour. 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.

Snap's response to misinformation

Our **Community Guidelines** apply to all content on Snapchat; these are publicly available online through our Privacy and Safety Hub, which can be accessed both through the app or through our Snapchat Support website. These Guidelines clearly prohibit "false information that causes harm or is malicious." This includes: "denying the existence of tragic events, unsubstantiated medical claims, undermining the integrity of civic processes, or manipulating content for false or misleading purposes."

The approach we have taken at Snapchat makes the app a highly unattractive environment for spreading such misinformation, and it's well recognised that we have been successful in preventing this kind of activity from publicly surfacing on Snapchat. The key reason for this is due to our focus on safety by design, and the protections we have in place:

- A Snapchat user cannot broadcast unmoderated Snaps or Stories to the whole Snapchat community, and if they share content with just their friends, it cannot be forwarded broadly.

- We do have a publicly viewable side to the app – our Spotlight and Discover platforms for news and entertainment – but content there is substantially curated and moderated, respectively, ensuring harmful or illegal content is not surfaced to large numbers of people. Media partners in Discover must adhere to our Content guidelines, which forbid content that is deceptive or deliberately spreads false information, or is not properly substantiated and fact-checked.

- All user-generated content on Spotlight or Discover is moderated before it can be surfaced to large groups of people. This ensures we can prevent content that violates our guidelines, including around false information, from surfacing there.

- Most content on Snapchat is designed to delete by default: this means that default settings are such that Snaps (visual messages) sent through Chat are no longer viewable in the app shortly after they've been opened, while chat messages and Stories are, by default, only viewable for 24 hours. This further limits how widely content can be shared.

Where harmful content and activity takes place, we have effective systems and processes to act quickly. We provide easy-to-use in-app reporting tools so users can notify us of potential safety issues, and our global Trust & Safety team works 24/7 to review user reports and take appropriate action.

Approach to private communications

We welcome the clarity in the Bill that private messages on a digital platform service should be out of scope of the ACMA's powers. This is a common-sense approach that mirrors our own approach to content moderation and enforcement on Snapchat: when you talk to your friends on the phone, you have a high expectation of privacy, whereas if you are a public broadcaster with the potential to influence the minds and opinions of many, you are subject to different standards and regulatory requirements.

However, in keeping with this approach, we consider that the Bill should adopt a broader definition of "private communications." In our view, ephemeral communications such as private Stories – a feature which enables users to share photos or videos with their friends, rather than publicly, and which is only visible for 24 hours – should clearly be considered as private content.

The Bill currently defines a "private message" as an "instant message sent using a digital platform service from one end-user of the service (the sender) to one or more other end-users of the service (the recipients) where the message is only observable to end-users of the service selected by the sender or any of the recipients." We recommend redefining "private message" as "private communication": "an instant message **or online content** sent using a digital platform service from one end-user of the service (the sender) to one or more other end-users of the service (the recipients) where the message **or content** is only observable to end-users of the service selected by the sender or any of the recipients." This would include content in users' private Stories, a feature which enables users to share photos or videos with their friends, rather

than publicly, and which is only visible for 24 hours. In our view this should clearly be considered as private communication, and should not be subject to regulatory requirements which are intended for content which is made available publicly, or broadcast out to a wide audience.

Snap recommendation: The Government should amend the Bill to broaden its definition of private message to "private communication," including both messages and online content that is only observable to end-users of the service selected by the sender.

The Bill should include safeguards to ensure that new powers are applied in a proportionate and risk-based way

The Bill seeks to establish a range of expansive new powers for the ACMA, relating to information gathering and record keeping; code and standard-making; and enforcement. It is a matter for the Government and Parliament to determine whether these new powers are necessary to manage the threats posed by misinformation and disinformation online. However, it is vitally important that any new powers are exercised in a risk-based and proportionate way that minimises unnecessary bureaucratic and administrative burden on industry participants.

This is important because responding to regulatory requests for information (RFIs), developing and complying with regulatory codes of practice or standards, and providing detailed transparency information requires significant time and resources. Often the teams at technology companies who are drafted into these exercises are colleagues who would otherwise be focused on keeping users safe. In several countries around the world, challenger companies are now working to manage a wide range of RFIs from regulators whose remit, and staffing numbers, have increased significantly in the wake of new legislation focused on issues related to online safety, privacy or competition.

Ultimately, the companies who are best served by overly burdensome and complex regulation are the largest firms, with the largest compliance teams, who can easily deal with the bureaucracy involved, while smaller companies struggle to handle the workload. The Australian Competition and Consumer Commission (ACCC's) 2023 report on social media has highlighted structural problems with this market in Australia. Prescriptive and burdensome regulation risks exacerbating these imbalances by disproportionately harming challenger companies and strengthening the advantages of the largest players.

The words "proportionate" or "proportionality" do not currently feature at all in the Bill, or in the Government's accompanying guidance note or fact sheet. Indeed, Section 18 of the Bill proposes that the ACMA can exercise its new information gathering powers "if it has reason to believe that the provider has information or a document that is relevant to a matter mentioned in subclause (2)" – essentially any information pertaining to misinformation or disinformation on an online service, and measures taken to address this – and if "the ACMA considers that it requires the information" for the performance of its regulatory functions. Essentially, this allows the ACMA to exercise broad powers to solicit extensive RFIs from companies, purely to address its own informational requirements.

Effective online regulators should have due regard to proportionality when considering applying information-gathering powers. In the UK Information Commissioner's Office's (ICO's) Regulatory

Action Policy, for example, the ICO states that it "will have regard to what action is appropriate and proportionate" when considering whether to issue an information notice, considering criteria including the risk of harm to individuals, the utility of a response, and public interest.

Snap recommendation: The Government should amend the Bill to specifically include requirements for the ACMA to have due regard to **proportionality** when considering the application of its new regulatory powers. The Bill should also be amended to ensure that powers are applied in a **risk-based** way: the ACMA should be required to establish a solid basis for any concerns related to misinformation or disinformation on a platform, prior to issuing a RFI. This basis could be informed by credible reports from the public, NGOs, academic institutions, or media outlets.

The ACMA should recognise responsible efforts to provide transparency information when considering application of its powers

Another factor that the ACMA should consider in the application of its new regulatory powers is existing efforts to provide transparency information. For example, Snap publishes bi-annual transparency reports detailing our response to illegal and harmful content on Snapchat. Currently, Snapchat is the only major platform to provide country-specific information about reports received, and our responses to these, in all the countries in which we operate around the world. There is no regulatory mandate for us to provide this breakdown; we have chosen to provide this information because we are committed to providing comprehensive information to the many stakeholders who care deeply about online safety and privacy.

It stands to reason that existing responsible best efforts to provide transparency information by providers of digital platform services should be considered before the ACMA utilises its powers, either to request information from companies or to request that the industry puts in place new mandatory codes of practice.

Snap recommendation: The Bill should be amended to include requirements for the ACMA to explicitly consider existing efforts made by providers of digital platform services to provide transparency information related to misinformation or disinformation, before exercising its powers to seek information from companies or to request the development of industry codes.

Considerations around adding new codes to a crowded regulatory ecosystem

In March 2022, a bipartisan Parliamentary Committee – the House of Representatives Select Committee on Social Media and Online Safety – produced a comprehensive report on social media. In its report, the Committee noted the complexity of the online regulatory environment in Australia, and recommended that the Department of Infrastructure, Transport, Regional Development, Communications and the Arts should conduct a review on the legislative framework and regulation in relation to the digital industry, including to "examine the need and possible models for a single regulatory framework under the Online Safety Act, to simplify regulatory arrangements."

The Department has not yet opted to establish such a review. In its absence, an already-crowded regulatory environment in Australia for online services has become even more

complex. Multiple new codes of practice for separate sections of the online industry have been registered by the eSafety Commissioner as part of the implementation of the Online Safety Act, with standards for separate sections of the industry still to come; another cross-industry exercise to develop a further set of codes under the Act is expected to begin later this year. The Attorney-General's Department has recommended the establishment of a new online code of practice modelled on the UK Age Appropriate Design Code. A further code of practice is mooted for online scams. Under this Bill, the ACMA would have powers to ask industry to develop further codes of practice in relation to misinformation and disinformation if it deems this "necessary or convenient," or to draft its own standards if the codes which are then developed are not considered adequate.

As we have set out above, overly complex regulatory regimes create real issues for challenger companies, who cannot always rely on large compliance, policy and legal teams to help them make sense of the myriad competing obligations, codes and guidance under these various initiatives. Perversely, this can serve to entrench the advantages enjoyed by the largest companies whose deficiencies have inspired much of recent online legislation.

As more regulatory codes continue to be developed and proposed, we recommend that the Government moves to establish a review of the Australian online regulatory framework, as first recommended by the Committee in March 2022. We also consider that there should be a requirement in the Bill for the ACMA to consider measures taken by providers of digital platforms services to comply with existing regulatory requirements, before opting to request the development of new codes for misinformation and disinformation. The Government's aim should be to ensure a clear and consistent regulatory environment for online services, while also enabling effective action against harmful content and activity online.

Snap recommendation: The Bill (Division 4, Section 38) should be amended to include a requirement for the ACMA to consider measures taken by digital platform services to comply with requirements in existing regulatory codes, before requesting the development of new codes for misinformation and disinformation.

The Government should establish a review of the Australian online safety framework as first recommended by the House of Representatives Select Committee on Social Media and Online Safety, with a view to simplifying regulatory arrangements while also ensuring the safety and security of Australian citizens online.

Conclusion

Thank you again for the opportunity to respond to this consultation. Snap shares the Government's objectives of preventing harmful online misinformation and disinformation. With the addition of some targeted amendments, we believe that the Bill can help tackle these threats, while ensuring appropriate safeguards and minimising unnecessary regulatory burden for industry participants.