Australian Government | eSafetyCommissioner

Senate Environment and Communications References Committee on Internet Search Engine Services Online Safety Code

Questions on Notice – OCTOBER 2025

Senator Dean Smith – QON's	

Regarding the social media minimum age changes, is it correct that accounts for children under the age of 16 need to be removed?
• Will the accounts of children which have parental supervision on them be impacted?
• Do you consider that children using an account under their parents account is a safe alternative?
  ○ If so – how and why?
  ○ If not – how and why?
	• Yes. Services that meet the definition of 'age-restricted social media platforms' under the Online Safety Act 2021 (Cth) (the Act) must take reasonable steps to prevent age-restricted users (being end-users under the age of 16) from having accounts with the platform.
	• This includes accounts on age-restricted social media platforms held by under-16s with some form of parental supervision enabled. The Act does not provide any exception for accounts which are supervised in some form by parents or carers.
	• Many factors affect children's online safety. There may be circumstances where using a parent's account is safer (for example, because the parent is actively supervising the experience) as well as circumstances where this is less safe (for example, because safety settings normally applied to children's accounts are not applied to the parent's account).

Senator David Pocock – QON's	
Can you please outline what work you have undertaken to progress the Digital Duty of Care the Labor government committed to in 2024?	• The Digital Duty of Care is yet to be legislated by the Government. eSafety has provided input into a range of materials relating to the duty of care developed by the Department and is considering how a duty of care model could work with current regulatory schemes.
Please provide a list of all stakeholders the E-Safety Commissioner and/or the office of the E-Safety Commissioner has met with in relation to a Digital Duty of Care.	• eSafety has not meet with any external stakeholders in relation to the duty of care.
What is the latest information you have regarding how many VPNs are currently being used by Australian Citizens?	• eSafety has not collected data about VPN use by Australian citizens.

Has the E-Safety Commissioner and/or the office done any consultation regarding device level age verification or API access?	• Between June and August 2025 eSafety undertook broad consultation on the implementation of the social media minimum age restrictions. eSafety met with over 345 people from over 160 organisations which included academics, civil society, parents, young people and tech companies. Device level age verification and API access was raised by some participants during these consultations. Summaries of the consultations are publicly available here • Prior to that, eSafety ran an extensive stakeholder consultation to support the development of our Age Verification Roadmap and Background Paper, provided to Government in 2023. Device level age verification was raised by participants and discussed in these documents, publicly available here.

Senator David Shoebridge – QON's	
Legal Basis and Framework	
What specific legislative provisions or regulations require social media companies to retain data from young people's accounts that are deactivated or removed due to the age restriction ban?	• The Online Safety Act does not require age-restricted social media platforms to retain data from young people's accounts, where those accounts are deactivated or deleted to comply with the social media minimum age obligation. • eSafety's regulatory guidance on the social media minimum age obligation explicitly states 'eSafety does not expect providers to retain personal information as a record of individual age checks' (page 25).
Is data retention a requirement imposed by the Online Safety (Basic Online Safety Expectations) Determination 2022, or will separate legislation or regulatory guidance be introduced?	• The *Online Safety (Basic Online Safety Expectations) Determination 2022 (BOSE)* set out the Australian Government's expectations about the steps that providers of social media services (SMS), relevant electronic services (RES) and designated internet services (DIS) should take to keep Australians safe online. • The Basic Online Safety Expectations do not place enforceable requirements on providers. • Section 19 of the Basic Online Safety Expectations sets out the expectation that providers will keep records of reports and complaints about specified types of material (such as class 1 and class 2 material) provided on the service for 5 years.
How does the data retention requirement align with the Privacy Act 1988 and its principles around data minimisation and retention limits?	• There is no data retention requirement. To the extent the Basic Online Safety Expectations create expectations relating to keeping records, these expectations do not affect any applicable protections in the Privacy Act 1988. • The Office of the Australian Information Commissioner (OAIC) is responsible for ensuring compliance with the Privacy Act.
Will there be exemptions for certain types of data?	• There is no data retention requirement.

What recourse will young people have it platforms remove their accounts and block access or delete photos, videos or other personal materials?	• Age-restricted social media platforms must comply with the social media minimum age (SMMA) obligation, which means taking reasonable steps to prevent under 16s from having accounts. The SMMA obligation does not include a requirement to provide recourse to affected young people for loss of access to their account data, but eSafety has made clear its expectations to platforms that steps to comply with the obligation be undertaken in a thoughtful, considerate and rights-respecting manner. • eSafety's regulatory guidance for platforms encourages platforms to provide young people with the opportunity to download their account information in a simple, seamless way prior to deactivation or request access to their information from the provider within a reasonable period after account deactivation (page 35). Where reasonable, platforms should consult with end-users, particularly those under 16, to understand their preferences and give them options regarding their account (page 35). • eSafety's guidance also encourages platforms to ensure end-users over the age of 16 have access to accessible review options if they feel their account has been wrongfully removed (page 30).
How will eSafety verify compliance? Will there be audits, reporting requirements, or other monitoring mechanisms?	• eSafety has published regulatory guidance for industry, which sets out eSafety's approach to compliance and enforcement relating to the social media minimum age (SMMA) obligation. • Section 63G of the Online Safety Act enables the eSafety Commissioner to require any information from a provider of an age-restricted social media platform that is relevant to their compliance with the SMMA obligation. • eSafety will use the information-gathering powers in s 63G to obtain information about a provider's systems and processes to detect and prevent Australian children under 16 years from having accounts on their service, not individual accounts. • To monitor compliance, eSafety will continue engaging closely with age-restricted social media platforms, use our information-gathering powers, and may draw on additional insights derived from research, relevant stakeholders and the public.
Implementation Requirements	
How long must companies retain data for accounts belonging to young people identified who are subject to the age ban?	• The Online Safety Act does not require age-restricted social media platforms to retain data from young people's accounts that are deactivated or deleted to comply with the social media minimum age obligation.
Are there requirements about what specific data must be retained e.g. user profiles, content posted like photos or videos, communication logs,	• There are no data retention requirements.

metadata, device information, location data, or all of the above?	
Are there different retention requirements for accounts of different age groups (e.g., under 13 vs. 13-16)?	• No, there are no data retention requirements.
How eSafety has engaged young people throughout the consultation process for SMMA.	• eSafety engaged the Australian Youth Affairs Coalition to lead consultations with 53 children and young people aged 13-23 from across Australia and from a variety of backgrounds and circumstances. • A summary of the consultation is available here. • Insights from the consultation supported the development of eSafety's approach to implementing the social media minimum age, including our regulatory guidance, statement of commitment to children's rights, and resources for children and young people.
How the gap will be filled for 2.5 million young people who are currently relying on social media for peer-to-peer support and mental health support under SMMA.	Measures in place include: • Access to non-age-restricted platforms: Under-16s will still be able to use online services, sites and apps that are not covered by the social media age restrictions. These include platforms designed primarily for messaging, online gaming, creativity, learning, and entertainment, many of which foster safe peer-to-peer interaction. • Support-focused services remain accessible: Online services that provide crucial information and support for young people experiencing distress are explicitly excluded from the age restrictions. This ensures continued access to mental health resources and crisis support. • Partnerships with mental health organisations: We have partnered with leading mental health organisations to ensure that the information and resources we've created are developmentally appropriate and genuinely supportive of young people's needs. These partnerships help us deliver trusted, evidence-based content across platforms that remain accessible. • Digital rights and wellbeing: eSafety acknowledge the importance of upholding young people's digital rights, including their ability to connect, express themselves, and seek help online in safe and age-appropriate ways. We understand that this remains a key focus for government policy.

Senator Hanson-Young	
Whether there were any payments from Ed Craven, one of the co-founders and owner of Kick, or any other owner in the company to the account [which hosted the livestreaming of the user's death] to promote this type of abusive and deadly behaviour?	• eSafety does not hold any information to confirm whether or not any payments were made to Raphaël Graven's account on Kick, also known by the pseudonym Jean Pormanove, by the owners of the Kick service."

Senator Henderson	
Senator Henderson: Could you please review the evidence of Mr Levy from Qoria, who gave compelling evidence that safety technology is available in other countries, particularly to schools, and there are huge limitations on accessibility, either by parents or children, to safety technology which is being made available to businesses and commercially but not to young people. Parents cannot access this safety technology to the same extent as in other countries.	• eSafety has reviewed the evidence of Mr Levy from Qoria. We note that network filtering policies and practices in public schools are the responsibility of each state and territory's respective Department of Education. • eSafety notes that device-level controls to prevent children's access and exposure to particular age-inappropriate material (such as online pornography) are included in the Phase 2 Codes. • The Equipment Online Safety Code (Class 1C and Class 2 Material) requires that users of portable interactive devices which enable general internet browsing (such as smart phones, tablets, etc) are given the option to create child accounts with relevant safety tools to prevent access to age-inappropriate material. This responsibility sits with the operating system (OS) provider (such as Microsoft's Windows, Apple's iOS and macOS, and Google's Android and ChromeOS). OS providers must also take appropriate steps to further develop and improve these safety tools. • Other devices that provide access to the internet must make available similar safety tools that end-users can choose to opt-in to. • Additionally, under the Internet Carriage Services Online Safety Code (Class 1C and Class 2 Material) Services must provide easily accessible and clear information about how to prevent children's access to harmful material, including through filtering products. Services must also address compatibility issues with third-party filtering products.