Public Submission
Restricted Access System - Online Safety Act, 2021

Nanodesign Pty Ltd

Stephen Gentle

0400 599 398

Tarragindi, Brisbane, Australia

I am commenting as an experienced software/electronics consulting engineer, who specialises in the development of communications systems (networking, microwave, satellite and fixed communications, military and civilian encrypted comms, etc.). In previous roles, I have experience in web development and applications software development.

Submission as follows (does not correspond to the questions in the discussion paper):

1. Protection of children from accessing adult content is primarily the responsibility of the parent/guardian

I think the entire discussion seems to be starting from an incorrect premise. I **do not** believe there is actually significant and *informed* community support for Government intervention or regulation beyond the existing classification system for the access of adult material, and the existing measures that sites like YouTube use to require accounts with a birthdate.

Parents have understood for years that adult and pornographic material exists on the internet, and that it's their responsibility to properly supervise children in their internet use.

The focus should be on empowering parents to better make choices to control what their children access online, and on guidelines for social media and other service providers, not on mandatory regimes controlling the access of information.

2. Age verification systems should generally be industry lead, and encouraged by guidelines, not regulation

While it's primarily the parent's responsibility to protect their children from adult content, sites like social media providers, YouTube, etc. have understood that it is good to provide flagging of age content, and require an account with a birthdate registered to access such material.

There may be scope to expand this to form an *industry-led* Code of Practice that forms guidelines for the restriction of adult material.

3. Web filtering should be an opt-in service that Internet Service Providers (ISPs) and cellular service providers can provide their customers

The **best** option is an opt-in web filter that parents can choose to have applied to Internet and mobile services that their children use. This need not even be mandatory for an ISP or telco to provide - in fact, it might be a point of differentiation for an ISP to provide this kind of service, which might incentivise them to provide it.

Websites that choose not to comply with industry-led guidelines for age restriction of material could then be blocked by these *opt-in* web filters.

This is the best middle-ground, keeping sites that Australian adults want to use on their own internet services free from having to block all Australians from accessing it if they don't want to abide by those guidelines. This means that this is the solution with the least red-tape, but just as likely to work as any other solution.

4. Even the best web filtering and access control systems will always tend to be fairly easy to circumvent

Unfortunately, there are no magical solutions to this problem though. VPNs and other systems exist for easily circumventing any kind of web filter or access control system that applies only to Australia. With different kind of access methods, people in Australia can access sites in Australia but appear to be accessing from somewhere else.

Such mechanisms obviously cannot be outlawed themselves, as they are required for many different legal reasons, for example, for connecting in to a workplace's private network for working at home.

5. It is a waste of time to do much more than ask for a birthdate, and if a site requires payment, check for a valid credit card

It's hard to understate the futility of doing much more for age verification. As was the case with point 4, it is generally easy to bypass systems by accessing sites from a different country by various means. Also, similarly to point 4, it would be nice if a good technological solution existed to solve this problem, but unfortunately no such magical technology exists.

Licenses can be taken out of parents' wallets and scanned in. Credit cards can be borrowed. Facial recognition systems can be fooled by holding photos up to cameras. Even two-factor methods where an app has to be opened on an adult's phone can be bypassed, because children often do have access to their parent's phones.

Again, it would be great if a magical technology existed that could fix this, but it doesn't.

6. Using biometric data is extremely inappropriate for age verification, or really *anything* online

The use of any kind of biometric data online is extremely dangerous, because such a system requires the collection of data that a person cannot change about themselves. This is different from a password, because a password can be edited if it is compromised. Biometric information, such as a face scan, fingerprint, etc. if compromised, is compromised forever. This is why systems like Apple's Touch ID or Face ID go to such measures to store this data in a special encrypted 'Secure Enclave' on the device, so biometric data is **never** transmitted even to third party software running on the device, let alone over the Internet.

Biometric data should **never** be transmitted over the internet, which rules out any kind of facial recognition methods or anything similar. It is too easy for hackers to intercept, people to fall to phishing attacks, etc.

Recommendations

1. There is no real reason that the current guidelines, classification system, access control methods are not sufficient for age verification at the moment.
2. Education of patents is probably the most important thing in protecting kids from adult content online. Parents should be reminded that it's their responsibility that children are **not** given unrestricted, unsupervised access to the Internet given that ways to bypass filtering or age verification systems exist, and that there's no magical technical solution to fix that.
3. An industry-led Code of Practice could be developed with guidelines for age-restriction of material
4. ISPs and mobile providers should be encouraged to offer opt-in web filtering. These opt-in filters could block sites that do not want to abide by regulations or a Code of Practice. This is actually as close as you can get to the **perfect solution**, because it does not place an unreasonable burden on providers of internet services that do not want to comply with regulations - they can just be blocked by these opt-in filters.
5. We should always keep in mind that there will always be numerous ways to bypass all sorts of age-verification, access control etc. so the conversation should always come back to the fact that it's the parent's responsibility to monitor their children's internet use.
6. Biometric data should **never** be used for anything that requires it to be transmitted over the internet.

Looking Ahead

As with adult material, as was discussed before, to create a system for the age verification of pornographic material, **the closest to perfect solution is opt-in internet filters offered by ISPs**. Unfortunately, like any system, there will be ways to bypass this, but it strikes the best balance.

The beauty of this system is that it doesn't require any personal or private material (such as biometric material, or anything linked to a Government ID) to be transmitted over the Internet for adults accessing legal content - because these sites would simply be blocked with the opt-in filter, and not blocked for a regular service. It also doesn't put up extra red-tape for web site providers.

Although there are flaws to such a system, I believe this is the least-flawed way of doing this, and the least able to be abused.

Therefore, my professional opinion is that an opt-in web filter from ISPs and mobile telephone providers should be the **core part** of this system.