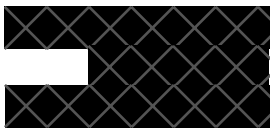


22 November 2024

eSAFETY COMMISSIONER
Level 32 Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC
ATTN: Industry Associations (defined below)

RE: AYLO'S SUBMISSION ON THE PHASE 2 CODES DISCUSSION PAPER

Dear Industry Associations,

We refer to the 'Discussion Paper: Draft Phase 2 online safety codes' ("**Discussion Paper**") in relation to the industry codes currently being drafted ("**Phase 2 Codes**") under the *Online Safety Act 2021* (Cth) (the "**OSA**") published by the Australian Mobile Telecommunications Association, Communications Alliance Ltd, Consumer Electronics Suppliers Association, Digital Industry Group Inc., and Interactive Games and Entertainment Association (together, the "**Industry Associations**") on 22 October 2024.

Aylo Holdings S.à r.l. ("**Aylo**", "**we**", "**our**", "**us**") is deeply interested in, and strongly committed to, reducing, and preventing online harmful behaviour, the spread of toxic content and the potential for adults and children to suffer harm on the internet. Aylo strongly supports the appropriate protection of children from content that is intended to be consumed exclusively by adults online and welcomes the introduction of appropriate age assurance requirements under the Phase 2 Codes.

Aylo is grateful for the opportunity to make a submission in response to the Discussion Paper.

In this submission, Aylo addresses questions 2, 3 and 4 in the Discussion Paper, particularly in relation to the:

- Consolidated Industry Codes of Practice for the Online Industry (Class 1C and 2 Material) Head Terms ("**Head Terms**"); and

- the 3 October 2024 draft of Schedule 3 – Designated Internet Services Online Safety Code (Class 1C and Class 2 Material) ("**DIS Code**").

1. Introduction

1.1. Aylo's business and core values

Aylo (formerly known as MindGeek) is a technology and media company and owner of a large portfolio of adult entertainment properties including Pornhub, YouPorn, RedTube and Brazzers. Aylo's platforms allow consenting adults to explore content that adheres to our core values of consent, freedom of sexual expression, authenticity, and diversity. Aylo's businesses are similar, in respect of the technology we deploy, as compared to other mainstream online platforms. Our primary businesses are comprised of both free and subscription video streaming sites, on which we sell advertising and collect membership fees.

In line with our values and business model, we have a zero-tolerance policy against any conduct that would result in online harms to the Australian community and audiences. In particular, child sexual abuse material ("**CSAM**") and non-consensual content have no place on our platforms, and Aylo has adopted a wide array of robust protective measures to prevent the sharing and consumption of such content.

Aylo is of the opinion that every online platform must be responsible for reducing online harm, and this requires collective action and constant vigilance. Aylo takes its own role in preserving the safety of the online environment very seriously, including by adopting and investing substantially in numerous trust & safety processes.

1.2. Device-level Ecosystem-based approach to Age Assurance

Further to the directed queries set out in the Discussion Paper, our contribution to this public consultation is intended to advocate strongly for a device-level, ecosystem-based approach to age assurance and to provide insights into the complexities of age assurance measures based on our experience, highlighting its challenges within the approaches proposed under the Head Terms and the unintended consequences such platform and site-based measures may present.

Aylo emphatically supports a device-level solution and wishes to situate the issue of age verification more broadly under the regulated areas of online activity that fall within the scope of the OSA. Age assurance and its necessary objective of protecting children from accessing exclusively adult content is best served by an ecosystem-wide approach in order to prevent incidental harms through the dissemination of harmful content on more traditional platforms.

Aylo reinforces the position it has raised in previous submissions regarding ongoing development of the OSA – that is, a device-level and ecosystem-based approach to age assurance is the **only** effective approach in preserving the online safety of children and other users while also balancing the principles and core values of privacy, data security and freedom of expression.

2. Question 2 – Balancing core principles with online safety

The Discussion Paper raises the following query under Question 2:

> *Do you think the Codes strike an appropriate balance between user privacy, data security, freedom of expression and online safety, particularly around services used for private communication and storage of material such as file storage services? Should providers of most relevant electronic services that allow users under 18 (such as email and private messaging services) be required to scan all Australian user's communications and messages to detect and remove lawful Class 1C and Class 2 materials?*

Aylo supports the spirit of the approach set out in the Head Terms which introduce mechanisms through which principles of privacy, data security and freedom of expression can be achieved. In particular, Aylo endorses the requirement for any compliance measures adopted under the Phase 2 Codes to be proportionate, and weighted against the possibility of arbitrary or unlawful inference with privacy, human rights and other matters (e.g. section 5.1(b) of the Head Terms)

Similarly, the Head Terms address the practical realities and potential gaps with respect to existing technologies in the context of age assurance under section 5.1(c). For reference, this section permits organisations to consider factors relating to: (i) technical accuracy, robustness, reliability and fairness; (ii) whether end-users can circumvent the relevant measure; (iii) the effectiveness of those measures in identifying the relevant end-user; and (iv) the potential impact on user privacy.

Lack of detail regarding how to balance principled-approach

However, while the Head Terms encourage regulated service providers to consider these factors at a principles level, the current draft of the Phase 2 Codes (including the Head Terms) do not specify *how* organisations are able to balance those principles of proportionality, privacy, human rights, accuracy and other matters with the underlying objective of the OSA to preserve the online safety of end-users.

Aylo is concerned that the concessions above offered under the Head Terms and principles-based approach are superficial and insufficient in their current form to ensure that user privacy, data security, freedom of expression are achieved while implementing the contemplated age assurance measures. The Phase 2 Codes do not offer industry participants any concessions or exceptions when attempting to balance those principles with their specific requirements under each schedule (i.e. the DIS Code), nor do the Phase 2 Codes prescribe or offer practical guidance on how regulated service providers can practically balance those issues.

Instead, the Head Terms places the onus on each industry participant "*to be able to demonstrate that the compliance measures it has adopted are reasonable*" (see section 5.1(b) of the Head Terms). This creates a disproportionate burden on industry participants who must show how they have effectively balanced those matters listed in that section. The technology agnostic approach

of the Phase 2 Codes contributes to significant uncertainty for industry participants.

Lack of clarity regarding age assurance measures in achieving principles

The Phase 2 Codes have not committed to either a platform-based or device-based approach to age assurance. While the Phase 2 Codes are outcomes-based (per the eSafety Commissioner's position paper), the Phase 2 Codes drive at improving online safety through age assurance methods despite the lack of clarity on the technologies and methodologies that industry participants can undertake to achieve such objectives while balancing principles of user privacy and data security. However, the platform-level (also known as "site-level") age assurance measures which are deemed to be appropriate under the Phase 2 Codes will actively prevent any successful outcome from being achieved, and fails on both objective fronts. As is clear from the documented outcomes from **every** jurisdiction where platform-level age assurance measures have been implemented, such measures are grossly inadequate in terms of their effectiveness to preserve the online safety of vulnerable end-users. Instead, these measures introduce greater harms to users' privacy and data security and compromise the privacy and security of the very people they are intended to protect.

Aylo's view is that the lack of any mandatory requirement to implement device-level age assurance measures creates a significant risk to the principle of user privacy and data security in the event certain industry participants deploy platform-level age assurance measures. Platform-level assurance measures require users to share their personal information repeatedly with every operator of an age-restricted site or platform. These models run contrary to principles of data minimisation championed in the Discussion Paper which provides that "*age assurance should be both effective, privacy preserving and data minimising*".

The lack of clarity under the Phase 2 Codes and the suggestion that platform-level age assurance measures are appropriate gives rise to the possibility that "honey pots" of personal information may be held by a vast number of providers, some of which may not have in place robust security measures to protect such information. This regulatory approach is likely to be highly attractive to cyber criminals who may prey on unsophisticated industry participants with poor cyber security hygiene, or establish fake adult website specifically to harvest valuable identity data. This may create a greater risk of data theft, fraud and online scams contrary to the objectives of the OSA. The kinds of personal information that is necessarily collected while undertaking age assurance may constitute sensitive personal information under the Privacy Act 1988 (Cth) given that an individual's sexual orientation and practices may be inferred using information that is held alongside the personal information, such as the title of the service or type of content provided.

As noted above, these privacy risks are further exacerbated by the fact that many organisations providing adult content may not have adequate resources to ensure the security of users' personal information or may otherwise use such personal information for purposes that are in breach of Australia's privacy laws. This is reflected in users' views — market research conducted for regulatory agencies found that 52% of respondents were "worried [their] data will not be protected" when engaging in age assurance measures to access adult material and that "trust in

the practices of pornographic sites is very low, with those who use them tending to have the least trust". [1]

In conclusion, Aylo submits that the Phase 2 Codes do not strike the appropriate balance between data security, user privacy and online safety. We submit not only that the Phase 2 Codes are ineffective in achieving their stated purpose of "establishing appropriate safeguards for the community", but also that the *outcomes-based* drafting of the requirement to implement appropriate age assurance measures will significantly negatively impact individuals' data security and privacy.

Case studies highlighting the ineffectiveness of site / platform level age assurance

Aylo would like to share relevant experience it has had applying certain age assurance measures in practice to inform the Industry Associations' in developing a nuanced understanding as to the appropriate age assurance approach and solution that must be adopted in Australia. In the below case studies, Aylo highlights its material concerns about site / platform level age assurance, the failure of other jurisdictions' attempts and trials of site or platform-level age assurance, and the clear detrimental impact these measures have on user privacy, data security, and freedom of expression.

More specifically, we would like to create an understanding of the fact that any effective age assurance solution needs to find an answer to the inherent risk of most (but not all) age assurance solutions: the simple re-direction of traffic to non-compliant sites. Given the enormous and constantly growing magnitude and geographic ubiquity of sites with adult content, one of the most critical features of any age assurance solution is to avoid such re-direction of user traffic to non-compliant sites. As we will show, any system that remains confined to age assurance on site-level, will be ill-equipped to deal with that challenge – as a meaningful compliance and control of all relevant adult content sites will hardly ever be achievable.

Results of Voluntary Tests conducted in France

In 2022, Aylo voluntarily tested the implementation of some standard site-level based age assurance solutions in the French market. The objective of these tests was to examine whether users would be willing to undergo a site-level based age assurance process in order to visit the well-known and trusted website "Pornhub" or whether users would rather be deterred by such age verifying measures and instead find another site which did not implement those measures.

The testing process was robust and comprehensive, and Aylo collaborated with four independent age assurance providers (Yoti Ltd., Very My Age of Verify Ltd., Agechecked Ltd, and AuthenticID Inc.) in undertaking the following measures: (1) hard identifiers based on user's official IDs, (2) age assurances via digital identity documents, (3) age assurance via facial or voice age estimation

[1] Ofcom. "Adult Users' Attitudes to Age Verification on Adult Sites," Executive Summary, 20 October 2022. https://tinyurl.com/574z4yrk

based on Artificial Intelligence, (4) the use of credit cards, or (5) the age of their email address. Some of these measures are endorsed in the Phase 2 Codes.

Despite the wide range of available methods to assure the age and despite Pornhub's high profile and attractiveness for users, the tested users **only assured their age in less than 0.5% of around 6.3 million sessions conducted**. In other words, the implementation of any of these (site-level-based) age assurance solutions **effectively drove all users away to other sites**. The outcome of the test thus clearly illustrates the users' overwhelming and strong reluctance to undergo site-level age assurance measures to consume adult content offered from a specific – even the best-known and most trusted – website.

The data recorded shows that the vast majority of the users exited the site even well before the actual age assurance was to take place. In total, **98.8% of users did not even make it to the point of starting the age verification process on the site**.

These findings are supported by a June 2020 IFP survey of 1020 French users of adult content websites which raised the following query: "*How will you react when you try to access a pornographic site that is either blocked or restricted by a mandatory majority verification system?*". The by far most common response, which fully aligns with our observations, was *"find a site that is not blocked or that does not require age control"* (64%). The second and third most popular responses were to *"bypass the [age verification] system,"* either by using VPN clients (41%) or by changing DNS settings (31%).

Louisiana: Age Verification Tied to the State's Electronic ID

In 2023, in the U.S., the State of Louisiana passed a law requiring websites that contain *"a substantial amount of adult material"* to implement age assurance in the form of an identity check. This age check is linked to an "**LA Wallet**" (i.e. Louisiana's electronic state ID). The LA Wallet is a well-established electronic ID integrated into the public legal system and widely recognised by Louisiana residents, who have been using it for various services for many years. Aylo implemented this age assurance solution on its sites.

However, despite citizens' level of familiarity with the LA Wallet and the general acceptance of this digital ID scheme in Louisiana, only a marginal number of users were willing to undertake this age assurance process on Aylo's sites. Instead, users preferred by a great majority to migrate to any of those many sites that were available without applying the age assurance solution required in the State of Louisiana.

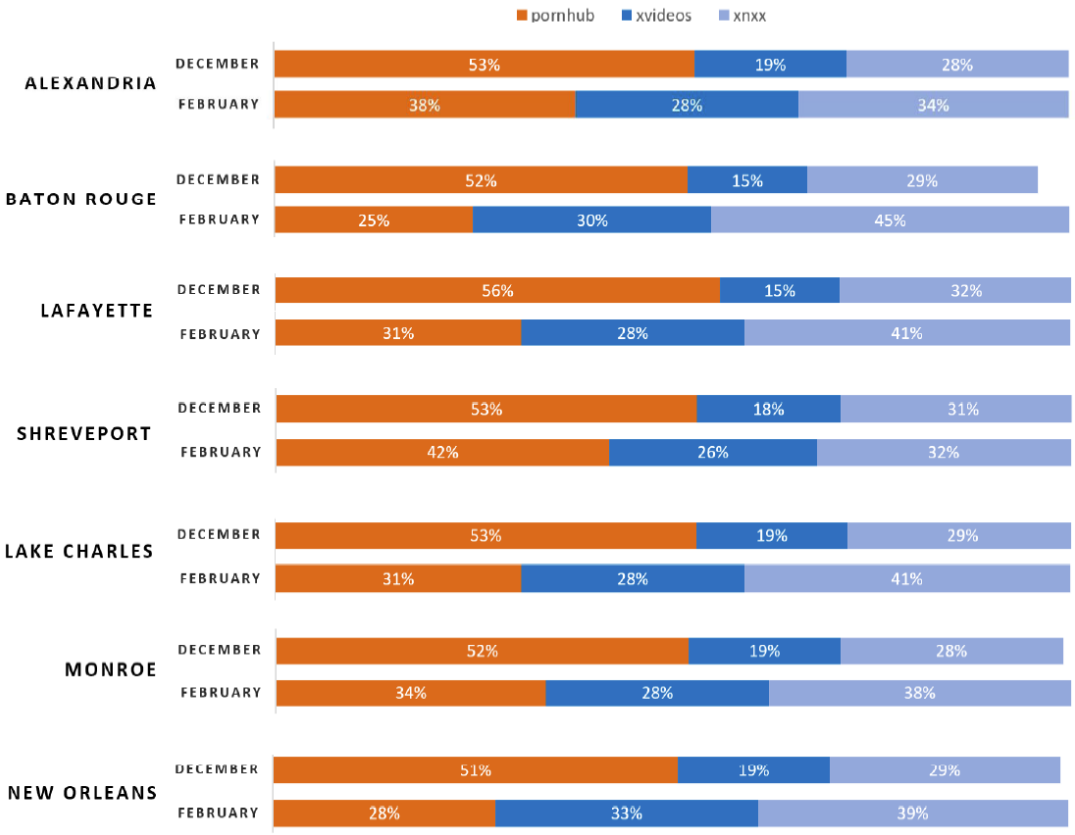
In concrete numbers, between the effective date of the legislation on January 1 and February 28, 2023, a total of 4,324,438 visits from Louisianan users took place on Pornhub in which the user was only granted access to the website after passing the age assurance process. **Out of these approximately 4.3 million visits, only 199,329 sessions (4.6%) included the completion of the age assurance process, while the overwhelming majority of users (95.4%) left the website without doing so.** Further, these findings are supported by the analysis of Google search results and related information (so-called "Google Trends") as well as evaluations by

Google Analytics and we understand these metrics are exceptionally reliable.

Compared to the status quo ante (before implementing hard site-level age assurance requirements), page views, which means the number of every (re-)load of the website as opposed to sessions and search queries of Aylo's content sites, have dropped dramatically.

At the same time, we observed that the demand for online consumption of adult content has not decreased. Rather, it appeared that users who refrained from undergoing age assurance measures, instead of refraining from looking for adult content, simply switched to other websites displaying such content. The fact that other websites, due to the absence of such extensive protective measures as Aylo's websites, present significantly higher security risks and offer infringing and potentially severely damaging content did not dissuade the users from making this switch.

The dramatic change in the users' preferences after implementing the age assurance requirement on Pornhub in Louisiana is also illustrated by the shifting interest distribution between these three websites in the various metro areas of Louisiana, which all demonstrate the same development:



Today, 23 months after the new law went into effect in Louisiana, only a handful of other adult websites are in compliance as well. As a result, the user numbers of Aylo's adult websites have decreased by around 80%. Until the legal situation changes, the return of these users is ruled

out due to a combination of three circumstances:

- the users' overwhelming natural reluctance to undergo any sort of (at least perceived) verification process right before entering a website designated to display adult content;

- the everlasting demand to consume such content (and, therefore, the constant emergence of new non-compliant websites filling the gaps created by established websites not being freely accessible anymore); and

- the authorities' natural inability to enforce the legislation against all of the tens of thousands of adult content websites available worldwide, let alone without any delay during which at least most are freely accessible.

Against this background, the only effect this legislation, based on our observations, so far has had, and will likely have in the future, is the displacement of users from established adult websites offering comprehensive safety measures and content moderation to such websites operating in a different way.

Circumvention of Enforcement Measures (Germany)

Around the year 2020, the media supervisory authorities in a certain German State (North-Rhine-Westphalia) mandated another operator of an adult content site to implement strict age verification measures on their site directed at German users. Given the anticipated reaction of most users to such measures (to shy away from such verification processes and to migrate to other sites), that other site operator circumvented any enforcement attempt by this German State Media Authority – by changing the URLs at which its German site can be visited.

We mention this incident as it illustrates the strong forces at play in circumventing typical age assurance solutions. This is a relevant point to keep in mind when evaluating different systems regarding their ability not to instigate such circumvention as we could witness in Germany.

3. Question 3 – Age Assurance

3.1. Where Age assurance measures could be introduced

The Discussion Paper raises the following query under Question 3(a):

> *Where should age assurance measures be introduced in relation to these Codes? Should users of email, messaging services and other types of private communication services and file storage services be subject to age assurance or other kinds of measures that restrict access to content?*

In light of the above, Aylo submits that ecosystem and device-level age assurance methods must

be prescribed as the only appropriate or approved age assurance methods that should be implemented by service providers who are subject to the Phase 2 Codes, including Designated Internet Service ("**DIS**") providers.

As part of this approach, it should be mandatory for operating system ("**OS**") providers to generate an age signal or other mechanism to be provided to other service providers.

Section 5(c)(vi) of the Head Terms contemplate a number of age assurance measures which are considered "appropriate" for the purposes of the Phase 2 Codes. For reference, these measures include:

- matching of photo identification;
- facial age estimation;
- credit card checks;
- digital identity wallets or systems;
- attestation by a parent or guardian of age or whether an Australian end-user is a child; and
- age assurance measures implemented by another party and confirmed by an 'age signal' or other mechanism provided to the service provider.

The DIS Code proposes to apply a number of age assurance obligations on regulated industry participants under the DIS Code (e.g. providers of "high impact class 2 DIS").

In light of the proposed regulatory framework, Aylo's response to this question of *where* age assurance measures should be introduced is covered in two parts: (i) age assurance measures, including participation in the scheme that results in the age of end-users being verified before accessing a service, should be rolled out to *all* participants in the online services industry on an ecosystem-wide basis; and (ii) age assurance mechanisms should be focused at the device-level.

However, before turning to the proposed ecosystem-wide and device-level approach, Aylo has set out its high-level views on the proposed age assurance measures under section 5(c)(vi) of the Head Terms, in particular those measures involving: (a) the matching of photo identification / official identity documents); (b) facial age estimation such as face scans; (c) proxies for official documentation such as credit card checks; and (d) digital identity wallets or systems. Aylo would be pleased to provide further detail on its views regarding any of these proposed age assurance measures if that would be beneficial.

Official Identity Documents (matching of photo identification)

This age assurance method of "matching of photo identification" presumably involves end-users providing verified identity documents (e.g. passport or drivers' licence) to prove their age. If this age assurance measure is deployed at a site or platform level in an online environment, this creates substantial risks of data retention and misuse of user data, as the verifier / website operator could simply retain the identity information for an unlimited period of time and share it with third parties for unknown purposes.[2] Several studies foresee that this age assurance method exposes users to significant identity theft risks and related data misuses of severe relevance.[3] The risks are, of course, exacerbated when deployed at scale across thousands or even millions of sites with potentially dubious security measures.

Facial age estimation

The Phase 2 Codes propose the use of facial age estimation measures, which we understand involves the use face scans which is an age estimation method that analyses a person's facial features to estimate a person's age, either based on a shared live image or video or on analysing an existing picture. These techniques are used to estimate rather than verify age. Accordingly, there will always be a rate of error and carry a potential for biases in the training dataset to produce inaccurate estimation results (including by approximating children as being close to the adult age threshold).[4]

Research studies further identify a high risk of privacy invasion and data fraud since face biometrics are sensitive information. If deployed at a site or platform level, it would be possible for a malicious actor to set up a fake age assurance process aiming at stealing users' facial images to generate deep fakes of the leaked data to facilitate impersonation or blackmail to the user of a pornographic website to reveal their identity or compromising photos or video.[5]

Credit card checks

We understand that the age assurance measure of credit card checks involves checking the

[2] See Mohammed Raiz Shaffique and Simone van der Hof, "Research report: Mapping age assurance typologies and requirements", published by Centre for Law and Digital Technologies (eLaw) Leiden University, The Netherlands on 19 April 2024, available at this link: https://digital-strategy.ec.europa.eu/en/library/research-report-mapping-age-assurance-typologies-and-requirements; and Martin Sas and Jan Tobias Mühlberg, "Trustworthy Age Assurance?" published by the Greens / EFA cluster on green and social economy on 8 March 2024, available at this link: https://www.greens-efa.eu/en/article/study/trustworthy-age-assurance.

[3] Sas and Mühlberg.

[4] See eSafety Commissioner, "Roadmap for age verification and complementary measures to prevent and mitigate harms to children from online pornography" published on August 2024 (see pages 155-156), available at this link: https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf?v=1727348999839; and Hilton and King, page 16; and Sas and Mühlberg, page 64.

[5] See Sas and Mühlberg, page 54.

holder of the card against a financial database to confirm the card's validity and the person's age. There are significant privacy and security concerns that are ostensibly present in providing such financial information to website operators. The potentially harmful privacy outcomes are exacerbated if such checks are required to be completed repetitively at a site or platform level, which will result in the creation of honey pots of financial information vulnerable to cyber-attacks.

Digital identity wallets or systems

Age assurance measures involving the use of digital identity wallets or systems may rely on government developed electronic identification systems which involve integrating chips into electronic identity cards and issuing digital identities as digital representations of personal identity. Digital ID cards allow citizens to scan their ID cards via a reader device to provide a certificate presenting only the minimum required information.[6] Similarly, digital identities may contain various identity attributes (e.g., name, age, place of birth, citizenship, school and university, address, and more) and credentials (e.g., digital ID card, e-passport, e-degrees, or e-driving license).

If this measure is deployed at a site or platform level, several studies highlight the risks that hackers may target users via phishing attacks or man-in-the-middle attacks.[7] As users are required to scan a QR code online to be redirected towards an address where they can share their digital IDs and verified signatures with the service provider, attackers may alter such QR code and lead users towards their server to register the user's digital IDs and verified signatures.

Device-level approach

Aylo submits that device-level age assurance which involves age assurance being undertaken at the operating system or device-level such that an individual's age is typically confirmed only once per operating system / device / account should be expressly adopted under the Phase 2 Codes as the required method of age assurance, and is the **only** appropriate method of conducting age assurance that is effective at safeguarding children and preserving individuals' privacy and security.

This kind of age assurance is contemplated at a high-level through the requirement under section 5(c)(vi) of the Head Terms endorsing age assurance measures being "*implemented by another party and confirmed by an 'age signal' or other mechanism provided to the service provider*". Aylo understands this age assurance measure to involve the device sending an age signal to service providers, for example high impact class 2 DIS providers, who would enable entry only in response to a valid age signal or otherwise lifting a locally applied block on access to high impact class online pornography.

However, given the proposed drafting in the Head Terms and DIS Code requiring DIS providers

[6] See EDRi position paper, page 20.

[7] See Sas and Mühlberg, page 64.

to implement 'appropriate' age assurance measures, device-level age assurance is not mandatory and is only one of a number of potential options.

Aylo strongly submits that this device-level approach should be expressly and exclusively prescribed as the requirement which must be undertaken by all members of industry (i.e. by those operating systems and device operators who are responsible for sending such age signals, and by the platform operators who are responsible for receiving the age signal and giving effect to the service restrictions).

The appropriateness of this approach is specifically referenced by the eSafety Commissioner in its submissions to the Phase 2 Codes who provides that "*industry has recognised that the sharing of age signals within an ecosystem is an 'appropriate form of age assurance' at clause 5(c)(vi)(G) of the Head Terms ('appropriate age assurance measures applied… [by] the service provider in respect of another service').*" Further to the eSafety Commissioner's views, this measure is consistent with the above ecosystem-wide approach and enables age assurance to be achieved in a practical and privacy preserving way.

In terms of efficacy of achieving this device-level approach, the prevalent operating systems (who share 95% of the operating systems installed on devices worldwide) have already developed the relevant technology to readily provide device-level age assurance.

Compared to both platform and ecosystem-level age assurance models, device-level age assurance is likely to pose the lowest privacy risk as information is either:

- stored at the device level, without the need for the developers of such operating systems to retain any personal information on their servers; or

- only retained in as many cloud locations as the individual has separate devices or operating systems.

Note that the only information that should be stored, following an age assurance check, is either an over/under 18 status, or an age band (e.g. under 13, 13 – 16, 16 – 18, over 18). Identity or any data used to assure age, does not need to be retained.

From our experiences, recent scientific studies as well as discussions with relevant stakeholders such as government officials, device providers, and NGOs, we take away the following central advantages of a device-level approach:

- **Easier, cheaper, and more effective enforcement**: The central device-level solution dramatically simplifies regulatory oversight and enforcement. By turning to OS providers, regulators can focus on a few major entities rather than overseeing countless individual websites, dramatically reducing the effort required to monitor compliance with youth media protection laws. This is also thanks to regulators (or even private entities) being able to add

non-compliant websites to a "blacklist" instead of conducting lengthy proceedings against each individual platform, all while new non-compliant platforms are being established.

- **Easy implementation across multiple countries:** Besides being relatively easy and cheap to enforce, combined device and site-level based age assurance allows consistent and quick implementation across different regions. The technology already exists and can, through worldwide software updates, make an immediate impact.

- **Significantly lower psychological hurdles:** One of our key understandings is that even the most secure age assurance methods on a site-level basis are not trusted by users for psychological reasons. Due to the large number of sites and providers where site-level age verification would have to be carried out, users fear (not without reason) data leakage and the associated consequences. This especially applies to sites that offer particularly sensitive services such as gambling or adult entertainment.

- **Significantly lower risk of circumvention:** Another psychological aspect is crucial in this respect since it is much more likely that users will verify their age once when purchasing the device (or installing the respective software update) than every time they visit an age-relevant website. Consequently, implementing such site-based age assurance does not dissuade them from visiting compliant platforms and websites, dramatically reducing the risk of circumvention. The same goes for any risk related to using VPNs (applied to manipulate one's location and geographical point of access), which will hardly play a role when verifying one's age when registering the device.

- **Substantially mitigated privacy risks:** In addition, the device-based solution ensures that user privacy is maintained throughout interactions by eliminating the need for websites and platforms or a larger number of age assurance services to store users' age-related data. Thereby, this approach significantly reduces the risk of data breaches or unauthorised access. This also results from the fact that only relevant age-related information is shared with the website, rather than detailed personal data like birthdates. The process remains efficient and secure, with encrypted age verification requests and data exchanges limited to what is necessary for determining appropriate content display. Thus, a device-based age assurance is inherently privacy-focused and designed to minimise the exchange of personal data between users and third-party platforms.

Ecosystem-wide approach

Aylo's view is that all industry participants should be subject to age assurance and other kinds of measures that restrict access to potentially harmful content. There is a much wider net of exposure methods that lead to children experiencing potentially harmful or adult content through online services (other than adult content service providers).

It is well-established that a child is more likely to be first exposed to pornography on a social media

website or search engine.[8] The research evidences the fact that children are frequently exposed to pornography and other adult content by messaging apps, or otherwise during their daily media consumption (e.g. on a social media site, or search engine platform). The evidence shows that the risk of children being exposed to adult content – particularly accidentally – is greater for mixed-content sites. In light of this, the requirements for age assurance should either be greater or the same across all sites which carry pornographic material when applying a risk-based approach.

The eSafety Commissioner shares a similar view on the incidental or accidental access to harmful or adult content by children which is set out in its submission on the Phase 2 Codes where it provides the following:

> "*In the case of online pornography, a major consideration for these types of services is that if exposure to harmful or age-inappropriate materials occurs on these services it may occur inadvertently or on an unsolicited basis because of the way in which it is delivered (for example via an automatic mechanism like ads or news/activity feeds; or via an unsolicited direct message). As discussed in the Position Paper and the AV Roadmap, this type of incidental exposure may be more harmful than where an end-user actively seeks out certain types of material, as it may be unexpected and unwanted.*"[9]

The eSafety Commissioner has also provided that:

> "*Given that eSafety's research (referenced by industry on p. 7 of the Explanatory Memorandum) indicates that a significant proportion of young people have been exposed to online pornography via services like group chats and direct messaging, the current RES Code may not adequately address the risks of exposure which exist on these services.*"[10]

However, only a limited number of industry participants are required to implement age assurance measures.

Aylo supports the Phase 2 Codes' approach to adopt a level of flexibility in terms of the age assurance measures that may be developed and applied (i.e. by endorsing a number of "appropriate" age assurance measures). However, further to our submissions under section 2, it is not practicable for all industry participants to deploy such age assurance measures given the varying levels of privacy and data security sophistication and infrastructure and the widespread dissemination of personal information (including sensitive information) across the online environment.

To that end, Aylo submits that the Phase 2 Codes should prescribe the adoption of age assurance

[8] See UK Children's Commissioner, ''A lot of it is actually just abuse' Young people and pornography', dated January 2023, available at this link: https://assets.childrenscommissioner.gov.uk/wpuploads/2023/02/cc-a-lot-of-it-is-actually-just-abuse-young-people-and-pornography-updated.pdf.

[9] See eSafety Commissioner, 'Initial feedback on draft Phase 2 Codes received 3 October 2024'.

[10] See eSafety Commissioner, 'Initial feedback on draft Phase 2 Codes received 3 October 2024'.

measures via a centralised user account which connects with existing internet ecosystems and which accounts for differences across services. This is consistent with the eSafety Commissioner's submissions on the development of the Phase 2 Codes as well as the Phase 2 Position Paper which calls for *interoperable* age assurance within and between the technological ecosystem systems.

3.2. Question 3(b) – Information gathering requirements in the context of age assurance

The Discussion Paper raises the following query under Question 3(b):

> *What kinds of information gathering requirements and processes should be implemented by relevant industry participants to conduct age assurance?*

Per the above, age assurance should be conducted by Operating Systems / Device Manufacturers. This significantly limits the number of times that data must be shared to prove age. It also limits the information gathering to a very small number of entities who the public already trust with their data.

That said, age assurance can be performed by third party age assurance providers on behalf of Operating Systems / Device Manufacturers, to further limit distribution of personal information.

In terms of the specific age assurance methods required, we would simply recommend an approach that gives users several options of how they can prove their age through their operating system/device so that no adult user is locked out of legal content they wish to access.

4. Question 4 – Scope of Age Assurance Processes

The Discussion Paper raises the following query under Question 4:

> *Should all Australian end-users who engage with online devices or services generally be required to undergo age assurance processes, or only those Australian end-users who wish to access high impact services (such as, for example, services that have the predominant purpose of high impact pornography)?*

Further to our response under Question 3(a), Aylo's view is that all Australian end-users who engage with online devices or services should undergo device-level age assurance processes to protect such end-users against the inadvertent and accidental exposure to adult or other age-inappropriate content. The predominant purpose of the service provider is not determinative of the kinds of content that may ultimately be shared through the relevant service / platform.

Moreover, the probability of this risk is exacerbated by the sheer number of websites containing

some form of adult content[11]. Globally, there are an estimated four million websites hosting adult content and, given our experience with compliance rates in other jurisdictions, a very large number of these will remain openly accessible.

Furthermore, a platform-level age assurance process would result in users (including children) who are intent on accessing online pornography to simply take the 'path of least resistance' and visit sites which place no additional burden of access on the user. The consequence is that the number of users visiting sites which undertake measures to reduce online harms will significantly decrease and, conversely, the number of users visiting sites which do not adopt measures to reduce online harm will increase.

To further reduce the risk of harm to end-users when implementing device-level age assurance, one possible solution would be for adult sites to be blocked by default, akin to turning on parental controls by default, as opposed to an opt-in model that is currently used by operating systems. This would effectively block access to all dedicated adult sites once a software update from the operating system is rolled-out representing the highest level of protection for children. At this point, if a user then wished to access an adult site, they would be prompted to age verify their device/eco-system account (e.g. Google, Apple, Microsoft account) to remove the block enabling access to adult sites.

An alternative to the above global approach would be to verify all users' age immediately upon account creation (or on a rollout of the relevant operating system software) and by creating an age signal which can be read by site and platform operators.

A final alternative may comprise a combination of both approaches. For example, adopting a global block, and an age signal to enable access. We highlight that such age signals would be implemented by compliant sites and platforms that install technologies capable of reading the age signal. All other sites who fail to comply and implement a mechanism to read the required age signal should be subject to the block. In that way, active compliance will result in the ability for age-appropriate users to access the site / platform and not the other way around which would be result of any platform level age assurance measure (i.e. where sites who fail to comply would be visited the most).

If the above is implemented, we are confident that this would create a huge overnight shift in child protection.

5. Other considerations

The ecosystem-wide and device-level approach to age assurance which is advocated for by Aylo in these submissions will also assist industry participants to readily comply with their other obligations

[11] Ahmed, Faraz et al., "The Internet is For Porn: Measurement and Analysis of Online Adult Traffic," Michigan State University, 2016 IEEE 36th International Conference on Distributed Computing Systems. https://tinyurl.com/39bhaynv

under the Phase 2 Codes. For example, an ecosystem-wide would enable specific privacy settings, safety tools, age-tailored filters and account settings to be migrated across services. The interconnected approach is only achieved through the adoption of device-level age assurance measures.

An ecosystem-wide and device-level approach based approach to age assurance is supported by the adult industry, many mainstream platforms, and child protection NGO. It is vital that such an approach is followed, not only to avoid the proven failure of site-level age assurance, but to create a data minimal, privacy preserving, and effective solution to the protection of minors online. Platform-level age assurance measures are unlikely to achieve the purpose of the Phase 2 Codes, described in the Head Terms as establishing "*appropriate safeguards for the community in relation to certain types of seriously harmful material or material not suitable for children*".

The effectiveness of platform-level age assurance relies on an expectation that all or almost all adult websites will comply with the requirements. As previously noted, in our experience, it is very unlikely this will occur. We have seen several jurisdictions impose platform-level (also known as "site-level") age assurance mandates. Without exception, compliance is only met by one or a few adult platforms which: (i) have the relevant resources and technical capabilities to adopt such measures; and (ii) are committed to regulatory compliance and alert to the legislative obligations that apply to them; and (iii) prioritise the commitment to reducing online harm. While Aylo is committed to ensuring full compliance, there are many sites and platforms featuring adult content who unfortunately make up the vast majority, which are operated by organisations who do not possess the above resources, commitments, or priorities to reducing online harm. The result has been that, in **every circumstance**, children have still been able to readily access adult material online.

The relationship between platform-level age assurance measures and worse outcomes for children is noted by the International Centre for Missing & Exploited Children, which has stated that website-based age verification mandates "may inadvertently drive children towards more dangerous online environments, both on the clear and dark web".[12]

We appreciate the opportunity to contribute to this important process. We strongly support the use of device-level age verification as the only solution for effectively preventing children's access to adult material online while also preserving privacy and security. The reduction and prevention of harmful behaviour online, the spread of toxic content and the potential for adults and children to suffer harm on the internet is central to Aylo's values and to the operation of our business.

Yours sincerely,

Aylo Holdings S.à r.l.

[12] International Centre for Missing & Exploited Children, "Statement on Age Verification," 27 June 2024. https://www.icmec.org/press/statement-on-age-verification/