Aylo response to Ofcom consultation on Guidance for service providers publishing pornographic content

As a provider of adult content platforms, we would like to express our commitment to the trust and safety of the public, and our interest in the Online Safety Act to secure and regulate the digital space. We feel very close with the issues raised in this bill, such as child safety in the digital environment.

In this context, we would like to share our concerns on certain provisions which are highly unlikely to achieve their aim, and will in turn create serious unintended consequences.

The challenge of age verification requires a global solution to ensure that minors do not **access age-inappropriate** material online, wherever it appears, while respecting **user privacy**, ensuring **equitable compliance**, and avoiding unintended consequences.

Aylo has publicly supported age verification of users for years, but we believe that any law to this effect must ensure minors do not access content intended for adults and preserve user safety and privacy.

We believe that the real solution for protecting minors and adults alike is to verify users' ages at the point of access—the users' devices—and to deny or permit access to age-restricted materials and websites based on that verification*.

To date, Aylo has implemented policies that surpass those of any other major user-generated platform on the internet, including mainstream social media platforms. This includes not just the unprecedented step of requiring all uploaders to provide third-party verified government ID, but also partnerships and collaborations with leading non-profit organizations around the world.

The technology to accomplish this exists today. Many devices already offer free and easy-to-use parental control features that can prevent minors' accounts from accessing adult content without risking the disclosure of sensitive user data. These features simply need to be mandated to block devices by default, unlocked only by age verification by an adult on the device.

Device-based age assurance*

- **Global**: To access the internet, with very few exceptions, the general population uses a device powered with an operating system made by one of three companies – Apple (iOS), Google (Android), and Microsoft (Windows)

- **Existing**: Operating system companies already have the available technology and, in some cases, already know the age of a user, so user impact would be low.

- **Integrated**: Devices have integrated security to access them (passwords and biometrics) in the case of shared devices, the same is true for accounts or profiles. This is the best and most appropriate place to integrate controls on age restricted material.

- **Effective**: This solution would instantly and effectively protect children from age-inappropriate content, and could be rolled out worldwide overnight.

*Device-Based Age Assurance refers to any approach to age assurance where the personal information that is used to verify the user's age is either shared in-person at an authorized retailer, inputted locally into the user's device, or stored on a network controlled by the device manufacturer or the supplier of the device's operating system. Whether through pre-installed content blocking and filtering software, the disabling of web-browsing permissions, or other means, the user will then be prevented from accessing age-restricted content over the internet unless they are age-verified. To come to fruition, such an approach requires the cooperation of manufacturers and operating-system providers.

The inherent issues with site-based age assurance

The age verification challenge requires a comprehensive solution to accomplish 3 things:

1. ensure that children cannot access age-inappropriate content on the internet
2. while respecting privacy of users, and
3. ensuring fair compliance.

Unfortunately, the way many jurisdictions worldwide, including the UK, have chosen to implement age verification is ineffective, haphazard, and dangerous. Any regulations that require hundreds of thousands of adult sites to collect significant amounts of highly sensitive personal information is putting user safety in jeopardy.

Moreover, as experience has demonstrated, unless properly enforced (giving platforms the opportunity to choose to comply), users will simply access non-compliant sites or find other methods of evading these laws. This is not speculation. We have seen how this scenario plays out in the United States.

The volume of adult sites online is very high. In order to regulate such a huge number of sites, Ofcom must be resourced correctly with a robust monitoring and enforcement regime. As evidenced in other jurisdictions, the vast majority of adult sites will not comply with the law. It is our opinion that such mass regulation is impossible.

In Louisiana, a law (Act 440) was introduced in 2023, allowing the attorney general to investigate and fine websites that do not verify age. Pornhub was one of the few sites to comply with the new law. Since then, our traffic in Louisiana dropped approximately 80 percent. These people did not stop looking for porn. They just migrated to other sites, easily found on the first page of search results that don't ask users to verify age, that don't follow the law, that don't take user safety seriously, and that often don't even moderate content.

The most recent example of this is in Texas, where we blocked our sites on March 14, 2024. According to Top 10 VPN, demand for VPNs peaked between March 14-18 at 275% higher than the daily average over the previous 28 days. Similarly, when Utah introduced their age verification law in May 2023, on May 2, demand for VPN services surged by 847%.

In 2022, Pornhub tested a portion of traffic in France, mandating age verification at the site level with various verification providers. The following methods were offered:

- Digital ID
- Document scan with liveness test
- Facial Age Estimation
- Voice Age Estimation
- Credit Card submission
- Email Address verification

This testing found that over 99% of users subjected to a verification requirement did not verify their age. Our data shows humans will take the path of least resistance, making the transition to non-compliant sites easy.

Outcome

It is vital that the outcome of currently envisaged age assurance measures is studied heavily before implementation. The failure of site-based age assurance is already clear from other jurisdictions, it does not protect children and it introduces severe risks across the population. Whilst Ofcom plans to enforce against non-compliant sites, the sheer number of sites will make this task impossible to achieve any real effect. Conversely, compliant sites will haemorrhage users, and will cease to be viable, leaving the entire adult market to non-compliant and criminal sites. This is not a positive outcome for anyone.

Ofcom have been handed a law which is unfit for purpose with no chance of success. It is often said that doing something is better than doing nothing, or "we can't make perfect the enemy of good". As we have experienced, "good" will not be achieved, in fact greater harms will be created. Mandating age verification at the level of each website makes things worse for both children and adults. This "something" is worse than "nothing". However, we are not advocating for "nothing" and we have articulated a device-based age assurance approach that is simple to achieve, easy to regulate, cost effective, privacy preserving, and most importantly – effective at preventing children from accessing adult material online. Operating systems & device manufacturers must be urgently consulted by Ofcom to create a workable device-based approach that protects minors by default. This is not the adult industry shifting responsibility to others, we maintain that adult websites should post disclaimers and label their websites as restricted for adults. However, to achieve a complete solution, we propose a route forward that will truly create a safer internet for everyone.

If Ofcom proceed with a site-based age assurance regime them the results will be:

1. No meaningful protection for minors
2. Privacy and data breaches of adults' PII
3. Increased exposure to illegal material
4. Circumvention by VPN usage
5. Ineffective and unscalable monitoring and enforcement.

Operating systems/device manufacturers have the power, expertise, and technology, to implement device-based age assurance that will avoid all these issues and they should be encouraged to do so immediately, before the UK makes a very severe and irreversible error. Three companies. Apple, Microsoft, and Google, which govern the operating system on nearly all internet connected devices globally, hold the keys to solving this concern for all children globally, without any added risk to adults, and without any need for decentralized legislation and regulation. A single point of verification on the device can be the gate to allow access to none, or all, websites, apps, or content restricted for adults.