

Today, Discord made a press release regarding the global rollout of Teen-By-Default settings, along with the age verification that it has been applying to accounts in the UK and Australia along with it.

As someone in Australia, having seen that rollout, the options available for age verification and the impact its had on my Discord experience, I can say that my confidence in this platform as something to actively participate in and try to support financially has completely waned.

I was hoping that with enough feedback and pushback that Discord, at minimum, would consider other options for verifying age that do not include facial scans or government ID. Account age or receiving a valid payment via a method that can only be used by an adult has been a common practice put in place by Newgrounds since the UK laws were introduced, as well as the age verification platform utilised by Bluesky.

Newgrounds article on age verification: <https://www.newgrounds.com/bbs/topic/1549829/1>
Kids Web Services on their age verification methods: <https://www.kidsweservices.com/en-US/services/age-verification>

Neither of these options have been publically talked about despite offering better privacy to users trying to verify their age.

Account age is a no brainer; if it has existed long enough, it is very likely owned by an adult. As Newgrounds notes, this is a reliable method of age verification akin to payment processing by using their own data to confirm the email attached to an account has been used for a long time. Considering Discord has been around long enough for accounts early in its life to reach 10-11 years, so it seems like a reasonable threshold to begin the process of flagging accounts, if not using this as a standard for automatically being unflagged; unless you have some way of showing the account has switched hands or suspect that the person created it when they were 5, this is relatively reliable as a starting point.

But obviously this can't be the only standard for verifying age, so being able to pay for something with a credit card could be the next step if there is suspect activity or an account is quite new. As noted in both links, there are varying ways to do this (Newgrounds even used its own supporter packs as a threshold for this), but a small fee to confirm a working credit card for that account is another option. This also utilises the services of payment processors which over many, many years of improvements has a far higher threshold of base security than any age verification on the market, both for Discord (fraud detection, etc.) and for users (no private information is exposed to Discord).

On the security and privacy front, I have a massive issue with biometrics and government ID being the ONLY options available for this verification process. Age verification of this type is relatively new and quite frankly untested or inadequate in terms of safe guarding that information;

demonstrated not even half a year ago when Discord's third-party for processing this information had a massive breach:

<https://arstechnica.com/security/2025/10/discord-says-hackers-stole-government-ids-of-70000-users/>

The breach of biometric or government documents is completely unacceptable, especially when there are NO other alternatives to verifying one's age with Discord. Even if the partner's change, there's language in the press release that, quite frankly, is an insult to its users. There is not nearly enough transparency in the partner they use, nor the security standards at play, or how this has improved assumes an ignorance regarding this matter in Discord's user base that I find incredibly concerning.

The phrasing I take particular issue with references how verification information "in most cases" be deleted immediately or the process is a one time thing.

I have an account that is 10 years old as of November 2025, I have interacted with people in Discords with NSFW content where everyone was 20+ minimum (verified through voice, social media presences, etc.) with an email that has existed for 20+ years. I've also spent money on Discord Nitro before I had to cancel it due to some previous worrying decisions in the past. There is plenty of data that Discord could correlate to create a baseline that an account like mine likely does not belong to someone who is a teenager.

I have seen discussion going around that Discord has some process of flagging accounts to begin with, and that this was not a blanket flagging of accounts being used in UK/Australia. The latter being the case is, again, a complete insult to its user base, so I will be charitable and assume that there is a process of identifying accounts that are suspicious. If the above information was not enough to at least lower the likelihood that my account would be flagged, then I have a serious concern on how Discord is operating in this regard.

From: [REDACTED]
To: [OAIC - COPC](#)
Subject: RE: Exposure Draft of Children's Online Privacy Code
Date: Thursday, 4 June 2026 10:26:25 PM
Attachments: [REDACTED]

CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

To who it may concern,

My name is [REDACTED], I am a Software Engineer living in Victoria and I've been using the internet and been involved in online communities for over 20 years. I am primarily speaking as a concerned citizen as opposed to an expert (I have some experience in general online security as part of my job, but not with regard to the exact subject of the Privacy Code) and a long time user of online spaces to raise concerns with regard to a section of the Children's Online Privacy Code.

My primary concern is Part 3, Division 1, Section 8 on page 4 of the Exposure Draft, 'Ascertaining the age of end-users of an entity's service' (which I will be referring to as 'the section' from now on).

The section lays out several subsections about determining the age of someone using an applicable service before obtaining other information about that person, which I assume and interpret that this is to determine whether the rest of the Code will apply to the collection of information about said person.

While the general goal of this section is agreeable insofar as ensuring that extra precaution is taken with regard to a child's information online, I have major concerns about the lack of guidelines around "reasonable steps" in the section in light of the roll out of Age Verification across several services that are available to Australians.

My key example here will be the online communication software "Discord". You can find an email I wrote to Discord on this topic attached to this email for reference, as I go into more specifics regarding how it has rolled out Age Verification, but to summarise:

- Discord has only been using Facial Recognition and Government ID as options for their Age Verification, which is the standard across many applicable services
- They mass flagged a lot of accounts with no disclosure on the ways that they determined the accounts were a concern wrt: age

Applying the section as written to this instance of Age Verification for the purposes of complying with the Privacy Code, there are major online privacy concerns for *all* Australian citizens due to the lack of defining these "reasonable steps", and neither does the section or the Code give the government the ability to critique or require a standard of practice to

ensure the safety of Australians online.

Firstly, there is no standard by which to gauge whether a service is taking "reasonable steps" with regards to online privacy. Though Facial Recognition and Government ID are certainly popular amongst the services that have implemented Age Verification, they require exposing private information, often to third parties of the applicable services (which I shall discuss later in this email), to validate someone's age. However, there are more reasonable ways to determine this information that have not been as widely adopted that are worth considering as "reasonable steps".

1. Account age. This, along with the analysis of activity of said accounts (often a core part of social media platforms for the purpose of detecting children using their services already), should be a major consideration for this purpose. Unless the service has some reasonable doubt as to whether the account has changed hands or has started acting suspiciously, there is little reason this can't be part of the consideration.
2. Making a payment with a credit card. A person must be 18 years or older in Australia to have a credit card, similar to the UK which has implemented similar Age Verification laws; if someone is able to be able to make a payment on a credit card that can be associated with the account in question, this can also serve as proof of the account user's age.

The above steps are used by some applicable services, like "Newgrounds", as well as online services that are used for Age Verification like "Kids Web Services":

Newgrounds article on age verification:

<https://www.newgrounds.com/bbs/topic/1549829/1>

Kids Web Services on their age verification methods:

<https://www.kidsweservices.com/en-US/services/age-verification>

However, these are not the most popular methods of Age Verification, with many applicable services resorting to third parties that perform Age Verification via Facial Recognition and Government ID, a set of sensitive information that, if leaked, could compromise a person's privacy and open them up to fraud, impersonation and more. While the section does specify that the applicable service destroy this information once it is done with its Age Verification, the relevant subsection does not note anything about a third party that is used for this purpose, which leads me to my second point.

Secondly, the section as written specifies nothing about how third parties used to satisfy the section should behave when used for these purposes. This creates another point of failure with regard to the information gathered for the purposes of Age Verification which, as explained above, is currently almost entirely gathered by using incredibly sensitive information, a person's facial biometrics and government proof of age.

Since the initial wave of Age Verification was implemented in response to the UK establishing laws that require their use, there have been several leaks of private

information from services used by applicable services for this purpose. The incident I am most familiar with is the third party "Discord" previously used for Age Verification, which is covered in this link:

<https://arstechnica.com/security/2025/10/discord-says-hackers-stole-government-ids-of-70000-users/>

These services, due to the fact that they collect this information, let alone potentially store or otherwise retain the information for some time, have been the subject of hackers and the like as they have a) collect highly sensitive information and b) have not had time to harden and refine security practices and processes for handling this data. Furthermore, there is little incentive at the moment for them to improve these services given the roll out of Age Verification laws, making it all the more important to establish how they should be handling this information alongside the applicable services subject to this Code.

Thirdly, the expansions of the practice of Age Verification to any site that may collect any information from people will hamper people's ability to judge legitimate services that require that information and sites that collect that information for malicious purposes.

In fact, since I submitted my email to "Discord" sharing such concerns, a joint statement from scientists who are experts in these fields was released expressing concerns about the methods and practice of Age Verification in the EU, which can be found here:

<https://csa-scientist-open-letter.org/ageverif-Feb2026>

I strongly recommend reading this letter as they are very precise with their concerns and cover this deeper than I can.

To quote part of the Executive Summary:

"Two critical issues have not been addressed: whether age assurance is efficacious and what the potential damages to general security and privacy are. We believe that it is dangerous and socially unacceptable to introduce a large-scale access control mechanism without a clear understanding of the implications that different design decisions can have on security, privacy, equality, and ultimately on the freedom of decision and autonomy of individuals and nations."

And to quote a relevant statement RE: my third concern:

"If minors or adults are deplatformed via age-related bans, they are likely to migrate to find similar services. Since the main platforms would all be regulated, it is likely that they would migrate to fringe sites that escape regulation. This would not only negate any benefit of the age-based controls but also expose users to other dangers, such as scams or malware that are monitored in mainstream platforms but exist on smaller

providers. Even if users do not move platforms, attempting circumvention to access mainstream services from a jurisdiction that does not mandate age assurance might also increase their risk. For example, free VPN providers might not follow secure practices or might monetize users' data (especially non-EU providers that are not subject to data protection obligations), and websites accessed in other jurisdictions through VPNs would not provide the user with the data protection standards and rights which are guaranteed in the EU."

In summary, the expansion of Age Verification as would be required to satisfy this Code risks Australians' private information and there is little in it that allows the government to address the issues that its current implementation has. I understand that the initial laws were written to allow experts to define these things, and the Code itself is not intended to expand on this, I believe that is a major flaw in the Code as written as, given the information I have provided, there are a lot of reasons that the current practice of Age Verification that would be employed to satisfy the Code should be scrutinised and regulated to ensure people's information is safe.

I am hoping by writing this I can encourage more thought and discussion surrounding the Age Verification practice, where it is lacking and may compromise any Australian using services subject to the Code, and what standards or even specific methods should be employed before asking Australians to hand over government ID or facial biometrics.

Thank you for your time.

[REDACTED]
[REDACTED]