From: s 22
Sent: Wednesday, 5 April 2023 4:10 PM
To: KChinnery@afr.com
Subject: eSafety piece on AI regulation [SEC=OFFICIAL]

OFFICIAL

Hi Kevin, hope you're well.

eSafety Commissioner Julie Inman Grant has a punchy opinion piece about AI we thought you may be interested in given the paper's recent coverage: https://www.afr.com/technology/too-important-not-to-regulate-fears-over-irresponsible-ai-use-20230402-p5cxhg

As one of the key regulators in this space already, and an outspoken advocate for Safety By Design, Julie has some good insight into how industry will need to implement AI to prevent some of the harms being flagged.

Let me know if you're interested. We should be able to share a draft tomorrow.

Cheers, s

s 22
Senior Media & Communications Advisor

Australian Government | eSafetyCommissioner

s 22 s 22 esafety.gov.au

eSafety acknowledges the Traditional Custodians of country throughout Australia and their continuing connection to land, waters and community.
We pay our respects to Aboriginal and Torres Strait Islander cultures, and to Elders past, present and emerging.

From: Media OeSC
Sent: Thursday, 6 April 2023 3:21 PM
To: s 22
Subject: FW: Generative AI op ed [SEC=UNOFFICIAL]

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Thursday, April 6, 2023 3:20:55 PM (UTC+10:00) Canberra, Melbourne, Sydney
To: s 22 @eSafety.gov.au>; s 47E(c), s 47F @eSafety.gov.au>; s 47E(c), s 47F @esafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>
Subject: RE: Generative AI op ed [SEC=UNOFFICIAL]

Nice one. s 22

From: s 22 eSafety.gov.au>
Sent: Thursday, 6 April 2023 3:20 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 47E(c), s 47F @eSafety.gov.au>; s 47E(c) @esafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>
Subject: RE: Generative AI op ed [SEC=UNOFFICIAL]

Done. Thanks everyone. Will share with the AFR now. Fingers crossed … s 22

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Thursday, 6 April 2023 3:19 PM
To: s 22 @eSafety.gov.au>; s 47E(c), s 47F @eSafety.gov.au>; s 47E(c), s 47F @esafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>
Subject: RE: Generative AI op ed [SEC=UNOFFICIAL]

I think that is fair, accurate and would play to the world view of Fin Review readers…if you want to be "rhetoric free" , you could replace "behemoths" with "current industry leaders"

From: s 22 @eSafety.gov.au>
Sent: Thursday, 6 April 2023 3:17 PM
To: s 47E(c), s 47F @eSafety.gov.au>; Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 47E(c) @esafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>
Subject: RE: Generative AI op ed [SEC=UNOFFICIAL]

Thanks s 47E( ) and Julie.
What about this: "The commercial lure of a tech revolution potentially worth trillions is simply too great, not to mention the risk of disruption to existing industry behemoths which fail to invest and adapt."

From: s 47E(c), s 47F @eSafety.gov.au>
Sent: Thursday, 6 April 2023 3:04 PM

To: s 22 @eSafety.gov.au>; Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 47E(c), s 47F @esafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>
Subject: RE: Generative AI op ed [SEC=UNOFFICIAL]

I had two very small edits plus I am not sure this paragraph is warranted

The commercial lure is simply too great to think anything other than the familiar Silicon Valley mantra will prevail: "move fast and break things".

Concerns are two-fold:

a. It is a broad brushed reference and paints all tech companies as being irresponsible
b. While I expect there will be a commercial hook, not clear what the business model is at this point

My preference is to delete that sentence.

s 47E( )

From: s 22 @eSafety.gov.au>
Sent: Thursday, 6 April 2023 3:01 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 47E(c), s 47F @esafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>; s 47E(c), s 47F @eSafety.gov.au>
Subject: RE: Generative AI op ed [SEC=UNOFFICIAL]

Thanks Julie, we would need to get it to them pretty soon but await s 47E(c), s input.

s 22

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Thursday, 6 April 2023 2:53 PM
To: s 22 @eSafety.gov.au>; s 47E(c), s 47F @esafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>; s 47E(c), s 47F @eSafety.gov.au>
Subject: Re: Generative AI op ed [SEC=UNOFFICIAL]

I've just tinkered and am happy. I'm conscious this needs to go the editors. If s 47E(c), s 47F want to have a look, please do so quickly. I am comfortable with the content.

Get Outlook for iOS

From: s 22 @eSafety.gov.au>
Sent: Thursday, April 6, 2023 2:06:43 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>; s 47E(c), s 47F @esafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>
Subject: RE: Generative AI op ed [SEC=UNOFFICIAL]

Julie, I've given it a fairly radical rewrite. s 22 (and possibly you) are not going to forgive me but it's now down to 850 words, which is just about viable for an AFR op-ed: Generative AI Op ed by eSafety Commissioner Julie Inman Grant.docx

I've moved up the core argument – summarised as "determined action is needed (not just an open letter)". It's now near the top. We still have the sci-fi theme but it's scaled back and I've removed a lot of the detail that explains AI and goes over recent media coverage.

In this context, I think that's less valuable for us as readers can get that information from elsewhere, if they don't already have it. I'd argue the key message (and insight) from us is what we think should be done.

From: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Sent: Thursday, 6 April 2023 12:27 PM
To: s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>
Subject: RE: Generative AI op ed [SEC=UNOFFICIAL]

Removing s 22 and adding s 47E who confirmed her team is looking at the DISER paper. I think the nod to Minister Husic is a limited one and the perspective from what an independent regulator needs and what they think is likely to work is going to remain regardless of what the policy decision is...

My question is – are we going to pitch this today? I fear if we don't with the 4 day weekend ahead of us, we really may miss the window and things may have moved on.

Let me know what other input you might need from me.

Julie

From: s 22 @eSafety.gov.au>
Sent: Wednesday, 5 April 2023 5:31 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Cc: s 47E(c), s 47F @esafety.gov.au>; s 22 @eSafety.gov.au>; Media OeSC s 47E(d) @esafety.gov.au>
Subject: FW: Generative AI op ed [SEC=UNOFFICIAL]

Hi Julie,

Here's the updated draft op ed which now includes elements of your earlier email suggestions.

I'm off for a week and a half beginning tomorrow, so s 22 and s 47 have kindly offered to shop this to media on my behalf.

It might be worth checking in with s 47E(d) before it goes as she mentioned this morning that there may be movement on the Ed Husic front around AI that may need to be updated

Generative AI Op ed by eSafety Commissioner Julie Inman Grant.docx

Thanks

s 22

s 22
Assistant Director, Media and Communications

s 22

s 22

esafety.gov.au

eSafety acknowledges the Traditional Custodians of country throughout Australia and their continuing connection to land, water, culture and community. We pay our respects to Elders past, present and emerging.

From: s 22
Sent: Thursday, 6 April 2023 3:36 PM
To: psmith@afr.com
Subject: RE: eSafety AI piece [SEC=OFFICIAL]
Attachments: Generative AI Op ed by eSafety Commissioner Julie Inman Grant.docx

OFFICIAL

Paul, sending again. Apologies for the mix-up.

Rgds, s 22

From: s 22
Sent: Thursday, 6 April 2023 3:27 PM
To: psmith@afr.com
Subject: eSafety AI piece [SEC=OFFICIAL]

OFFICIAL

Hi Paul, thanks for your interest in this.

As you may know, Julie Inman Grant has been a leader globally in addressing online harms, both in her time in the industry with Microsoft and Twitter, and now as Australia's eSafety Commissioner.

Here she outlines the risks as she sees them, and argues measures of far greater weight then the recent Open Letter are required to reign in the AI juggernaut, possibly including mandating Safety by Design for all new related products.

Let me know if you're interested or need a shorter version.

Cheers, s 22

s 22
Senior Media & Communications Advisor

Australian Government | eSafetyCommissioner

s 22 s 22 esafety.gov.au

eSafety acknowledges the Traditional Custodians of country throughout Australia and their continuing connection to land, waters and community.
We pay our respects to Aboriginal and Torres Strait Islander cultures, and to Elders past, present and emerging.

To Regulate or Not to Regulate AI: That is not the question

By eSafety Commissioner Julie Inman Grant

Popular culture is littered with fictional dystopias where sentient machines go rogue, causing mayhem for humanity. Maybe there's a reason for that.

The powerful artificial intelligence systems unleashed on the real world by corporations recently (of which ChatGPT is just one) are not sentient – so far – but the threat they pose is genuine.

We've already seen reports of chat bots exhibiting sociopathic behaviour or generative AI creating false, highly defamatory claims, hyper-realistic deepfakes and even distressing child sexual abuse imagery.

This is what happens when appropriate detection capabilities and other guardrails are not embedded in these powerful tools from the start.

And it will take more than an open letter like the one we saw from Future of Life Institute – signed by thousands of tech industry luminaries last week – to stymie this AI juggernaut.

The commercial lure of a tech revolution potentially worth trillions is simply too great, not to mention the risk of disruption to current industry leaders which fail to invest and adapt.

Just like in the movies, we can't rely solely on good intentions. Only determined human action can restore the narrative order and reassert human values like truth, justice, democracy and, ultimately, ensure societal safety.

Unlike *Terminator*, however, our protagonist won't be a doomsday prepper with a gun. What's needed is something more mundane: a coalition of political leaders, technical ethicists, community groups, regulators, academics and other experts working to embed Safety by Design at the outset.

Existential threats to humanity aside, the everyday consequences of failure to address these challenges are deeply concerning.

Some experts have highlighted how conversational AI – where automated systems can engage individual users in flowing and coherent conversations – could be used to unduly influence via a pre-loaded persuasive agenda.

We tend to refer to this as "social engineering" but one of the scariest things for me is that these tools could soon open the door for much more persuasive forms of child grooming, sexual extortion and impersonation, alongside new forms of networked harassment and abuse.

We need to ensure that the fundamental user safety building blocks are applied with forethought and that safety interventions are constantly re-applied with each iteration. Open AI has a laudable safety charter, but we haven't seen evidence to date that these guardrails have been effectively applied.

So, the question many governments and regulators are grappling with now is not whether or not to regulate, but *how* to regulate.

Italy has been a first – and very decisive – mover by preventing ChatGPT from processing Italians' data, effectively banning the technology.

The European Commission has had an AI Act in the works for the past two years but it is not quite ready for implementation.

Just this week, US Federal Trade Commissioner Alvaro Bedoya warned the tech industry: “We have frequently brought actions [for deceptive trade practices] against companies for failure to take reasonable measures to prevent reasonably foreseeable risks.”

This echoed an important dialogue I had with Commissioner Bedoya late last year around Safety by Design and eSafety’s transparency powers as part of the Online Safety Act, and where similarities in our approaches lie.

For one thing, we all agree you cannot have accountability without transparency, and eSafety’s powers to issue legal notices under the Basic Online Safety Expectations have enabled us to compel some of important algorithmic transparency insights around recommender systems.

From a technical point of view, there are a number of algorithmic auditing techniques that could provide even greater windows of transparency – including code, API or scraping audits – but this will require a significant scaling of skills and capability.

As Australia’s online safety regulator, I do not believe that a ban would be effective or that post-facto regulatory action - after the damage has already been done – will put us in a better position. Indeed, we want to continue stimulating innovation and harnessing all the promise that AI has to offer too.

This is why eSafety has been so focused on working with industry and other stakeholders over the past five years to ensure that Safety by Design is a primary consideration in the development, deployment and refresh of any kind of technology.

To date, this has largely been a voluntary initiative to lift industry safety protections, share innovative best practices and enable better compliance with our laws, but perhaps we need to take a different tack?

Shifting the burden of proof onto technology companies to show they have taken meaningful steps to assess risks, understand potential harms and engineer out potential misuse before these products are released into the wild could make a decisive difference.

As eminent Professor of AI and NSW Chief Scientist Toby Walsh recently said to me: “Responsible design beats regulation.”

But what about a combination of both?

To that end, eSafety supports the Australian Government’s efforts, led by Minister for Industry and Science Ed Husic, to examine the range of potential regulatory issues around AI and algorithms, and we continue to work in tandem with other national and international platform regulators across issues and borders.

The current crop of large language AI models may not be hellbent on taking over the world and destroying us, but it doesn’t mean they don’t pose a critical threat to modern societies and democracies.

There is no question that Australia must move quickly and decisively. The end of this script is yet to be written but shaping our post-AI world will be entirely dependent on bold actions we are prepared to take today.

Op ed

SUMMARY AND APPROVALS TABLE		
For internal use: remove table prior to despatch		
CONTENT SUMMARY		
Lead writer/contact:	s 22	
Deliverable/title/ subject line:	NA	
Channel:		
Audience/reach and analysis:		
Strategic intent:		
Top key messages (3-4 only):		
Notes (optional):		
APPROVALS		
Deadlines:	Final approval required by:	Publication/go-live:
	Click or tap to enter a date.	Click or tap to enter a date.
Approvals tier:	Choose an item.	
Approvals pathway:	Approvers	Cc/for noting
(Add lines if required)	1 s 22 03/03/26	1. s 47E(c), s 02/03/26
	2. Heidi Snell	2 s 47E(c), /Richard Fleming
	3. s 22	3. s 47E(c), s
	4. Julie Inman Grant	4. Kathryn King
Final despatch:		

Codes op ed By Julie Inman Grant

A child cannot walk into a bar and order a drink. They cannot stroll into a strip club, browse an adult shop, or sit down at a blackjack table in a casino.

These safe boundaries are enforced not because we are prudish and over-reaching, but because we recognise something simple, profound and universal: children are not adults. Their future selves are still under construction.

Their emotions, judgment, identity, perceptions of relationships and consent, impulse control, and understanding of risk are far from fully formed.

And so, historically society has stepped in—not to control them but to guide and protect them until they are ready.

When it comes to the online world, however, these common-sense protections inexplicably dissolve.

It's not because the risks are fewer online. If anything the potential for harm is far greater.

A child who could never enter a physical adult venue can, within seconds, access pornography more extreme than anything sold behind the counter of a bricks-and-mortar adult store. They can stream high-impact violent footage far worse than anything they might see by sneaking into an R-rated movie. Violent pornography, including choking and strangulation porn, is widely available and is concerningly normalising harmful youth sexual behaviours.

That's not to mention the new wave of AI companion chatbots entrapping and entrancing impressionable young minds with human-like, sycophantic and often sexually explicit conversations, some even going as far as encouraging self-harm and suicide.

We have tacitly allowed the growth of a digital world that ignores principles and rules we enforce in the physical one.

From Monday, that is changing. Australia is drawing a line in the digital sand in the form of enforceable industry codes, which effectively take many of the protections applied to children in the offline world and installs them into the online one where seriously harmful content is concerned.

Known as the Age Restricted Material codes, these new rules cover most corners of the online ecosystem, from device manufacturers, gaming services and app stores to social media, messaging services, generative AI systems, websites and search engines.

These codes require the entire online industry to put in place meaningful protections preventing children's exposure to content they are not ready to see – and cannot unsee – such as high -impact violence, pornography, self-harm, suicide and disordered eating content.

These Codes complement rules already in place which deal with material like child sexual exploitation material, and pro-terror material.

Let me be clear, there is nothing in these codes to stop adults accessing legal adult material. Sites which provide adult material will be required to conduct privacy-preserving age checks but the precise methods are up to them. It is the protective outcomes that matter here.

The technical and business decisions are a matter for the companies. but I am confident they have the capability to comply because they wrote the codes, and develop and deploy the technologies that can provide such protections.4

Australia's Online Safety Act requires industry to develop codes about their online activities. It's the law. My role as eSafety Commissioner was to ensure that the codes industry drafted met "appropriate community safeguards" set out in the Act and to ensure industry meets their responsibilities going forward.

We know more and more young people are encountering age-inappropriate content unintentionally at a very young age.

Our own research supports this with 1 in 3 young people telling us that their first encounter with pornography, for example, was before the age of 13 and this exposure was 'frequent, accidental, unavoidable and unwelcome' with many describing this exposure as being disturbing and 'in your face'.

Consider how seriously we take age checks in the physical world. While these systems are not perfect, they are visible, deliberate, and socially expected. No one argues that asking for ID at a bar is an unacceptable burden on a business, or that the responsibility should fall upon the alcohol distributor.

Commented [s 22 1]: Shoutout to the previous Codes never hurts but could cut for length if needed

Commented [JG2R1]: agree

Commented [RF3]: This often gets missed, and we are seen as the originator of the codes and standards s 22 interested in your views

Commented s 47E(c) R3]: Agree. We need to say this loudly and often. Proposed adding a few words for readers who don't immediately connect 'Act' with 'law' (trust me, they exist).

Commented s 22 R3]: Very happy to emphasise this point as often as we can!

The entity that controls the entryway to the risky environment carries the duty of care. You control the room, you own the door.

The digital world, by contrast, seems to have taken a near-enough-is-good-enough approach to age checks with a "Are you over 18? Yes/No" often the only barrier between our children and this content.

For years, the dominant and often self-serving narrative has been that digital spaces are too complex, too global, or too technologically fluid to regulate in the same way as physical ones.

But complexity should never be used as an excuse for inaction. Financial systems are complex and global and yet we still regulate them. Pharmaceutical supply chains are complex and global and we still regulate them. We require almost every consumer good from cars to electronics imported into Australia to be built to our safety standards. Complexity demands innovation. Why should such technological exceptionalism continue to persist?

The same companies which say they're on the cutting edge of technology – and can target you with deadly precision for advertising purposes - also try to say that they can't possibly figure out if it's an adult or child is using their services for the purpose of applying safety measures – it just doesn't stack up.

Commented[s 22 6]: Feel free to delete - this is just a sentiment that has come up a few times recently in stakeholder discussions/other jurisdictions which I think is a good point to make

And I've also heard some argue that rather than regulate the internet to protect children, the answer lies in parents doing more to control what their kids access online. I can already imagine parents reading this with their heads in their hands.

While parents of course play a key role in digital parenting, we don't say that a parent's supervision alone should replace laws keeping minors safe in the physical world. If a 14-year-old sneaks into a bar and gets drunk, we don't write it off as solely a family matter. The business that allowed that child onto its premises and profited from serving that child alcohol carries a significant level of responsibility, too.

That also assumes that every child has a responsible and supportive parent to provide that safety net – which is sadly far from the truth.

So why should the world's biggest tech platforms - many of which generate enormous revenue from Australian users - be exempt from a similar responsibilityto protect children than what we expect from the local pub or cinema?

If we agree that a minor cannot enter an adult shop because of the psychological impact of explicit adult content they might encounter there, why is streaming explicit material to a smartphone treated as inevitable?

The idea behind these codes is that these principles should be consistent: environments designed for adults should not be freely accessible to children, regardless of whether they are built with bricks or code.

If we believe children deserve protection in the physical world, then it stands to reason they should deserve it online, too.

From: s 22
Sent: Tuesday, 10 March 2026 12:01 PM
To: Jeremy Sammut
Subject: RE: Age Restricted Material Codes op ed By Julie Inman Grant (003).docx [SEC=UNOFFICIAL]

Ok great, thanks Jeremy.

From: Jeremy Sammut <jeremy.sammut@nine.com.au>
Sent: Tuesday, 10 March 2026 12:00 PM
To: s 22 @eSafety.gov.au>
Subject: Re: Age Restricted Material Codes op ed By Julie Inman Grant (003).docx [SEC=UNOFFICIAL]

Yep will take thanks. jeremy

Jeremy Sammut
Associate Editor - Opinion. Leader Writer.

FINANCIAL REVIEW

T 0406122966
A 1 Denison St NORTH SYDNEY, NSW, 2055
E jeremy.sammut@nine.com.au

On Tue, 10 Mar 2026 at 11:54, s 22 @esafety.gov.au> wrote:

> Hi Jeremy
>
> Hope you are well.
>
> We thought this op ed from eSafety Commissioner Julie Inman Grant on the commencement of Australia's Age Restricted Material codes yesterday might be of interest to the AFR.
>
> This obviously follows on from extensive media coverage (including in the AFR) on the announcement by Aylo, the Canadian owner of the world's most popular porn site - Pornhub, that they have restricted access to paid subscribers only, in order to comply.
>
> If you decide it's not for you we'd just ask if you could let us know as soon as possible so we can shop it around elsewhere.

Thanks

s 22

s 22
Assistant Director, Media and Communications

eSafetyCommissioner

s 22

s 22

esafety.gov.au

eSafety acknowledges the Traditional Custodians of country throughout Australia and their continuing connection to land, water, culture and community. We pay our respects to Elders past, present and emerging.

Age Restricted Material Codes op ed

By Julie Inman Grant

A child cannot walk into a bar and order a drink. They cannot stroll into a strip club, browse an adult shop, or sit down at a blackjack table in a casino.

These safe boundaries are enforced not because we are prudish and over-reaching, but because we recognise something simple, profound and universal: children are not adults. Their future selves are still under construction.

Their emotions, judgment, identity, perceptions of relationships and consent, impulse control, and understanding of risk are far from fully formed.

When it comes to the online world, however, these common-sense protections inexplicably dissolve.

It's not because the risks are fewer online. If anything, the potential for harm is far greater.

A child who could never enter a physical adult venue can, within seconds, access pornography more extreme than anything sold behind the counter of a bricks-and-mortar adult store. They can stream high-impact violent footage far worse than anything they might see by sneaking into an R-rated movie.

That's not to mention the new wave of AI companion chatbots entrapping and entrancing impressionable young minds with human-like, sycophantic and often sexually explicit conversations, some even going as far as encouraging self-harm and suicide.

We have tacitly allowed the growth of a digital world that ignores principles and rules we enforce in the physical one.

But as of yesterday, this is changing. Australia is drawing a line in the digital sand in the form of enforceable industry codes, which effectively take many of the protections applied to children in the offline world for generations and installs them into the online one.

Known as the Age Restricted Material codes, these new rules cover most corners of the online ecosystem, from device manufacturers, gaming services and app stores to social media, messaging services, generative AI systems, websites and search engines.

They require the entire online industry to put in place meaningful protections preventing children's exposure to content they are not ready to see – and cannot unsee.

We're talking about high -impact violence, pornography, self-harm, suicide and disordered eating content.

These new Codes complement rules already in place which deal with material like child sexual exploitation material, and pro-terror material.

But despite their active involvement in writing the codes, we've already seen Aylo, the Canadian owner of Pornhub, announce it will only offer 'safe for work' content on its free services in Australia.

In order to access its more explicit content, the company says it will now move to age check requirements for paid, age-restricted services.

But this is a business decision for Aylo rather than a technical one. I am confident companies have the capability to develop and deploy the technologies which both protect children from age-inappropriate material and still allow adults to access this content.

Sites which provide adult material will be required to conduct privacy-preserving age checks but the precise methods are up to them. It is the protective outcomes that matter here.

We know more and more young people are encountering age-inappropriate content unintentionally at a very young age.

Our own research supports this with 1 in 3 young people telling us that their first encounter with pornography, for example, was before the age of 13 and this exposure was 'frequent, accidental, unavoidable and unwelcome' with many describing this exposure as being disturbing and 'in your face'.

No one argues that asking for ID at a bar is an unacceptable burden on a business, or that the responsibility should fall upon the alcohol distributor.

The entity that controls the entryway to the risky environment carries the duty of care. You control the room, you own the door.

For years, the dominant and often self-serving narrative has been that digital spaces are too complex, too global, or too technologically fluid to regulate in the same way as physical ones.

But complexity should never be used as an excuse for inaction. Financial systems are complex and global and yet we still regulate them. Pharmaceutical supply chains are complex and global and we still regulate them.

And we require almost every consumer good from cars to electronics imported into Australia to be built to our safety standards. Complexity demands innovation.

So why should the world's biggest tech platforms - many of which generate enormous revenue from Australian users - be exempt from a similar responsibility to protect children than what we expect from the local pub or cinema?

If we agree that a minor cannot enter an adult shop because of the psychological impact of explicit adult content they might encounter there, why is streaming explicit material to a smartphone treated as inevitable?

The idea behind these codes is that these principles should be consistent: environments designed for adults should not be freely accessible to children, regardless of whether they are built with bricks or code.

If we all agree children deserve protection in the physical world, then it stands to reason they should deserve it online, too.

From: Julie Inman Grant
Sent: Tuesday, 10 March 2026 1:44 PM
To: s 22
Cc: s 22
Subject: RE: AFR to run op ed [SEC=UNOFFICIAL]

great

From: s 22 @eSafety.gov.au>
Sent: Tuesday, 10 March 2026 1:20 PM
To: Julie Inman Grant s 47E(c), s 47F @eSafety.gov.au>
Cc: s 22 @esafety.gov.au>
Subject: AFR to run op ed [SEC=UNOFFICIAL]

HI Julie

AFR have said they'll run the op ed tomorrow, so we're holding off the blog version for now.

s 22

s 22
Assistant Director, Media and Communications

eSafetyCommissioner

s 22

s 22

esafety.gov.au

eSafety acknowledges the Traditional Custodians of country throughout Australia and their continuing connection to land, water, culture and community. We pay our respects to Elders past, present and emerging.