1 60 words or less

A seemingly well intentioned document that seeks to make the Internet a safer place for Australians.

Unfortunately, this determination draft is riddled with overly vague and subjective requirements made catastrophically harmful to Australian citizens by abolishing the ability to be anonymous online and forcing service providers to intercept and scan all digital communications for "unlawful or harmful" content.

2 Introduction

I am writing to provide feedback on the ‘Draft Online Safety (Basic Online Safety Expectations) determination 2021 consultation’ as published on the 8th of April 2021.

My name is Aidan Clarke, and I am a product manager who has worked for both Australian and US based technology companies for the last 20 years. I am a technology enthusiast and a staunch privacy advocate. I have been using the Internet almost since its arrival in Australia. I have built networks and security solutions for private organisations, the federal government and a state education department.

Over the course of my career, I have provided technology solutions to some of the largest online entities in the world such as Facebook, Apple, Amazon and Telstra. In the past, I have delivered IT security and computer forensics training to many organisations, including members of state police computer crimes squads tasked with investigating online crimes and paedophile rings.

I am a proficient user of online systems. On any given day, I will use between 2 and 20 different online identities to access a wide number of services. Of these identities, some will be directly linked to my real world identity, others will be pseudonyms, while others still will be what I would consider to be heavily anonymised. I do this, as I am aware that different parts of the internet carry different levels of risk, whether it be risks to the safety of my personal information, identity, finances, possible risks to my person or family, or anything else in between.

I am a father of two teenagers, and a step father to another two children.

2.1 Understanding and Experience

Generally speaking, I understand the desire to have methods to address the nastier parts of the Internet; hate groups, cyber bullying, revenge porn attacks on individuals, heinous content depicting the abuse of children, major crime syndicates and even terrorism.

While I have not been on the front lines of having to deal with these threats directly, my professional experience over the last two decades has seen me be closer to more of these kinds of environments than many Australians have been.

2.2 Summary

The Internet has become a core part of how we live our lives today. Each year that passes, there are fewer and fewer people or places that the Internet does not yet touch and connect.

While the desire to bring control and safety to the Internet is clear and understandable, I find the proposed determination lacks significant objective detail in most places, and tackles the two most difficult problems, encryption and anonymity in ways that will be more harmful to all in the long run.

With this as my pre-amble, I have broken up my concerns into two sections; personal and professional.

3 Personal Concerns

My experience as both a technology professional and a father to four children has given me a solid perspective on the challenges of ensuring the Internet remains a safe place for people to use, particularly those in my family. Given this background, following are my personal concerns with the determination as it stands today:

3.1 *“able to use the service in a safe manner”*

When the determination state that providers `“will take reasonable steps to ensure that end-users are able to use the service in a safe manner”`, it is not clear to me what this initiative thinks the definition of `“use in a safe manner”` should be:

1. This is not clearly defined in the draft.
2. Without more concrete definitions, it feels like this could me massively open to very subjective interpretation and possible abuse.

I will speak more to this in the professional section of my response

3.2 *“default privacy and safety settings of the children”*

In relation to section 6, item 3b, I am encouraged and supportive of the desire to ruggedise protections for children. I am wholly supportive of the sections that propose `“—ensuring that the default privacy and safety settings of the children’s service are robust and set to the most restrictive level;”`

3.3 *“If the service uses encryption”*

The elements in Section 8 outlining expectations on providers in relation to encrypted services I find alarming.

Specifically, the section stating `If the service uses encryption, the provider of the service will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is or may be unlawful or harmful.`

As mentioned in my preamble, I have had a closer than normal proximity to those involved in investigations into child abuse and the heinous material from my time training members of state police computer crimes squads.

Even armed with this knowledge, I feel strongly however that mandating every service provider to scan proactively for this and other such content, is simply going too far. My problems with section 8 can be summarised as follows:

1. I find the mandate for all service providers, requiring them to proactively scan all content, to be a major intrusion into the private lives of every Australian citizen, and the beginnings of a dragnet surveillance apparatus.

2. Given that the determination scope includes social media, and all email, messaging, sharing services and sms providers, the requirements requiring the scanning of all content would include almost all electronic communications used in modern day to day life.

(a) The requirement for service providers to intercept all end to end encryption to scan for unlawful content would systemically weaken the privacy and security of electronic communications for all Australian's everywhere.

(b) I am totally shocked that any part of the controls suggested in section 8 would ever be proposed as appropriate in a country with democratically elected leaders.

3. I feel this is the government outsourcing the back-dooring of encryption into all aspects of modern online communication.
4. Any attempts to interfere with the protections provided by properly deployed strong encryption never ends well.
5. History has shown that once these tools are in place they become:

    (a) very easy to abuse;

    (b) subject to pervasive pushes for small incremental additions to the types of 'thing' being scanned for;

    (c) Any such system has the tendency to grow to become a distributed pervasive surveillance mechanism.

6. I feel that police 'use' (or 'misuse') of these facilities is almost guaranteed, as seen by recent state police uses of COVID check-in data as a tool to investigate crimes, which was certainly not the intended use of the systems that were build or the data that was collected:

    (a) Once the ability to scan and report on user owned content is enabled, the likelihood of the police gaining access to the tools or the scan results for reasons NOT related to scanning for the content types listed in item 11 is almost guaranteed.

3.3.1 Special note on Section 8 and any measures involving encryption:

There are very important lessons from history that should be heeded when authorities talk of steps or actions to weaken or bypass the security afforded by the use of strong and properly deployed encryption systems.

History has shown that eventually, the interference leads to significant problems.

A somewhat recent example of this is visible in new reporting on the implications of the US NSA's interference with encryption standards back in the early 2000's.

- A picture is now emerging through the media with evidence that the NSAs deployed encryption weakening methods and tools in the Dual Eliptic Curve (DualEC) encryption standard.
- The introduced weaknesses were subverted and used against the USA by foreign nations.
- The abuse of these weakened encryption systems is now thought to be linked to some of the worst security breaches in US government history.

Generally speaking, strong and properly deployed encryption is one of the bedrocks of Internet security and safety, and when done properly, it works really well.

Don't mess with this please…

3.4 “reasonable steps regarding anonymous accounts”

The requirements surrounding controls associated with the use of anonymous accounts in section 9 run counter to my experience using services very safely with a varied level of anonymity online.

3.4.1 Family protections

As mentioned in my preamble, I use a myriad of online identities as part of my standard safe usage of the internet. There are a large number of completely reasonable and legal reasons I use pseudonyms, partial or fully anonymous accounts. This does not just stop with just my own usage:

I strongly encourage my children to use anonymous accounts when accessing online services. We do this:

1. as part of our family toolkit to ensure the safety of their real identity against nefarious actors online;
2. to ensure that they can learn how to interact online in a way that will not punish them in later life for mistakes made as a minor.

It is common practice in my household for my children to annually delete their anonymous accounts from the year prior and start a new one.

This process is designed to ensure that the online profiles for their REAL identity, and the attached reputations that we know will become so critical in later life, do not become disproportionately tainted by honest (and totally expected) mistakes made while simply being a child growing up in an online world.

3.4.2 Community Protections

In addition to the family reasons that we regular users of anonymous online personas, there are very good reasons that the ability to access online services, communities and platforms in an anonymous fashion need to be protected:

1. People struggling with any aspects of life need ways to seek help, information, and find supportive communities safely without fear of being identified. The NUMBER ONE way to achieve this often is through the use of anonymous accounts for online platforms.
2. Anyone who wants to legitimately engage in debate or social discourse that is, by its very nature progressive or conservative, should be able to do so without fear. After all, how do we decide that an existing law is unjust or needs amendment if people aren’t able to challenge the status quo in a safe way?

3.5 “reasonable steps to prevent access by children to class 2 material”

With two teenage sons, and two younger step children, I can certainly understand the desire to prevent children being adversely affected by exposure to inappropriate content, such as Class 2 material. My simple response to the proposed requirements is that based on my experience, they simply will not work.

It has been my experience that curious children will ALWAYS find ways to satisfy their curiosity.

It is my experience as both a provider of network security solutions and as a father that any requirements for age verification systems simply won’t work:

1. Children will simply use a myriad of other mechanisms to gain access to this kind of content.
2. Short of a complete content censoring system akin to the “Great Firewall of China”, these systems will be trivially bypassed.
   (a) I have first hand knowledge of this gained from building network and security solutions for schools, and for the family home.

If we were to mandate an age verification system for any Australian users, one could reasonably assume we would expect offshore content providers to implement this for any customers arriving to their site from Australia.

Given the ease with which an Australian can connect to a site via an infinite number of systems or services that mask the original source of the traffic:

1. These age verification systems will be trivial to bypass by anyone in Australia who does not wish to participate.
2. I fear that these requirements will only give parents who are less savvy a false sense of security on their children's actual ability to access Class 2 material.

Additionally, my experience as a father has shown me that any attempts to lock all adult content away from children runs the risk of causing an outcome that is the opposite to the desired effect, making the concerning adult material even more mysterious, intriguing and sought after.

Having been through this with two children already, and being prepared to go through this with two more step children, my feeling is that the **only** way to combat the ill affects of children's potential access to **any** kind of inappropriate material (Class 2 or otherwise) is for families to handle this inside the family unit itself.

We have tackled this in our family with education, mature conversation with teens at times that we as parents deemed appropriate. We have had candid discussions of what these types content are, and are not, and ongoing support in our children's individual growth journey to adulthood.

Additionally, given that teenagers will always find a way to bypass or avoid age restrictions, the suggested age restriction controls will only serve to lump legitimate and age appropriate users of these systems, services and content providers with the need to firmly identify themselves to the content providers.

This, I find to be an inappropriate and scary side affect of the suggested solutions that I feel must not be ignored. These are legal systems providing legal content to legal adults. I do not feel you should have to identify yourself remotely in order to access them.

On a positive note however, I applaud the encouragement for content providers to `"conduct[ing] child safety risk assessments"`, but again need to point out that there is little or no tangible guidance or structure on how exactly this should be done. I will speak more on this point in the professional concerns section of this response.

4 Professional Concerns

Following are the concerns that I have if I look at the proposed determination through a professional lens

4.1 Who this determination applies to: "Purpose of this Part"

In reading through the determination and the linked legislation, the defined targets of the determination will likely sweep up a large number of Software as a Service (SaaS) providers like the one I work for currently.

1. Defining the difference between a "facebook" and a SaaS provider with online chat capabilities will be very difficult.
2. These requirements are only for systems accessed by people located in Australia. For SaaS providers both overseas and in Australia (Startups in particular).
   (a) this will force a large burden on these providers and startups as they could potentially have to double their infrastructures to satisfy different requirements for on and offshore usage.

3. These requirements completely fail to take Business to Business providers into account.
   (a) In a B2B online platform, the business customers of these systems who then make them accessible to end users would typically be better placed to address the spirit of the requirements I feel the determination is trying to achieve.
4. The majority of the requirements are, to put it bluntly, *wishy-washy*. To quote Justin Warren from Electronic Frontiers Australia, who points out many of the requirements lack "clear definition and objective thresholds for competence".
   (a) This applies to *many* of the requirements, including the core tenet
   (b) There is a lack of detail defining an objective and measurable outcome for what it means to `"ensure that end-users are able to use the service in a safe manner."`
   (c) This *also* applies to what and how, in particular, should be assessed in the recommended risk assessments.
   (d) As someone who would be required to map out my employers compliance to requirements such as these, I simply could not write a set of requirements to give to my engineering teams with the proposed level of definition.
   (e) I simply could not define "what success looks like" under the current draft.

4.2 Australian Innovation, startups, small businesses and technology giants

The majority of the requirements in this determination will limit the ability for small organisations (i.e.: those who are not Facebook/Apple/Telstra) to get off the ground.

1. All of the requirements in this determination are applied regardless of organisational size.
2. The requirements in this determination could be financially crippling for startups and small businesses.
3. These overly restrictive requirements will dampen if not weaken the ability for innovation and growth of technology based products from Australian innovators.
4. A major side effect of these kinds of regulations, when applied to small businesses, the burden of the compliance to regulations can be so heavy that it leaves the small businesses with no alternative but to rely on larger players, like Google or Facebook, to provide key systems and services that carry the overheads of the regulation.
5. Given the current concerns with the ever growing power of these technology giants, this might be counter to the desired effect.

4.3 Professional implications of “If the service uses encryption”

In addition to the elements described in my personal response on handling of encryption, the requirements outlined in Section 8 will mean that products made in Australia will not be able to deliver reputable hosted or SaaS services to Australians, or from Australian data centres.

For example, if I wanted to start a secure online backup service for consumers in Australia, I simply could not do this in a way that guaranteed the privacy of the end user’s backed up data AND complied with the requirements in this determination.

I could think of many more products and services that I could **never** be able to deliver in a trustworthy fashion from Australia as a result of this determination - This is a **major** problem.

Additionally, in my professional experience over the last few years, every time the Australian government enacts legislation that further interject into online systems, security, privacy or encryption, I have observed that it serves to significantly weaken the trustworthiness of Australian solutions to foreign customers.

Eventually, undermining the trustworthiness of encryption in any way will significantly impact our ability to sell Australian solutions overseas.

1. I have had to handle this first hand with overseas customers of technology products when the Assistance and Access bill was passed in 2018.

This point is significant enough to re-iterate again: Properly deployed strong encryption protects more than it risks, and is the bedrock of all trust online. This needs to be fiercely protected, not weakened.

5 Conclusion

While the noble goal of making the online world safer for individuals seems to be a straightforward task, the Internet’s size, complexity and popular dependence by people everywhere exposes this task for what it really is: a massively complicated and nuanced topic.

While there are a small number genuinely good elements in the proposed determination, it lacks maturity and is massively overshadowed by the catastrophic harms that would come from the approaches to encryption and anonymity.

In order to proceed, there is a great deal of input, consultation, analysis and communication required to move forward thoughtfully with the goal of developing a practical, objective and measurable set of requirements that carry the best chance of success and the lowest risk of harm to the Australian public.

Most of all, this process **must not** be rushed, it **must** provide greater opportunities for input from community stakeholders and subject matter experts, and **must not** be allowed to become a political football.