Submission

by

THE NEW ZEALAND INITIATIVE

to the Education and Workforce Committee

on the

Inquiry into the harm young New Zealanders encounter online, and the roles that Government, business, and society should play in addressing those harms

5 August 2025

Prepared by:

Dr Eric Crampton, Chief Economist
The New Zealand Initiative
PO Box 10147
Wellington 6143
eric.crampton@nzinitiative.org.nz

1. INTRODUCTION

1.1 This submission to the Inquiry into online harms is made by The New Zealand Initiative (the Initiative), a Wellington-based think tank supported primarily by major New Zealand businesses. In combination, our members employ more than 150,000 people.

1.2 The Initiative undertakes research that contributes to the development of sound public policies in New Zealand, and we advocate for the creation of a competitive, open and dynamic economy and a free, prosperous, fair and cohesive society.

1.3 The Initiative's members span the breadth of the New Zealand economy. The views expressed in this submission are those of the author rather than the New Zealand Initiative's members.

1.4 This Inquiry has been established in response to concerns regarding youths' experience with social media and consequent calls for compulsory minimum age requirements for access to social media.

1.5 This submission argues that:

1.5.1 Regulating social media requires defining social media. Doing so is harder than it sounds. Remember that if people enjoy being able to interact with each other, and are prohibited from doing so on one platform, many will shift to the next-best alternative.

1.5.2 Practicable ways of implementing a social media age limit would result in at least one of three undesirable outcomes. Systems may be easily worked around by those under the age limit; they may be cumbersome for users over the age limit; and, they may have pernicious consequences for privacy and for the potential for online pseudonymity.

1.5.3 On balance, one option could have less potential for adverse consequences than other alternatives. Google's Play store (for Android apps) and the iPhone App Store provide parental control options that rely on the date of birth provided when a child sets up their phone. Installing social media apps could require parental permission for users under the age limit.

1.5.4 If Parliament takes the option presented in 1.5.3, it should do so knowing that many youths will work around the restriction. Their inevitably doing so should not be taken as evidence that tighter restrictions are justifiable. Tighter restrictions have their own adverse effects.

2. DEFINING SOCIAL MEDIA

2.1 Everyone knows what social media is in the same way that everyone knows what basic foods are, when the conversation is about removing GST on basic foods. It sounds straightforward but quickly becomes a nightmare when tight legal definitions are required.

2.2 Australia's legislation considers a platform to be "age-restricted social media" if its sole or significant purpose is enabling social interaction and if it allows users to post material. Platforms with other primary purposes, like online gaming sites, would be exempt. YouTube was initially considered exempt, but that exemption is now in question. Most people use

YouTube to watch content. But it is possible to upload videos to YouTube and encourage friends to comment on them. Is it the primary purpose of the site? Almost certainly not. But a survey found minors have reported finding harmful content on YouTube, so on 30 July, the Australian government decided to remove the exemption.[1]

2.3 Chat groups within messaging apps can quickly be used for social media purposes if fifteen-year-olds are barred from accessing other platforms for communication. For example, sharing videos and photos is easily done with WhatsApp. Roblox is a gaming site that also enables user communication and may or may not be social media.[2]

2.4 Despite social interaction not being the primary purpose of a site, it could become the primary use of a site – if the site is an effective substitute for an alternative that has been prohibited to youths. If activities causing current concern on initially-designated platforms shift to undesignated platforms, there will be pressure for designation of those additional platforms.

2.5 Sites that facilitate user interaction but are not designated as social media may decide to remove or worsen chat functions to make them less hospitable as alternatives to designated sites, so they might avoid designation.

2.6 At a fundamental level, any website with any chat or interaction functionality could be considered social media. Comments sections on newspaper websites. Blogs and their comment sections. If talkback radio is hosted on the internet, could it count as social media? It facilitates interaction among two or more users; what a caller says on talkback radio could count as posting material on the service. Definitions are inherently fraught.

2.7 A Member's Bill in New Zealand is modelled on definitions used in Australia. It will have similar problems.

2.8 As the Australian legislation is not yet in force, it is hard to assess what further problems might be experienced. It seems premature to adopt their framework. Especially where their current framework seems more than somewhat vibes-based. Last week, under pressure to deem YouTube social media, Prime Minister Albanese declared, "I want Australian parents to know that we have their backs." YouTube would be considered social media. Whatever definition is set in legislation will not withstand parental pressure if other sites can be designated whenever the Minister "is satisfied that it is reasonably necessary to do so in order to minimise harm to age-restricted users."[3]

3. A SOCIAL MEDIA TRILEMMA

3.1 Leave to one side the very substantial problem of defining social media. Legislation placing liability on companies if they fail to prevent youths from accessing a designated platform seems inherently fraught.

3.2 An age verification system has three obvious failure modes. A system could be easily worked-around by those under the age limit. It could impose substantial hassle and cost on adults who will be required to prove that they are not under the age limit. It could also substantially erode

1 https://www.reuters.com/legal/litigation/australia-widens-teen-social-media-ban-youtube-scraps-exemption-2025-07-29/

2 https://www.theverge.com/policy/612577/roblox-kids-online-safety-legislation-social-media

3 https://www.reuters.com/legal/litigation/australia-widens-teen-social-media-ban-youtube-scraps-exemption-2025-07-29/

online privacy and the potential for online pseudonymity. More likely, any feasible system will have elements of all three. Let us take each in turn.

3.3 An age verification system could be easily evaded by those under the age limit. A youth could misrepresent their age to a particular website; present a friend's identification documents if challenged; misstate their age when initially setting up a Google or Apple account; use a Virtual Private Network to pretend to be located in a jurisdiction where age limits do not apply; use a web browser rather than an age-gated app; or, could use a site without logging into it.

3.4 Systems that do not make it easy for youths to evade age restrictions will impose burdens on adult users or come with risks to online privacy or pseudonymity. Technological solutions based on zero-knowledge proofs could prevent youth access while preserving adult privacy. Such solutions would have a credentialing authority, like RealMe or a private sector alternative, verify that an authorised user over the required age limit is associated with a one-time key being tested by a regulated social media provider. How would that work?

3.4.1 Every Kiwi wishing to use social media would be required to register with RealMe or a private alternative. That credentialling authority, on a user's request, could produce a one-time key confirming that the key was generated at the request of a user over the age limit. The key could be provided to a social media platform. That platform could anonymously verify the key's authenticity with the credentialling authority. Under that 'zero-knowledge proof' solution, RealMe would not know the social media company or account that the user sought to have verified, and the platform would not know the real-world identity of the account being verified.

3.4.2 This kind of zero-knowledge proof solution can be highly robust in scenarios where a user does not wish to be impersonated, like in a financial transaction. It will not work if users do not mind being impersonated. Social media users can have multiple accounts for multiple purposes with one or many providers. A user age-authenticating an additional account could be doing so for their own use, or for the use of an underage friend. Neither RealMe nor the social media provider would ever know.

3.4.3 Maintaining user privacy and the potential for pseudonymous accounts while reducing the risk of youth access would involve frequent re-verification challenges: users would need to renew their age-verification at frequent intervals, which would be more difficult to do if the youth needed to find an above-age-limit friend each time the social media site demanded an age check. This solution imposes substantial burdens on adult users, who would need to be re-verified.

3.5 Platforms would be incentivised to use available tools, AI-powered or otherwise, to provide more frequent challenges to accounts that seemed more likely to be held by those under the age limit. In that case, the burden of frequent re-verification would fall more heavily on users within a few years of the age limit.

3.6 Avoiding imposing undue burdens on users above the age limit while minimising the risk that youths accessing the site would mean the end of online privacy. Sites would gather users' real identification or photos of their faces that can be easily linked to their real identification. They would remember forever that the user is over the age limit; they would wish to maintain those records for regulatory compliance purposes to avoid penalties for failing to take practicable steps to keep youths off their site. Records held by a site can be hacked from a site, as has happened even to District Health Boards. And New Zealanders with families living in places

like China may be discouraged from posting under a pseudonym, fearing their families could be punished.

3.7 Solutions could have a blend of all three problems. This is not just a theoretical concern.[4]

The Online Safety Act

3.8 The United Kingdom's Online Safety Act, which spans over three hundred pages of legislation and thousands of pages of codes of conduct,[5] requires that websites prevent youths from viewing potentially harmful content, for example, including pornography, violence, terrorist material, and content promoting self-harm.[6] The Act was passed in response to real harms. It is not going well.

3.9 Companies can be fined up to £18 million or 10 percent of their qualifying worldwide revenue, whichever is greater; criminal penalties against senior managers are also possible.

3.10 The regime came into force on 25 July 2025.

3.11 Facing high fines and potential criminal penalties, internet companies responded in predictably risk-averse ways. UK Twitter and Reddit users found that videos of some Parliamentary speeches were considered sensitive content that they would be unable to view unless they verified their identity with those platforms, with a censorship message blocking the deemed-sensitive posts. Katie Lam, MP, has been blocked from sharing her speech in Parliament on Twitter because Parliament set legislation that could impose hefty penalties on Twitter if they did not block her speech.[7]

3.12 In short order, 468,000 people signed a petition asking for the law's repeal.[8]

3.13 Meanwhile, the Financial Times reported a surge in UK subscriptions to VPN services[9]. UK tech entrepreneur Anthony Rose said, "This is what happens when people who haven't got a clue about technology pass legislation." He noted that it takes "less than five minutes to install a VPN." On 30 July, half of the top ten free apps in Apple's download charts were VPNs, and searches for VPNs have skyrocketed, particularly between midnight and 2 am.[10] Privacy lawyer David Fraser reports UK calls for bans on VPNs in response to the predictable use of VPNs to evade poorly considered regulatory controls.[11]

3.14 The UK did not try to age-gate social media entirely. Parliament there simply wanted to prevent the display of potentially sensitive content to youths. However, that requirement means that social media sites and others must set age gates for content lest they be subject to substantial penalties. In the process, they have set up a system easily evaded by youths, who are turning

---

4 For more detailed discussion of both the in-theory and in-practice issues with "Segregate and Suppress" approaches to online child protection, please see Eric Goldman, 2025. "The 'Segregate-and-Suppress' Approach to Regulating Child Safety Online." 28 Stan Tech L Rev 173. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5208739

5 https://thecritic.co.uk/the-road-to-online-hell-is-paved-with-good-intentions/

6 https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer

7 https://x.com/Katie_Lam_MP/status/1949416623766458816

8 https://news.sky.com/story/x-criticises-online-safety-act-and-warns-its-putting-free-speech-in-the-uk-at-risk-13405434

9 https://www.ft.com/content/356674b0-9f1d-4f95-b1d5-f27570379a9b

10 https://thecritic.co.uk/vpn-nation/

11 https://x.com/privacylawyer/status/1949924378105233475

to VPNs; inconvenienced adult users, who either need to use a VPN themselves or present their real identification to sites with dubious security; and have created a looming privacy and security nightmare. It will be interesting to see which Members of Parliament or of the House of Lords inevitably wind up having their real identification and viewing histories hacked from pornography sites by foreign intelligence services, by blackmailers, by activists for opposing political parties, or by freelancers for the Daily Mail.

3.15 This outcome was both predictable and predicted. In 2022, the Institute of Economic Affairs warned that the bill threatened free speech, innovation, and privacy.[12] Their warnings have proven correct.

3.16 The Critic's Melissa Tourt concluded, "The Online Safety Act emerged from ministerial chaos, technological illiteracy, and a parliamentary process dominated by emotion rather than evidence."[13] New Zealand can avoid such an outcome by simply waiting to see how regimes elsewhere pan out, rather than rushing ahead.

3.17 In response to regulation in some US states, YouTube has been rolling out an AI-powered age check system. Users suspected of being under 18 must submit a government ID, credit card, or selfie as age verification. The Electronic Frontier Foundation has warned that data will be retained, which will have implications for user privacy.[14]

4. A LEAST-BAD OPTION

4.1 Every option in this space is fraught. If Parliament is determined to do something, one option seems less fraught than the others.

4.2 If every potential policy in this space must choose at least one of the three ways these policies can fail, we suggest that being less than perfect in blocking youth access is less bad than imposing substantial costs on adult web users or ending internet privacy.

4.3 Google and Apple accounts already include a user-stated age. Apps in the app stores can be age limited, based on the user's age as stated when the account was first set up and linked to the phone. Youth accounts are linked to a parent or guardian's account through, for example, Google's Family Link.

4.4 Parliament could require an age-gate on social media apps through the Google and Apple app stores, linked to the user's age as stated when the phone and associated account were set up. Parental permission would be required to install the app for those under the age limit.

4.5 This solution is easily worked around.[15] Youths could set up accounts on a web browser rather than on their phone. They could access social media without themselves logging in. They could set up an alternative account. They could use a VPN to pretend they are no longer based in New Zealand or another jurisdiction with an age limit. Some youths may have lied about their age when setting up their initial account, with or without their parents' knowledge. The rule

---

12 https://iea.org.uk/publications/an-unsafe-bill-how-the-online-safety-bill-threatens-free-speech-innovation-and-privacy/

13 https://thecritic.co.uk/the-road-to-online-hell-is-paved-with-good-intentions/

14 https://arstechnica.com/tech-policy/2025/07/youtubes-selfie-collection-ai-age-checks-are-concerning-privacy-experts-say/

15 See discussion in Goldman, 2025 (op. cit.), at page 190. The entire paper is very much worth reading.

would simply make it harder for most youths to access social media on their phones without the consent of the parent or guardian who manages the family's account.

4.6 A child asking a parent or guardian's permission to maintain a social media account, with the parent or guardian prompted to use the family tools to provide access, could spark the parent to set time limits or other access restrictions – like bedtimes – if they had not done so already. Parliament could provide more information about those options, while recognising that both Apple and Google do provide ample information already.

4.7 Even if this option could be perfectly enacted, it would have its own inherent trade-offs. Some youths find warm and helpful online communities. They could be harmed if their parents, worried about harms from social media, denied access. Some youths may be protected against harmful online activities; others may be harmed by losing treasured and harmless communities. Both are real.

4.8 If Parliament chooses this route, it should do so *knowing* that many youths will still find ways of accessing social media, and that some youth access to social media is preferable to substantially hindering every adult's access to social media, or ending online privacy. No one should feign surprise later if some youths bypass the restrictions. They should not pretend that it is Big Tech's fault or that youth access is caused by any loophole. Every option in this policy area has substantial trade-offs.

4.9 We appreciate the opportunity to submit to this Inquiry. We hope the Committee finds our submission constructive. We would be happy to discuss this with the Committee should they consider it helpful.

ENDS