Submission of Brendan Sherrin. (Personal Views only)

Read to the end, I'm suggesting a solution to the problem in answer 8.

Question 1:

Under the Online Safety Act 2021, the RAS will only apply to Restricted Material that is provided from Australia on a social media service, relevant electronic service or designated internet service, or that is hosted in Australia. What elements should be part of an effective system to limit access to that kind of material?

Answer 1:

Anything hosted in Australia is a very small part of the overall internet. Since Australia does not allow any websites containing content higher than R18+, most remotely spicy content is hosted offshore and has been for a long time.

Question 2:

Has industry experienced any difficulty complying with the Restricted Access System Declaration 2014?

Answer 2:

See Answer 1: Since everything's hosted offshore, in 10 years in the web hosting industry, I've only encountered one spicy site hosted onshore as part of my employment. I've never encountered the RAS system, which shows how much it's used.

Question 3:

Has the Restricted Access System Declaration 2014 allowed industry the flexibility to develop access-control systems appropriate to their business models?

Answer 3:

See answer 1, anything likely to be affected voted with their feet and went offshore so they didn't have to deal with it.

Question 4:

What is the nature of the impact that has been experienced by: (a) industry; and (b) the Australian public as a result of the Restricted Access System Declaration 2014? Have financial and administrative burdens been placed on service providers by the 2014 RAS Declaration? Have there been any indirect effects (for example, costs being passed on to customers or suppliers)? Please provide examples.

Answer 4:

If anyone is still left hosting spicy content in Australia, they'd have very low customer traffic. Soon as you encounter any form of blocking (paywall, slow loading page) most people generally just go somewhere else.

Question 5:

What factors should be considered when assessing the effectiveness and impacts of systems, methods and approaches to limiting access or exposure to age-inappropriate material?

Answer 5:

Can a 12 year old using a VPN get around this? Remember John Howard's flawed "Internet Filter".

I grew up bypassing access controls to the computer/tv. My children will even more so do this. Relevant quote "The internet interprets censorship as damage and routes around it"

Question 6:

What systems, methods and approaches do you consider effective, reasonable and proportionate for verifying the age of users prior to limiting access age-inappropriate material?

Answer 6:

Credit cards are out, search engine's are a thing so asking the age specific questions of yesterday no longer works. No one's going to connect to Australia.gov.au or put in their tax file number to gain access to a website etc. Someone will come up with an "unblock Australia" browser extension and it'll all be for naught.

Question 7:

Should the new RAS be prescriptive about the measures used to limit children's exposure to age inappropriate material, or should it allow for industry to determine the most effective methods?

Answer 7:

The government tried to filter the net before and it didn't work, let the engineers make the decision instead of bureaucrats.

Question 8:

Is there any additional information eSafety should consider in drafting a new Restricted Access System declaration?

Answer 8:

It won't make any difference since 99% of the stuff you are trying to block is hosted offshore. Facebook anti-vax videos = offshore, Tiktok videos of people self harming = offshore, X-rate video sites = offshore.

The only thing I can see that would make a difference is offering a clean feed vlan via the NBN. The NBN as originally designed allowed 4x VLAN's for different providers to the one customer address.

Utilise that existing idea/infrastructure to offer a government "child friendly" clean feed, the same way schools do with all the content filtering engaged. Since you're not affecting adults you won't have any civil libertarians up in arms.

Since it's vlan (virtual lan) based you can block all the vpn (virtual private network) traffic, external DNS providers and whatever other stuff you want to protect the children you want. It'll be there be default on each consumers connection anyway, which is "pro-choice/personal responsability". Sell it to the public as "clean feed for the kids", which'll also QoS (limit) their traffic so Netflix doesn't interrupt Dad's work video call.

Drawbacks: it might need new hardware if the capability has been lost from the original NBN design but this can be phased in over time. The same should be possible on the mobile phone front. iPad's require nomination as child/adult devices, the same should be true of mobile phones and set at the carrier end on purchase at the same time you're providing id for a sim card.