Ms Julie Inman-Grant
Office of the eSafety Commissioner
By email: submissions@esafety.gov.au; avroadmap@esafety.gov.au

CC: The Hon Paul Fletcher MP, Minister for Communications, Cyber Safety, and the Arts
CC: Bridget Gannon, Assistant Secretary, Digital Platforms and Online Safety, Department of Infrastructure, Transport and Regional Development and Communications
CC: codes@esafety.gov.au

Friday September 10, 2021

Submission to Restricted Access Systems and Age Verification consultation processes

Dear Ms Inman-Grant,

The Digital Industry Group Inc. (DIGI) thanks you for the opportunity to provide our views on a new Restricted Access System (RAS) to limit the exposure of minors to age-inappropriate online material, and the implementation roadmap on age verification (AV Roadmap). While we note these initiatives are the subject of separate consultation processes, both address the extremely important topic of the harm that exposure that certain online materials can have on minors. This is why we have combined our input for both processes into this one submission.

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's members are Apple, eBay, Facebook, Google, Twitter, Yahoo, Redbubble, Linktree, Change.org and Gofundme. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI shares the Office of the eSafety Commissioner's (the Office) commitment to online safety, and the broad objectives behind these two initiatives. Our founding members have made, and continue to make, major, longstanding investments in the safety of their users, with many specific products and initiatives aimed at protecting minors in particular. We have provided a brief, high level overview of some of our members' relevant work at the end of this submission.

We understand that the RAS and AV consultations will further inform the work being done by the Office on the development of other regulatory tools under the *Online Safety Act 2021 (*Cth) (the Act). From our previous discussions in relation to the Codes, we understand that the process for developing the RAS and AV will guide the Office's engagement with stakeholders on the development of industry-wide codes in relation to Class 1 and Class 2 materials (the Codes). We understand that the expectations for the Codes will be released in a forthcoming position paper in September 2021, and that the Codes must be developed by industry associations and registered for eight sections of the online industry by July 2022.

In addition, there is a ministerial determination under the Act outlining Basic Online Safety Expectations (the BOSE) with a consultation deadline of October 15, which is being progressed separately by the Office and the Department of Infrastructure, Transport, Regional Development, & Communications (the

Department). The interaction of the BOSE,and the Codes under the legislation, with the RAS and AV is currently unclear.

Furthermore, the outcome of each of these four workstreams (i.e. the RAS, AV, the Codes and the BOSE), is currently unknown. This gives rise to questions on our part regarding how industry associations can progress the work needed to produce registrable Codes by July 2022 and meaningfully engage with four parallel regulatory projects within the specified time frames, noting the interdependencies between the four workstreams. We ask the Commissioner to consider this and adjust the time frames as needed so as to provide a sufficient opportunity for industry associations to meet both your and the Government's expectations in developing the Codes.

The aim of this submission is to provide our initial thoughts about a range of considerations that we consider to be relevant to the development of this suite of regulatory tools being developed by the Office. We provide feedback in the following areas:

1. The need for the Office to provide more information concerning the scope of these consultation processes;
2. Key policy considerations for both consultation processes, including:
    a. the need for a coordinated, efficient whole-of-government approach that balances safety, privacy and online security; and
    b. the need to take into account public sentiment about solutions to age verification where these require individuals to confirm their identity online;
3. The importance of transparency in the consultation processes for the RAS and AV Roadmap;
4. An overview of the work being done by our members to protect minors from exposure to age inappropriate online content.

DIGI looks forward to further engaging with the Office's consultation process for the RAS, the AV and the Codes in the coming months.

Should you have any questions about the representations made in this submission, please do not hesitate to contact me or DIGI's Director of Regulatory Affairs, Policy & Research Dr Jenny Duxbury.

Best regards,

Sunita Bose
Managing Director, DIGI

Recommendations in this section

1. We ask the Commissioner to adjust the development timeframes for the Codes as necessary so as to enable an environment which is conducive for industry associations to produce the Codes on behalf of the entire Australian online industry.

More information is needed on the RAS and AV Roadmap Consultations

DIGI supports the aims of the Online Safety Act 2021 (the Act) to improve and promote online safety for Australians. We want to emphasise that DIGI's members share the Office's goal in these initiatives to ensure tools are available to support limiting access by minors to age inappropriate material, and detail some of this work in the final section of this submission.

As noted, the initiatives of the Office to develop a Restricted Access System (RAS) and the Age Verification (AV) Roadmap are linked in that they concern the development of solutions to protect minors from inappropriate materials online. While acknowledging the importance of the work being done by the Office in this area, this submission raises concerns about the scope, feasibility, and transparency of the work program of the Office concerning RAS and AV roadmap, as currently outlined in the explanatory materials provided on the Office's website[1]. Addressing these concerns will provide a clear foundation and pathway to ensure that both industry and the public have confidence in any solutions that the Office may implement. We have therefore provided specific recommendations about how to address these concerns, which we hope will be useful in strengthening the Office's work program.

[1] https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification-call-for-evidence; and https://www.esafety.gov.au/about-us/consultation-cooperation/restricted-access-system.

Need for clarity around the scope of RAS and AV Roadmap

The breadth and lack of clarity around the scope of these consultation processes makes it difficult for industry to engage in the questions raised by each.

Scope of RAS

First, the scope of the proposed RAS covers content that is, or is likely to be, classified as Class 1 and Class 2 materials under the National Classification Scheme and will be extended to apply to "social media services," "designated internet services," "relevant electronic services," and "hosting services" that are providing access to material from Australia (as these services are defined in the Act). **Following these definitions, we understand that the RAS will now encompass all private messaging services along with every website in Australia, and any service that enables online interaction between Australians.**

As well as the broad scope of application, the Class 1 and Class 2 materials categories are extremely broad, and it is unclear how they will be interpreted by the Commissioner under the revised directive and the Act in general. It is important to note that the Classification Board publishes information about how it applies the criteria of the Classification scheme to films, print publications, computer games and broadcast media. In contrast, the Commissioner is not required under the Act to publish data or guidance as to the kinds of materials that are classified as Class 1 or Class 2 on social media, instant messaging, online games, websites, apps and the range of electronic and internet service providers.

Scope of AV Roadmap

Second, it is unclear what type of online content will be subject to age verification under the AV roadmap. The work of the Office on age verification is intended to take forward the Government's commitments on age verification based on the report of the House of Representatives Standing Committee on Social Policy and Legal Affairs inquiry on into age verification for online wagering and online pornography.[2] In June 2021, the Government provided in principle support to the Committee's recommendation that the Australian Government resource the Office to develop and publish a roadmap for the implementation of a regime of mandatory age verification for online pornographic material, setting out:

a. suitable legislative and regulatory framework;
b. a program of consultation with community, industry, and government stakeholders;
c. activities for awareness raising and education for the public; and
d. recommendations for complementary measures to ensure that age verification is part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.[3]

---

[2] *Protecting the age of innocence Report of the inquiry into age verification for online wagering and online pornography (*House of Representatives Standing Committee on Social Policy and Legal Affairs, Febuary 2020*)* https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2freportrep%2f024436%2f72805.

[3]*Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence, June 2021* https://www.infrastructure.gov.au/department/ips/government_responses/government-response-protecting-the-age-of-innocence.aspx.

In its call for evidence, the Office says that the AV roadmap is intended to address "online pornography and other age-inappropriate material", but no further information is provided about how the Office defines those concepts. For example, it is unclear if the Office is concerned with certain types of sexually explicit Class 1 or Class 2 materials under the National Classification Scheme, which is a well established regime for evaluating the suitability of content for minors or if the roadmap will have a broader remit. More importantly, questions remain about what kind of services Australians will be restricted from accessing without age verification. Will all Australians be required to undergo age verification before accessing specific types of websites that have a significant volume of content with a particular classification? Or is the intention that all Australians will need to undergo age verification in general in order to determine their eligibility to access certain content or websites?

Need for detailed guidance from the Office on both RAS and AV

Before the RAS and AV roadmap are finalised, it is critical that the Office publishes detailed guidance on how it assesses the different categories of online material and services that will be subject to age restrictions. This transparency will facilitate industry compliance with these initiatives and is also extremely important to the Australian public so that they understand the types of materials that they might be restricted from accessing and sharing, and the types of services that will require age verification. We recommend that the provision of this guidance be discussed with representatives of the industry in the next phase of consultation on the RAS directive and AV Roadmap.

Need for an approach to AV that is targeted at websites that pose greatest risk to minors

In implementing the AV roadmap, we caution against the proposed approach in the RAS directive that applies to an extensive range of intermediary services including social media services, apps, messaging services, online gaming, websites and internet service providers, regardless of their risk profile, and whether or not they host or enable access to the content of concern.

We would also draw to the Office's attention to the considerable challenges of applying age verification requirements to such a broad range of services. For example, if the AV roadmap requires online intermediaries to age-gate users' access via their services to third party sites that host adult content, this places those intermediaries in a challenging position; It will not always be evident to intermediaries who owns or controls those third-party sites, what content is hosted on the site, or where that content is geographically hosted. Private messaging services also face unique challenges, especially if businesses will be required to remove or age-gate specific pieces of content. Private messaging works very differently to publicly accessible services like websites or social media. Users of messaging services have greater expectations about the privacy of their personal communications and will likely be seriously concerned about the imposition of regulations that require businesses to monitor or control the content of their messages.

In the light of these challenges we suggest that the Office focus on developing solutions for those specific types of adult websites that pose the greatest risk to minors, as this would be a more effective way to address the root cause of the issue. Furthermore, we would also suggest that the assessment of the risk of harm take into account the tools currently available on a range of intermediaries that support limiting access by minors to age inappropriate material, such as those that require age confirmation or give parents the ability to monitor minors' behaviours online. This would ensure that the AV roadmap is a

proportionate response to the policy concern about protecting minors from exposure to age inappropriate content.

Recommendations in this section

2. We ask the Commissioner to publish guidance about:
    a. The specific types of materials on social media services, apps, messaging services, online gaming, websites and internet service providers that the Office categorises as Class 1 or Class 2 for the purposes of the RAS directive and the enforcement of the Act in general.
    b. How the Office defines "Online pornography and other age inappropriate material" that will be covered by the AV Roadmap; and
    c. The scope of the services that adults will be restricted from accessing under the AV Roadmap.

3. We recommend the provision of the guidance outlined in recommendation 2 above be discussed with representatives of the industry in the next stage of consultations on the RAS directive and the AV Roadmap.

4. We ask that in developing the AV Roadmap that Office focus on age verification solutions for those types of websites operated by online businesses that pose the greatest risk to minors because of the nature of the content and services they offer, rather than taking the approach in the RAS directive which applies to a range of social media services, apps, messaging services, online gaming, websites and internet service providers, regardless of their risk profile.

Need for clarity about how the Office has used the current RAS system

Our understanding is that the proposed new RAS system directive will broaden the scope of services that are subject to the requirements under the existing RAS, while limiting its application to material that is unsuitable for a minor to access. The Office does not currently publish information about the operation of the existing RAS system and its effectiveness, nor does the discussion paper on the RAS shed light on those questions. Without transparent data about the enforcement of the current directive, online businesses and the public may be unclear about the need for the new scheme. It would be helpful if the Office could provide that data, together with an assessment of the effectiveness of the current system and the need for the system to be revised. Going forward, we would suggest that data about the operation of the revised directive be regularly updated and published on the Office's website.

Recommendations in this section

5. We ask the Office to publish data about the enforcement activities undertaken by the Office on the existing RAS directive to date, together with an assessment of the effectiveness of the current system and the rationale for the proposed changes to the system.
6. We ask the Office to commit to regularly publishing details about the future enforcement activities undertaken by the Office under the new directive.

Attempts to implement schemes for age verification in other countries

The explanatory materials provided by the Office in launching the RAS and AV Roadmap consultations do not include any analysis of the experience of countries around the world with implementing age verification solutions for online content.

An evaluation of the experience of comparable democracies with age verification solutions is critical in assessing the likely feasibility of different kinds of solutions in Australia and in giving the public confidence in the approach that is adopted. For example, possible solutions might require users to upload their identity documents, scan their fingerprints, use facial recognition technology or have their age estimated by artificial intelligence. Due to concerns about user privacy and cyber security, these types of solutions have met considerable disputation overseas. In particular, the UK Government announced in October 2019 that it would not proceed with Part 3 of the Digital Economy Act 2017 concerning age verification for online pornography after undertaking an extensive consultation process over several years. The scheme was criticised for being easily circumvented and raised considerable concerns around user privacy. This example indicates the vital importance for public confidence in the technical solution for age verification and the practical issues associated with relying on national identification systems as age verification solutions. Any solution that gives the Government access to users' personal identification data is likely to raise serious privacy concerns that could impede the implementation of an AV roadmap in Australia.

Recommendations in this section

7. We ask the Office to research attempts to implement schemes for age verification in other countries, and publish an analysis of the experience of comparable democracies with age verification solutions. This should include issues that arose with the implementation of the United Kingdom age verification scheme, and how the Office plans to ensure that similar concerns do not undermine the implementation of its AV roadmap.

Key policy considerations for RAS and AV Roadmap consultations

A key factor in the effectiveness of the RAS and the AV Roadmap will be the extent to which they provide effective protections for minors, and safeguard the cyber security and personal information of Australian Internet users. A consistent theme in evidence to the Parliamentary inquiry into age verification for online wagering and online pornography was the importance of any system for online age verification having strong controls for the safety, security, and privacy of users[4]. It is our initial assessment that these two initiatives encourage the widespread collection of age data, potentially even identity verification documentation such as drivers' licences. This runs counter to the universally accepted privacy best practice of data minimisation that forms part of the Australian Privacy Principles under the Privacy Act

[4] See APP 3 and APP 11. APP 11: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/. APP 3: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information/

1988 (cth). Data minimisation is also a key principle of the Consumer Data Right.[5] In this section we offer our views on the key policy considerations which should inform the development of the approaches to developing solutions to protect minors from age inappropriate content in Australia:

1. The need for a coordinated, efficient government approach that balances safety, privacy and online security; and
2. Public sentiment about online identification solutions.

Safety, security, and privacy of online users

Both the RAS and AV roadmap will likely require potential additional data collection and changes to the security protections for personal data on the part of these services in Australia including:

a. age data, perhaps including drivers' licenses or other documentation in order to verify age;
b. personally identifiable data about people who visit websites.

In addition to the two factors above, as noted, the Department has commenced an open consultation process on a draft instrument called the Basic Online Safety Expectations (the BOSE). The BOSE would apply to social media services, private messaging services, online gaming and websites. It states: "If the service uses encryption, the provider of the service will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful." There are fundamental impracticalities and barriers to services detecting and addressing encrypted material; if this becomes law, a result could be the weakening of encryption, which is crucially important to ensuring adequate levels of cyber security across a wide range of services.

DIGI predicts that the potential increase in data collection for all websites, and the sensitive nature of the data being collected, will create increased cyber security risks to a whole range of websites in Australia. A pertinent example is provided by the 2015 Ashley Madison data breach in the United States. In July 2015, user data was stolen from the company Ashley Madison, a commercial dating website associated with extramarital affairs, and threatened to be released if the company did not shut down. The following month, more than 60 gigabytes of company data was leaked, including user data such as real names, home addresses, search history and credit card transaction records[6]. It is a reasonable prediction that similar widespread attacks, intended to publicly shame users of certain websites through personally identifiable data, may occur if widespread age verification solutions are imposed. This example highlights the potential cyber security implications of these particular initiatives, and demonstrates the need to ensure that the Office's solutions for protecting minors from inappropriate content do not increase cyber security risks to Australian users. While the protection of minors from online pornography is undoubtedly of concern, it will be critcal for the public to have confidence that the chosen solutions will improve the safety of minors online and will not put the data of adults and minors alike at risk.

It is also worth noting the potential for the initiatives concerning RAS and the AV Roadmap to clash with other policy initiatives by the Government in the area of cybersecurity and privacy, highlighting the need for a coordinated, whole-of-Government approach to digital regulation. There is clearly a risk of direct conflict between the Government's expectations that online businesses will protect users' privacy and the introduction of new online safety rules that require online businesses to reduce the level of user privacy on their services or collect vastly increased volumes of personal information. For example, there is need

[5] https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-3-privacy-safeguard-3-seeking-to-collect-cdr-data-from-cdr-participants/

[6] See for more information: https://www.forbes.com/sites/zakdoffman/2019/08/23/ashley-madison-is-back-with-30-million-cheating-spouses-signed-since-the-hack/?sh=5aac67123878

to ensure that the RAS and AV Roadmap requirements do not conflict with requirements in the Australian Privacy Principles that businesses protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure[7]. Similarly there is a need to ensure that the RAS and AV roadmap are congruent with the Australian Privacy Principles under the Privacy Act that require businesses to minimise privacy risks by minimising the amount of personal information they collect and store[8]. We also understand that there are proposed reforms to the Privacy Act 1988 (Cth) that will require social media services to develop codes that spell out the measures they take to protect users personal data, including the data of minors. Again, there is potential for the content of these privacy codes to conflict with the RAS and AV Roadmap. Additionally, the Department of Home Affairs is currently undertaking a consultation about how to strengthen Australia's cyber security regulations and incentives, in response to a discussion paper titled *Strengthening Australia's cyber security regulations and incentives*.

To avoid conflicts between such initiatives and the work of the Office on age verification, it will be critical for the Office to coordinate with the extensive range of departments and regulatory bodies which are key stakeholders in cyber security issues. Specifically, we encourage the Office to consult with the Department of Home Affairs, the Attorney General's Department, the Office of the Australian Information Commissioner (OAIC), Australian Cyber Security Centre in the Australian Signals Directorate, and the Department of Communications.

Recommendations in this section

8. We ask the Office to:
    a. Ensure that the Offices' solutions for protecting minors from inappropriate content do not increase cyber security risks to Australian users.
    b. Coordinate with the extensive range of departments and regulatory bodies which are key stakeholders in cyber security issues. Specifically, we encourage the Office to consult with the Department of Home Affairs, the Attorney General's Department, the Office of the Australian Information Commissioner (OAIC), Australian Cyber Security Centre in the Australian Signals Directorate, and the Department of Communications.

Public sentiment about use of certain technologies for online identification

A separate policy concern in developing an RAS or RV Roadmap is the potential for vehement public opposition and significant government backlash to any solution that requires Australians to provide personal data to an entity that could be used to identify their activities online. The submission by the Department of Home Affairs to the inquiry into age verification for online wagering and online pornography submitted that it was developing a Face Verification Service (FVS) legislation, which it proposed could assist in age verification, to allow the government to provide identity matching through this technology was rejected by the Parliamentary Joint Committee on Intelligence and Security in 2019 for failing to adequately protect citizens' rights with proper safeguards. This legislation was met with

[7] APP 11, as above.
[8] APP 3 and APP 11, as above.

considerable criticism from the public and human rights bodies.[9] Former Australian Human Rights Commissioner Edward Santow called for a moratorium on facial recognition technology until more discussions and safeguards were considered, emphasising that while new technologies could deliver societal benefits, they shouldn't come at the risk of human rights.[10] The FVS legislation has yet to be reintroduced. This example highlights the need for transparency about the technologies that may be under consideration in the development of the RAS and AV Roadmap.

Recommendations in this section

9. We ask the Commissioner to publish information about the technologies that the Office is considering in developing the RAS and AV Roadmap, and in particular if any solutions will require the public to provide data to an entity that could identify their activities online.

The importance of transparency in the consultation processes for the RAS and AV Roadmap

We have two key concerns around the transparency of the consultation processes for the RAS and AV:

1. The extent to which the Office will publish submissions received to these consultations and its response to the issues raised; and
2. How the engagement process with key stakeholders' in the AV roadmap will be conducted.

These processes have broad ranging implications for the privacy and cyber security of Australians, as well as technical and other implications for the companies required to implement these schemes, which is why transparency is critically important.

Publication of submissions and the response of the Office to key issues

We understand that submissions responding to the call for evidence on the AV Roadmap will not be made public. As noted in our covering letter to this submission, these initiatives are linked since both involve the development of regulatory tools that aim to protect minors from being exposed to age-inappropriate online material. We understand that the input provided into the RAS and AV Roadmap consultation processes will also influence the Office's approach to other initiatives such as the Codes. As a result we ask that the Office reconsider its decision not to release submissions on the AV roadmap and commit to publish all the feedback they are receiving in relation to both consultation processes.

As noted above, the discussion paper for the RAS and call for evidence on the AV Roadmap provides very limited information on the policy considerations that will inform the development of those initiatives. As a result, we would ask that the Office provide the public with visibility into the considerations that have informed the development of the draft RAS directive and the draft AV Roadmap, when these are publicly released. At a minimum, we would appreciate it if the Office could outline the key issues raised by submissions and how it has responded to these concerns.

---

[9] https://www.itnews.com.au/news/govt-told-to-rewrite-facial-recognition-bills-532885; https://www.abc.net.au/news/2019-10-24/parliamentary-security-committee-rejects-identity-matching-bill/11634742; https://www.canberratimes.com.au/story/6962043/you-cant-ever-get-privacy-back-act-delays-biometric-licence-upload/

[10] https://www.canberratimes.com.au/story/6962043/you-cant-ever-get-privacy-back-act-delays-biometric-licence-upload/

Recommendations in this section

10. We ask the Commissioner to:
    a. Publish all submissions the Office receives to the consultation processes for the AV Roadmap and the RAS.
    b. Publish details of the key issues raised by submissions and how the Office has responded to these in developing proposals for RAS and the AV roadmap.

Engagement process for AV Roadmap

We understand that the Office will undertake an engagement process with key stakeholders (identified in the call for evidence), to analyse insights to inform the AV Roadmap. No information has been provided to date about that engagement process and the extent that industry or the public will have visibility over how it is conducted. We ask that the Office publish further details of what the engagement process will involve and who will be asked to participate. At a minimum, the engagement process should provide a further opportunity for the public to provide feedback on the draft of the AV Roadmap before it is finalised. In our view, this degree of transparency is critical to encouraging public and industry confidence in the development of these initiatives.

Recommendations in this section

11. We ask the Commissioner to publish details of the process that it will adopt to develop the AV Roadmap, including:
    a. Details of the key stakeholders who it will engage with subsequent to the conclusion of the consultation process.
    b. Details of when a draft of the AV Roadmap will be published.
    c. The time frame for the public to give feedback on the AV Roadmap before it is finalised.

Overview of DIGI members work on protecting minors from age inappropriate materials online

We want to emphasise that DIGI's members share the Office's goal in these initiatives to ensure minors are protected from pornography. DIGI's founding members have age restrictions in place for their services, processes to address reports of violations of those restrictions in accordance with their policies, restrictions in their content and advertising policies on pornography, and an enforcement infrastructure comprised of proactive technology detection and/or human moderators. They also have tools to restrict the experience of minors online and invest in social programs aimed at minors and parents.

In relation to age restrictions, relevant members set age restrictions on their user-generated content platforms and many other products to limit and discourage the use of services by underage users, ranging from under 13 to 18 as appropriate to the service. When a notice or express admission that a user is underage is received, it will be investigated and accounts will be suspended accordingly. Some services will also take steps to prevent users lying about their age to access an account after it has been denied, by placing a persistent cookie on the device to prevent the child from attempting to circumvent the age restriction or by using artificial intelligence to understand the true age of a user.

All members have strict content policies in relation to pornographic content. On social media and content platforms, there are policies in their community guidelines restricting nudity, pornography and sexually explicit content. On Google Search, sexual and violent terms are removed from auto-complete and pornography in demoted in search results unless the user is clearly searching for it. These policies are enforced through a combination of human moderation and machine learning that detects problematic content for further review. For example, YouTube runs classifiers across videos looking for unusually high numbers of flesh coloured pixels. Such proactive detection technology is proving highly effective. Facebook does not allow nudity or sexual activity content: in the last quarter, they removed 32.8 million pieces of content for adult nudity or sexual content, 98.9 percent of which was detected proactively before it was reported by a user.

These policies are also reflected in members' advertising policies. Google Search does not allow hyperlinks that drive traffic to commercial pornography sites, nor does it allow pornography ads to be placed within its Search engine, or run Google ads against pornographic websites. On social media and content platforms, all members have strict controls on pornography, adult products and services, and nudity.

In addition to the measures outlined above, DIGI members have a range of tools to protect the experience of minors online. Google's Safe Search filter prevents ads containing or promoting nudity, sexually suggestive content, adult entertainment and other services from appearing within search results. Android phones and tablets offer restricted profiles where more mature content can be filtered out of the app store, and on Chrome parents can create restricted profiles for minors that allow parents to block and approve sites viewed, and Safe Search is on by default in such accounts. Twitter has also Safe Search settings which hide Sensitive Content and remove blocked and muted accounts.Instagram defaults users between the ages of 13 and 17 into private accounts upon sign-up, and use a number of safety measures for users in this category, including making it harder to adults to comment or interact with them, steps to inhibit inappropriate interactions with adults in private messaging, and preventing teens from seeing age-sensitive ads).Linktree enforces sensitive content warnings in relation to specific URL links that contain materials that are not appropriate for all audiences.

In addition to strict policies and enforcement, DIGI members also proactively deliver social programs in the community to assist minors and parents to understand how they can safely engage online. For example, many of our members work with expert partners such as Project Rockit and the Alannah and Madeleine Foundation on youth education programs, that include content relating to nudity, sex education and safe browsing, as well as initiatives to support parents, such as the Instagram Parents Guide.

Our members regularly engage with experts to inform their approach to policy development. These consultations involve complex policy issues that require parental oversight and education, as well as technical solutions. In relation to technical solutions, some DIGI members have participated in an expert working group convened by the Office of the the eSafety Commissioner, that produced a Cabinet-in-confidence report around limiting the exposure of minors and young people to online pornography. We would encourage the Commissioner to review and take into account the thorough and consultative contributions made by the working group on this issue that resulted in the Cabinet report.

12. We ask that in developing the RAS and AV roadmap the Office take into account the contributions of the working group convened by the Office of the eSafety Commissioner around limiting the exposure of young people to pornography.