



PARLIAMENT OF AUSTRALIA
DEPARTMENT OF PARLIAMENTARY SERVICES



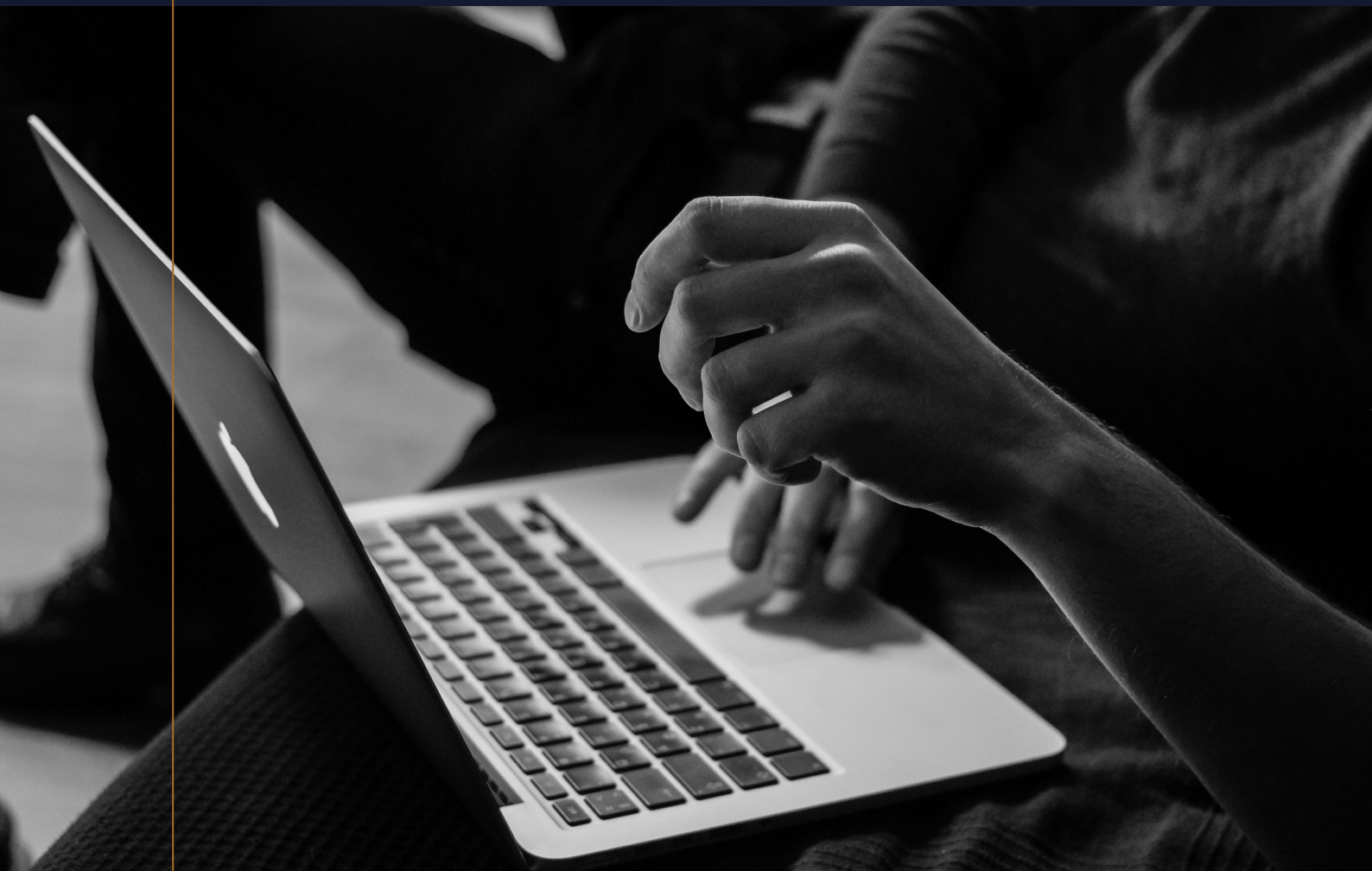
PARLIAMENTARY LIBRARY

Research Paper | 21 August 2024

Children's online safety legislation and regulations – a backgrounder

Nell Fraser

Research Paper Series, 2024–25



Confidential, Impartial, Timely

ISSN 2203-5249

Executive summary

- Australia led the world with online safety regulation with the introduction of the *Enhancing Online Safety Act 2015* and the establishment of the eSafety Commissioner in 2015.
- Australia's online safety regulation is primarily governed by the *Online Safety Act 2021* (the Act), which is currently under review. Key features of the Act include a set of Basic Online Safety Expectations for online service providers; complaints and objections systems; and an Online Content Scheme backed by industry codes, a complaints system and removal and remedial notices.
- The eSafety Commissioner is currently working with industry to develop industry codes for the treatment of 'class 2' material – including pornography. Alongside this, eSafety is undertaking a pilot of age assurance technology, for online pornography and broader social media platforms.
- Draft and enacted online safety legislation and industry codes from the United Kingdom, Singapore, the European Union, France, the United States of America, Canada and New Zealand provide useful points of comparison to Australia's online safety system.
- A common feature among many international regulations is the use of age verification to provide modified accounts to children to protect them from harms, including age-inappropriate content, communication with strangers, addictive design features, recommender algorithms, and data collection.

Contents

Introduction 4

Children’s online safety – Australia 4

 History of the Act 4

 How the Act currently protects children 5

 Children’s online exposure to pornography and an age verification roadmap 9

 Other measures and considerations 12

 Next steps 12

Children’s online safety – International approaches 13

 Five Eyes countries 13

 Other jurisdictions 19

Conclusion 23

Introduction

This backgrounder provides an overview of the Australian government's approach to online safety for children – including discussion of the *Online Safety Act 2021* and eSafety's proposed roadmap for age verification – and outlines a sample of children's online safety measures in other jurisdictions.

This paper does not cover treatment of child abuse and exploitation material.

Children's online safety – Australia

Australia's [eSafety Commissioner](#) (eSafety) is the 'world's first government agency dedicated to keeping people safer online.'¹ The work of eSafety is primarily governed by the [Online Safety Act 2021](#) (the Act). While the Act's aim is to improve and promote the online safety of *all* Australians, the safety of *children* is a key focus.² Since eSafety was established in 2015, numerous other countries have legislated their own approaches to safeguarding children online.

History of the Act

The [Online Safety Act 2021](#) came into effect on 23 January 2022, replacing the [Enhancing Online Safety Act 2015](#). The Act was born out of a recommendation of the 2018 'Briggs Report', the [Report of the statutory review of the Enhancing Online Safety Act 2015 and the review of schedules 5 and 7 to the Broadcasting Services Act 1992 \(Online Content Scheme\)](#). The Briggs Report recommended that 'existing out-of-date and inconsistent legislation should be replaced by a new Online Safety Act and a new single code of industry practice'.³ In 2019, the Coalition made an election commitment to introduce a new Online Safety Act, in response to the Briggs Report.⁴ Consultation and drafting of the new legislation began on 11 December 2019, with the Online Safety Bill 2021 introduced into Parliament on 24 February 2021.⁵ The Bill passed both houses on 23 June 2021 and the Act came into effect on 23 January 2022.

1 'Who we are'. eSafety Commissioner.

2 The 2021 Act changed the Commissioner's title from the 'Children's eSafety Commissioner' to the 'eSafety Commissioner', reflecting the Commissioner's role in protecting all Australians.

3 Lynelle Briggs AO, [Report of the statutory review of the Enhancing Online Safety Act 2015 and the review of schedules 5 and 7 to the Broadcasting Services Act 1992 \(Online Content Scheme\)](#), (the Briggs Reports), (Canberra: Department of Communication and the Arts, 2018), 2.

4 Scott Morrison (Prime Minister), Christian Porter (Attorney-General) and Mitch Fifield (Minister for Communications and the Arts), '[Keeping Australians safe online](#)', media release, 5 May 2019.

5 Material provided throughout the consultation and drafting is available at '[Consultation on a Bill for a new Online Safety Act](#)', Department of Infrastructure, Transport, Regional Development, Communication and the Arts; and '[Consultation on Online Safety Reforms](#)', Department of Infrastructure, Transport, Regional Development, Communication and the Arts.

In February 2024, the government announced a review of the effectiveness of the Act.⁶ The review is obligatory under section 239A of the Act. The Terms of Reference for the review outline a number of items that will be considered in the Review, including:

- 5. Whether the regulatory arrangements, tools and powers available to the Commissioner should be amended and/or simplified, including through consideration of:
 - a. the introduction of a duty of care requirement towards users (similar to the United Kingdom's Online Safety Act 2023 or the primary duty of care under Australia's work health and safety legislation) and how this may interact with existing elements of the Act
 - b. **ensuring industry acts in the best interests of the child.**⁷

How the Act currently protects children

Basic Online Safety Expectations

A core part of the Act is the provision of 'Basic Online Safety Expectations' (BOSE).⁸ A factsheet published by eSafety summarises that:

These expectations are designed to help make sure online services are safer for all Australians to use. They also encourage the tech industry to be more transparent about their safety features, policies and practices.

The Basic Online Safety Expectations are a broad set of requirements that apply to an array of services and all online safety issues. They establish a new benchmark for online service providers to be proactive in how they protect people from abusive conduct and harmful content online.

eSafety now expects online service providers to take reasonable steps to be safe for their users. We expect them to minimise bullying, abuse and other harmful activity and content. We expect them to have clear and easy-to-follow ways for people to lodge complaints about unacceptable use.⁹

Part 4 of the Act outlines that the Minister may, by legislative instrument, determine basic online safety requirements for online service providers. Core expectations include but are not limited to expectations that the provider of a service will take reasonable steps to prevent children accessing inappropriate content, ensure end-users are able to use the service in a safe manner and ensure that the service has a robust reporting and complaints system.¹⁰ The current expectations are outlined in the [Online Safety \(Basic Online Safety Expectations\) Determination 2022](#), updated on 31 May 2024, following a review.¹¹ New expectations include

6 Michelle Rowland (Minister for Communications), '[Ensuring our online safety laws keep Australians safe](#)', 13 February 2024.

7 Department of Infrastructure, Transport, Regional Development, Communication and the Arts, [Terms of Reference – Statutory Review of the Online Safety Act 2021](#), (Canberra: Department of Infrastructure, Transport, Regional Development, Communication and the Arts, 2024), 4. Emphasis added.

8 See '[Basic Online Safety Expectations](#)', eSafety Commissioner, for more information.

9 eSafety Commissioner, [Online Safety Act 2021: Fact Sheet](#), (Canberra: eSafety Commissioner, January 2022), 2.

10 [Online Safety Act 2021](#) (Cth), section 46.

11 Michelle Rowland (Minister for Communications), '[Online safety expectations to boost transparency and accountability for digital platforms](#)', 30 May 2024.

that 'the best interests of the child are a primary consideration in the design and operation of any service that is likely to be accessed by children'.¹²

Critically, the Act states that these requirements are *not enforceable* in court.¹³ However, the Act does provide that eSafety can require service providers to report on their compliance with the expectations in various ways. Failure to report is an offence.¹⁴ According to the eSafety website, this reporting requirement is 'designed to improve providers' safety standards and improve transparency and accountability'.¹⁵

Complaints and objection systems

The Act provides for the creation of a complaints system for cyber-bullying material targeted at an Australian child, as well as complaints and objection systems for non-consensual sharing of intimate images, for cyber-abuse material targeted at an adult, and relating to the Online Content Scheme (discussed below).¹⁶ The system for cyber-bullying material targeted at an Australian child allows children, and responsible persons on behalf of a child, to lodge a complaint through an online form on the eSafety website regarding 'online communication to or about an Australian child that is seriously threatening, seriously intimidating, seriously harassing or seriously humiliating'.¹⁷

As summarised in the Simplified Outline of the Act:

The complaints system for cyber-bullying material targeted at an Australian child includes the following components:

- (a) the provider of a social media service, a relevant electronic service or a designated internet service may be given a notice (a **removal notice**) requiring the removal from the service of cyber-bullying material targeted at an Australian child;
- (b) a hosting service provider who hosts cyber-bullying material targeted at an Australian child may be given a notice (a **removal notice**) requiring the provider to cease hosting the material;
- (c) a person who posts cyber-bullying material targeted at an Australian child may be given a notice (an **end-user notice**) requiring the person to remove the material, refrain from posting cyber-bullying material or apologise for posting the material.¹⁸

Section 12 of the Act defines 'removed' as when 'the material is neither accessible to, nor delivered to, any of the end-users in Australia' using the regulated service.¹⁹ Failure to comply

¹² [Online Safety \(Basic Online Safety Expectations\) Determination 2022](#), section 2A.

¹³ [Online Safety Act 2021](#), subsection 45(3).

¹⁴ [Online Safety Act 2021](#), part 4, division 3.

¹⁵ 'Basic Online Safety Expectations', eSafety Commissioner.

¹⁶ The section on complaints about cyber-bullying material targeted at an Australian child is outlined at [Online Safety Act 2021](#), part 3, division 2.

¹⁷ eSafety Commissioner, [Cyberbullying Scheme: Regulator Guidance](#), eSC RG 1 (eSafety Commissioner, November 2021), 3.

¹⁸ [Online Safety Act 2021](#), section 4.

¹⁹ Regulated services are **social media services**, **relevant electronic services**, **designated internet services** and **hosting service providers** as defined in the Act (see sections 5, 13, 13A, 14, 17, 19, 238). Further, whilst not explored in detail in this paper, the meaning of 'removed' was the key issue in *eSafety Commissioner v X Corp* [2024] FCA 499, where the Federal Court rejected the eSafety Commissioner's argument that references to 'remove' in the Act should be interpreted to include 'the ordinary sense of the word rather than the meaning

with the above notices may lead to a number of possible enforcement actions including a court injunction, and a civil penalty notice.²⁰

Online Content Scheme

The Act includes an Online Content Scheme that regulates illegal and restricted online content, which eSafety describes as:

online content that ranges from the most seriously harmful material, such as images and videos showing the sexual abuse of children or acts of terrorism, through to content which should not be accessed by children, such as simulated sexual activity, detailed nudity or high impact violence.²¹

The Act provides that eSafety 'can direct an online service or platform to remove illegal content or ensure that restricted content can only be accessed by people who are 18 or older'.²² Illegal and restricted online content is classified as either class 1 or class 2 material, with class 1 material being 'material that is or would likely be refused classification under the National Classification Scheme' and class 2 material being 'material that is, or would likely be, classified as either':

- X18+ (or, in the case of publications, category 2 restricted), or
- R18+ (or, in the case of publications, category 1 restricted) under the National Classification Scheme, because it is considered inappropriate for general public access and/or for children and young people under 18 years old.²³

eSafety has proposed simplified subcategories for class 1 and class 2 materials, which it argues are based on, and consistent with, the National Classification Code and film classification guidelines.²⁴ These subcategories have been devised for the purpose of industry codes, recognising that within class 1 and class 2 material, 'some content is more harmful than other content, and industry participants may handle this material in different ways'.²⁵

in s 12 of the Online Safety Act 2021' (see paras [15] and [42]: "Removed", as noted above, is defined by s 12 of the OS Act... other grammatical forms of the same word [must] be given corresponding meanings. "Removal" of material from a social media platform is a process that results in the material being "removed" in the defined sense...).

20 eSafety Commissioner, [Cyberbullying Scheme: Regulator Guidance](#), eSC RG 1 (eSafety Commissioner, November 2021), 6.

21 '[Illegal and restricted online content](#)', eSafety Commissioner.

22 '[Illegal and restricted online content](#)', eSafety Commissioner.

23 '[Illegal and restricted online content](#)', eSafety Commissioner. Definitions of class 1 and class 2 materials (without any specific subcategories) are provided at sections 106 and 107 of the [Online Safety Act 2021](#) (Cth). Read more about the National Classification Scheme at '[Legislation](#)', Australian Classification, Department of Infrastructure, Transport, Regional Development, Communication and the Arts.

24 eSafety Commissioner, [Development of industry codes under the Online Safety Act: Position Paper](#), (eSafety Commissioner, September 2021), 22–24.

25 eSafety, [Development of industry codes under the Online Safety Act: Position Paper](#), 21. For example, an industry code may have different provisions in place for terror related content (class 1A) and drug related content (class 1B), recognising that these materials have different risk profiles.

Industry codes and standards

Division 7 of Part 9 of the Act provides that industry should develop industry codes and standards that include procedures for dealing with class 1 and class 2 content. Codes must be registered with eSafety, and once registered industry is required to comply.²⁶ eSafety may refuse to register codes if they do not meet the statutory requirements, in which case eSafety can develop an industry standard for that section of the online industry, which must be complied with.²⁷ Repeated non-compliance may lead to a Federal Court order for a service provider to stop providing that service in Australia.²⁸

To date, 6 industry codes addressing class 1A and class 1B material have been registered and have come into effect, with a further 2 set to take effect on 22 December 2024.²⁹

Development of codes to address class 2 material – which is considered inappropriate for children – formally commenced on 1 July 2024, with final draft codes expected on 19 December 2024.³⁰

Complaints system and removal notices

The Online Content Scheme is strengthened by a complaints system.³¹ Subsection 38(1) provides that a person may make a complaint to eSafety if they believe class 1 material or class 2A material that shows actual sexual intercourse or sexual activity between consenting adults, i.e. pornography, is accessible online via a regulated service.³² Subsection 38(2) provides that a person may also make a complaint to eSafety if class 2 material that has been or is likely to be classified R18+ or Category 1 Restricted under the National Classification Code (class 2B) is accessible and not subject to a restricted access system (discussed below).³³ In response to a complaint, eSafety may:

- issue a removal notice requiring a service provider or hosting service provider to remove class 1 material or class 2A material that shows actual sexual activity between consenting adults or
- issue a remedial notice requiring a service provider or hosting service provider to either:
 - remove content that is likely to be classified R18+ or Category 1 Restricted (class 2B material) or
 - to ensure that access to the material is subject to a restricted access system.³⁴

²⁶ [Online Safety Act 2021](#), sections 140 and 143.

²⁷ [Online Safety Act 2021](#), section 145.

²⁸ [Online Safety Act 2021](#), sections 156, 157, 158 and 159.

²⁹ Industry codes are available at '[Register of industry codes and industry standards for online safety](#)', eSafety Commissioner. Specific definitions of Class 1A and Class 1B material as they apply to industry codes are provided within the [Consolidated Industry Codes of Practice for the Online Industry \(Class 1A and Class 1B Material\) Head Terms](#), 12 September 2023.

³⁰ '[Industry codes and standards](#)', eSafety.

³¹ Outlined at [Online Safety Act 2021](#), part 3, division 5.

³² Specifically class 2 materials that are covered by paragraph 107(1)(a), (b), (c), (d) or (e).

³³ Specifically class 2 materials that are covered by paragraph 107(1)(f), (g), (h), (i), (j), (k) or (l).

³⁴ [Online Safety Act 2021](#), sections 109, 110, 114, 115, 119 and 120.

The provisions related to class 1 material apply to material that can be *accessed* by end-users in Australia, regardless of from where they are provided or hosted.³⁵ However, the provisions related to class 2 material only apply to services that are *provided or hosted from Australia*.³⁶ As outlined in the Explanatory Memorandum for the Act:

This is intended to capture, for example, social media services who have a registered office or carry on business in Australia or a website based in Australia. It is not intended to capture services based overseas that provide X 18+ material. This type of content is instead intended to be dealt with through industry codes and standards.³⁷

Civil penalties apply for non-compliance with removal notices and remedial notices. Continued non-compliance with a removal notice may lead to a Federal Court order for a service provider to stop providing that service in Australia.³⁸

In summary, these provisions provide that pornographic material that is hosted in or provided from Australia may be subject to a removal notice and necessitate that material that is classified as inappropriate for children and is hosted in or provided from Australia must be subject to a restricted access system.

Restricted access systems

The requirements for restricted access systems are specified in the [Online Safety \(Restricted Access Systems\) Declaration 2022](#), as provided for in Section 108 of the Act.³⁹ The Declaration includes requirements that the access-control system:

- requires an application for access to relevant class 2 material
- gives warnings and safety information for relevant class 2 material
- incorporates reasonable steps to confirm the age of applicants and
- limits access to relevant class 2 material.⁴⁰

Importantly, this includes a requirement that 'the access-control system must incorporate reasonable steps to confirm that an applicant is at least 18 years of age'.⁴¹

Children's online exposure to pornography and an age verification roadmap

Safeguarding children from accessing harmful and inappropriate material online, specifically pornography, has been an area of longstanding government and parliamentary focus.

³⁵ [Online Safety Act 2021](#), subsections 109(1)(c) and 110(1)(c).

³⁶ [Online Safety Act 2021](#), subsection 114(1)(e), subsection 115(1)(f), subsection 119(1)(e), and subsection 120(1)(f).

³⁷ [Explanatory Memorandum](#), Online Safety Bill 2023, 128. eSafety's Regulatory Guidance for the Online Content Scheme reiterates this interpretation. eSafety Commissioner, [Online Content Scheme: Regulatory Guidance](#), (eSafety Commissioner, December 2023), 13.

³⁸ [Online Safety Act 2021](#), sections 156, 157, 158 and 159.

³⁹ See also '[Restricted Access System](#)', eSafety.

⁴⁰ [Online Safety \(Restricted Access Systems\) Declaration 2022](#), clause 5.

⁴¹ [Online Safety \(Restricted Access Systems\) Declaration 2022](#), subclause 8(1).

In 2015–2016 the Senate Standing Committee on Environment and Communications held an inquiry into the '[Harm being done to Australian children through access to pornography on the Internet](#)'. The Government supported the committee's recommendations to commission further dedicated research into young people's exposure to pornography online.⁴² In late 2017, the Australian Institute of Family Studies (AIFS) released the '[Effects of Pornography on Children and Young People](#)' report, which synthesised the findings of research into the impacts of exposure to pornography on young people. It highlighted that research shows young peoples' consumption of pornography online influences expectations of sex; shapes sexual practices, including sexual health safety; reinforces gender stereotypes; and positively correlates to an increase in sexual aggression.⁴³

In 2018, eSafety published a report on '[Parenting and pornography: findings from Australia, New Zealand and the United Kingdom](#)'. While the findings from Australia included that only 24% of surveyed parents thought their children had been exposed to online pornography, 40% of those parents believed their children had come across the content accidentally, while a further 8% responded that they were sent material by a stranger.⁴⁴

Following this, in 2019, the House of Representatives Standing Committee on Social Policy and Legal Affairs launched an '[Inquiry into age verification for online wagering and online pornography](#)'. The inquiry made 6 recommendations, including that 'the Australian Government direct and adequately resource the eSafety Commissioner to expeditiously develop and publish a roadmap for the implementation of a regime of mandatory age verification for online pornographic material'.⁴⁵ This recommendation was supported by government.⁴⁶

In March 2023, eSafety completed this work and submitted an age verification background report and age verification roadmap to the government for consideration.⁴⁷ The roadmap's key recommendation is to 'develop, implement, and evaluate a pilot before seeking to prescribe and mandate age assurance technologies for access to online pornography'.⁴⁸ As outlined in the roadmap, eSafety's research found that 75% of 16–18-year-olds surveyed had seen online pornography.⁴⁹ In light of these findings, and the harms of children's exposure to pornography, as referenced above, eSafety suggested that:

If a service allows pornography, it should apply settings to prevent it from being accessed by and recommended to children. Among other things, this requires robust age assurance measures at sign-

42 Australian Government, [Australian Government response to the Senate References Committee on Environment and Communications report: Harm being done to Australian children through access to pornography on the Internet](#), March 2017, 6.

43 Antonia Quadara, Alissar El-Murr and Joe Latham, [The effects of pornography on children and young people: an evidence scan](#), (Melbourne: Australian Institute of Family Studies, 2017), 11.

44 eSafety Commissioner, [Parenting and pornography: findings from Australia, New Zealand and the United Kingdom](#), (eSafety Commissioner and Netsafe, December 2018), 13–14.

45 The House of Representatives Standing Committee on Social Policy and Legal Affairs, [Protecting the age of innocence](#), February 2020, xv–xvi.

46 Australian Government, [Australian Government response to the House of Representatives Standing Committee on Social Policy and Legal Affairs report: Protecting the age of innocence](#), June 2021, 5.

47 '[Age verification](#)', eSafety Commissioner.

48 eSafety Commissioner, [Roadmap for age verification: and complementary measures to prevent and mitigate harms to children from online pornography](#), (Canberra: eSafety Commissioner, March 2023), 28–29.

49 [Roadmap for age verification](#), 7.

up to ensure the service knows the age of its users. If a service does not allow pornography, this rule needs to be enforced through effective reporting mechanisms and proactive content detection and moderation tools, developed and deployed in consultation with the user community.⁵⁰

eSafety also outlined that:

While the roadmap focuses on children's access to online pornography, the ability of online service providers to ascertain the age of their users is essential to keeping children safe from a wider spectrum of risks and harms beyond pornography.⁵¹

The roadmap approaches the roll out of age-assurance technology cautiously, noting that any enforcement is contingent on appropriate technology.⁵² The independent assessment of available age assurance technologies, contained within the report, found the market to be 'immature but developing' – and that interest in age-assurance technologies by governments worldwide is spurring the development of robust age-assurance processes by online companies.⁵³ In light of this, the report recommended that 'age assurance technologies should be trialled in Australia, based on lessons from pilots conducted elsewhere, before being mandated'.⁵⁴ Further, it suggests that while the technology will likely reduce children's access to pornography, 'age assurance on its own will not address this issue'.⁵⁵

The Government issued its [response to the roadmap](#) on 30 August 2023.⁵⁶ The response noted the roadmap's recommendation regarding a pilot of age assurance technologies but decided to 'await the outcomes of the class 2 industry codes process before deciding on a potential trial of age assurance technologies'.⁵⁷ This approach was reviewed, however, following a National Cabinet meeting on 1 May 2024 focussing on measures to end violence against women. The Government announced that it would 'provide resourcing to conduct a pilot of age assurance technology to protect children from harmful content, like pornography and other age-restricted online services' and outlined that:

The new pilot... is part of a suite of interventions aimed at curbing easy access to damaging material by children and young people, and tackling extreme misogyny online.

The pilot will identify available age assurance products to protect children from online harm, and test their efficacy, including in relation to privacy and security.⁵⁸

50 [Roadmap for age verification](#), 12.

51 [Roadmap for age verification](#), 16.

52 [Roadmap for age verification](#), 16–18.

53 [Roadmap for age verification](#), 17.

54 [Roadmap for age verification](#), 8.

55 [Roadmap for age verification](#), 7.

56 Department of Infrastructure, Transport, Regional Development, Communication and the Arts, [Government response to the Roadmap for Age Verification](#), August 2023, 2.

57 [Government response to the Roadmap for Age Verification](#), 4–5. In contrast, the Opposition committed to conducting a trial of age verification technologies, independent of the class 2 industry codes, and on 27 November 2023 Shadow Minister David Coleman MP introduced the [Online Safety Amendment \(Protecting Australian Children from Online Harm\) Bill 2023](#), which 'amends the *Online Safety Act 2021* to require the minister to conduct a trial of age verification technologies'.

58 Anthony Albanese, Katy Gallagher, Amanda Rishworth, Mark Dreyfus, and Michelle Rowland, '[Tackling online harms](#)', media release, 1 May 2024.

This measure was funded in the May 2024 Budget.⁵⁹

A key difference between the potential inclusion of age verification mandates within class 2 industry codes and the current provisions related to accessing class 2 content, is the scope of application. Under the *Online Safety Act*, eSafety may only issue removal notices and remedial notices and mandate the use of restricted access systems for class 2 content *if it is provided from or hosted in Australia*.⁶⁰ However, if a class 2 industry code were to mandate the use of an age assurance system, this would apply to all 'online services so far as those are provided to end users in Australia'.⁶¹

Other measures and considerations

The government's response to the 2023 report of a two-year review of the *Privacy Act 1988* agreed-in-principle to a 'suite of proposed additional protections' which would apply to all children.⁶² This includes agreeing to the development of a Children's Online Privacy code.⁶³

Further, the harm of recommender algorithms in social media feeds has been a recent topic of interest.⁶⁴ In December 2022, eSafety published [Position Statement: Recommender systems and algorithms](#) which outlines a range of risks posed by recommender systems and potential mitigating actions.⁶⁵

Next steps

As indicated above, the next regulatory step in the protection of children from online harms is the development of industry codes for class 2 content, which began on 1 July 2024.⁶⁶ The development and registration of these codes will create a responsibility for online service providers to control access to class 2 material such as online pornography that is considered harmful to children.

59 Australian Government, 'Online Safety', [Budget Measures: Budget Paper No. 2: 2024–25](#), 150.

60 [Online Safety Act 2021](#), subsection 114(1)(e), subsection 115(1)(f), subsection 119(1)(e) and (f), and subsection 120(1)(f) and (g).

61 eSafety Commissioner, [Development of Phase 2 Industry Codes under the Online Safety Act: eSafety Position Paper](#), (eSafety Commissioner, July 2024), 8. This wider scope is important given that the most accessed pornography sites from Australia are hosted overseas (see [Roadmap for age verification](#), 24–25). It is worth noting that age verification is not the only measure that may be included in industry codes for class 2 content. Other potential measures are outlined at pages 63–67 of [Development of Phase 2 Industry Codes under the Online Safety Act: eSafety Position Paper](#).

62 Australian Government, [Government Response: Privacy Act Review Report](#), ([Barton]: Attorney-General's Department, 2023), 13–14.

63 [Government Response: Privacy Act Review Report](#), 13. Further information on the proposed Children's Online Privacy Code is provided on the [Alannah & Madeline Foundation website](#).

64 See, for example, the Department of Social Services' [The Hidden Trends of Disrespect](#) resource, published on 17 June 2024. Amanda Rishworth and Justine Elliot, '[New Stop it at the Start campaign launched](#)', media release, 17 June 2024.

65 eSafety Commissioner, [Position statement: Recommender systems and algorithms](#), (eSafety Commissioner, December 2022).

66 '[Industry codes and standards](#)', eSafety.

As noted, the Government has also funded a pilot of age assurance technology, which will underpin the enforcement of these codes, and run in parallel to the codes' development.⁶⁷ Statements by government have confirmed that the trial of age-assurance technologies will not only relate to accessing 'age inappropriate material' and age-restricted services, but also to social media services.⁶⁸ To complement the technology trial, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts will undertake research into potential age-limits to be imposed on social media generally, restricting access to child users.⁶⁹ Any regulatory developments in this area sit outside the current development of class 2 industry codes.⁷⁰

The current [review](#) into the Online Safety Act also provides an opportunity to consider the effectiveness of the current Act, consider any necessary reform, and evaluate Australia's approach against other jurisdictions.

Children's online safety – International approaches

This section outlines some examples of online safety legislation in international jurisdictions, with a specific focus on measures related to child users' safety online. Examples are provided for the Five Eyes countries – as countries comparable to Australia – as well as other jurisdictions that have taken notable, recent legislative action in the online safety space. This overview is representative, not exhaustive. Given the constitutional, political, legislative, and structural differences between countries, it is not always possible to draw clear comparisons between Australian and overseas legislation.

Five Eyes countries

United Kingdom

In the UK, a draft Online Safety Bill was first published in May 2021, with various changes made to the Bill before its introduction to Parliament in March 2022.⁷¹ The [Online Safety Act 2023](#) (the UK Act) received Royal Assent on 26 October 2023.⁷²

As outlined in the UK Act's introduction, the 'Act provides for a new regulatory framework which has the general purpose of making the use of internet services regulated by this Act safer for individuals in the United Kingdom.' Towards this purpose, the UK Act imposes duties

67 Senate Environment and Communications Legislation Committee, Estimates, [Official Committee Hansard](#), 30 May 2024, 43; [Development of Phase 2 Industry Codes under the Online Safety Act](#), 35.

68 Michelle Rowland, '[New industry codes to protect children from online pornography](#)', media release, 2 July 2024.

69 Senate Environment and Communications Legislation Committee, Estimates, [Official Committee Hansard](#), 30 May 2024, 38.

70 eSafety, [Development of Phase 2 Industry Codes under the Online Safety Act: eSafety Position Paper](#), 29.

71 '[Draft Online Safety Bill](#)', GOV.UK; Nadine Dorries, '[World-first online safety laws introduced in Parliament](#)', media release, 17 March 2022.

72 Michelle Donelan, Alex Chalk and Suella Braverman, '[UK children and adults to be safer online as world-leading bill becomes law](#)', media release, 26 October 2023.

on providers of regulated services to identify, mitigate and manage the risks of harm from content and activity that is harmful to children. The duties seek to ensure that services are 'designed and operated in such a way that a higher standard of protection is provided for children than for adults'.⁷³

Duties of Care

Part 3 of the UK Act imposes various duties of care on providers of regulated services. In summary, these duties focus on mitigating and managing the risks arising from services hosting harmful or illegal content, or facilitating harm or illegal activity. Services must have robust content reporting and complaints systems and must have regard to users' freedom of expression and privacy.

Additional duties are imposed on services that are likely to be accessed by children.⁷⁴ These provide that relevant services must carry out, and keep up to date, suitable and sufficient children's risk assessments, and that they must take proportionate measures to reduce the risk of children accessing harmful content. There is also a requirement for user-to-user providers (i.e. social media services) to use age verification or age estimation to prevent children from encountering primary priority content that is harmful to children. Content deemed to be harmful to children for the purpose of the Act includes pornographic content as well as content that encourages, promotes, or provides instructions for suicide, self-harm, or an eating disorder.⁷⁵

Other duties

Part 5 imposes duties on providers of pornographic content. This includes a duty to ensure, by the use of age verification or age estimation (or both), that children are not normally able to encounter content that is regulated provider pornographic content in relation to the service.⁷⁶

Compliance with duties

The UK Act provides that OFCOM (the UK's communications regulator) must prepare and issue a code of practice for service providers recommending measures for the purpose of compliance with their various duties. Comprehensive [Draft Children's Safety Codes](#) for search engines and user-to-user services were published on 8 May 2024.⁷⁷ OFCOM is also responsible for enforcement of the UK Act.⁷⁸

Section 131 provides a list of duties that are enforceable requirements, which appears to cover all duties outlined above in relation to children's online safety and access to

⁷³ [Online Safety Act 2023](#) (UK), subsection 1(3)(b)(i).

⁷⁴ Outlined at [Online Safety Act 2023](#), sections [11](#), [12](#), [13](#) and [28](#), [29](#), [30](#). [Section 37](#) provides that a service is deemed to be 'likely to be accessed by children' if it is possible for children to access the service or part of it and the 'child user condition' is met, or if the service fails to complete the required 'children's access assessment' (both defined at [Section 35](#)).

⁷⁵ [Online Safety Act 2023](#), Part 3, [Chapter 7](#).

⁷⁶ [Online Safety Act 2023](#), [section 81](#).

⁷⁷ Ofcom, '[Consultation: Protecting children from harms online](#)', 8 May 2024.

⁷⁸ [Online Safety Act 2023](#), Part 3, [Chapter 6](#). [Chapter 6](#) of Part 7 outlines OFCOM's enforcement powers.

pornographic content. OFCOM may give a provisional notice of contravention (effectively a warning) to the provider of a regulated service if there are reasonable grounds to believe that they have failed to comply with an enforceable requirement.⁷⁹ A provisional notice of contravention may lead to a confirmation decision – an order to require a person to take steps to comply with a notified requirement or an order to pay a penalty.⁸⁰ OFCOM may proceed in issuing a confirmation decision (without a provisional notice) if it is satisfied that a provider has failed to comply with a risk assessment duty or duty regarding children's access requirements.⁸¹

Failure to comply with requirements imposed by OFCOM in a confirmation decision may lead to imprisonment or a fine, or both.⁸² OFCOM may also restrict the service of non-compliant providers.⁸³

Canada

The proposed [Bill C-63](#) (Online Harms Act) was introduced by the Canadian Government on 26 February 2024 and is currently before parliament.⁸⁴ The bill aims to create 'a baseline standard for online platforms to keep Canadians safe', with a special focus on children.⁸⁵ Alongside standards for online platforms, the bill proposes a new ecosystem of regulatory infrastructure through the establishment of the Digital Safety Commission of Canada, the Digital Safety Ombudsperson of Canada, and the Digital Safety Office of Canada.⁸⁶

The Bill specifically targets 7 types of harmful content including content used to bully a child and content that induces a child to harm themselves.⁸⁷ It also subjects social media services to 4 duties – to act responsibly, including by mitigating the risk of users being exposed to harmful content; to protect children; to make certain sexually exploitative or intimate content inaccessible, and to keep records.⁸⁸ The Duty to Protect Children includes that the design of regulated platforms must respect the protection of children.⁸⁹

New Zealand

The New Zealand Government recently ceased work aimed at modernising the country's online safety regulation, with the decision to not progress work developed through a 3-year

79 *Online Safety Act 2023*, subsection [130\(1\)](#).

80 *Online Safety Act 2023*, [section 132](#). The penalties that OFCOM may impose with a confirmation decision are outlined at [Section 137](#).

81 *Online Safety Act 2023*, sections [134](#) and [135](#).

82 *Online Safety Act 2023*, section [138](#). [Section 139](#) provides that OFCOM may instead issue a penalty for non-compliance.

83 *Online Safety Act 2023*, sections [144-148](#).

84 '[Proposed Bill to address Online Harms](#)', Government of Canada, updated 4 April 2024.

85 '[Proposed Bill to address Online Harms](#)', Government of Canada, updated 4 April 2024.

86 [Government Bill \(House of Commons\) C-63 \(44-1\)](#) (Canada), first reading, Online Harms Act parts 1–3.

87 [Government Bill \(House of Commons\) C-63 \(44-1\)](#) (Canada), first reading, Online Harms Act subsection 2 (1).

88 [Government Bill \(House of Commons\) C-63 \(44-1\)](#) (Canada), first reading, Online Harms Act part 4.

89 [Government Bill \(House of Commons\) C-63 \(44-1\)](#) (Canada), first reading, Online Harms Act section 65.

review.⁹⁰ The [Safer Online Services and Media Platforms](#) (SOSMP) review ran from June 2021 to May 2024, with the objective 'to improve the regulation of online services and media platforms to boost consumer safety for all New Zealanders, with a particular focus on minimising content harms for children and young people'.⁹¹

The review aimed to streamline and address holes in the current regulatory system, which is comprised of the *Films, Videos, and Publications Classification Act 1993*, the *Broadcasting Act 1989*, and 'voluntary self-regulation by operators', and does not comprehensively cover online content.⁹² A discussion paper published by the government in June 2023 proposed an industry regulation model overseen by a new regulator, to operate at arm's length from government, with the view to 'cover all platforms, regardless of format or type', with a focus on larger platforms.⁹³ The paper called for submissions from stakeholders in response to specific policy proposals, and indicated that a draft Bill was to be expected in 2024 at the earliest.⁹⁴

A summary report released in April 2024 synthesised submissions made to the review – including general support from social media platforms and from organisations.⁹⁵ However, 18,978 of the approximate 20,000 submissions received were template submissions from the Free Speech Union and Voices for Freedom, which were strongly negative and concerned that 'the proposals would result in the narrowing of people's right to freely express themselves'.⁹⁶ In response, the Minister for Internal Affairs, Brooke van Velden, announced on Facebook the government's decision to not progress with these reforms, citing the strong opposition to the reforms and the 'principle of free speech'.⁹⁷

In lieu of legislation, social media platforms have signed up to the voluntary [Aotearoa New Zealand code of practice for online safety and harms](#), which was developed by Netsafe – an independent online safety charity – in consultation with stakeholders and launched in 2022.⁹⁸ Current signatories include Meta, Google, TikTok, Twitch and X.⁹⁹

United States of America

There has been much action in the children's online safety realm in the United States, with various laws proposed and enacted at the state level, and relevant legislation introduced at the Federal level. These various laws build on the foundation of the federal [Children's Online](#)

90 Hayden Donnell and Colin Peacock, '[Media oversight one-stop-shop stopped](#)', RNZ, 19 May 2024. Fiona Sing and Antonia Lyons, '[Big tech companies were open to online safety regulation - why did NZ's government scrap the idea?](#)', *The Conversation*, 25 June 2024.

91 '[Media and online content regulation](#)', Te Tari Taiwhenua | Department of Internal Affairs.

92 '[Media and online content regulation](#)', Te Tari Taiwhenua | Department of Internal Affairs. Department of Internal Affairs, [Safer Online Services and Media Platforms: Discussion Document](#), (Department of Internal Affairs, June 2023), 4.

93 Department of Internal Affairs, [Safer Online Services and Media Platforms: Discussion Document](#), 21–22.

94 Department of Internal Affairs, [Safer Online Services and Media Platforms: Discussion Document](#), 11.

95 Department of Internal Affairs, [Safer Online Services and Media Platforms – Summary of Submissions](#), (Department of Internal Affairs, April 2024), 9–10.

96 Department of Internal Affairs, [Safer Online Services and Media Platforms – Summary of Submissions](#), 7, 9, 25.

97 Brooke van Velden MP, '[Under the previous government, the Department of Internal Affairs proposed a regulator for online platforms](#)', Facebook, 13 May 2024.

98 '[About Netsafe](#)', netsafe. '[The Code](#)', The Code.

99 '[The Code](#)', The Code.

[Privacy Protection Rule](#) (COPPA), issued in 1999, which protects the privacy of children online and has effectively limited the use of most social media services for children under 13 without parental consent.¹⁰⁰

A common feature of much of the legislation at state level is the mandatory use of age verification – for social media platforms and for sites hosting pornography.¹⁰¹ Analysis from June 2024 notes that Arkansas, Connecticut, Louisiana, Ohio, and Utah have passed laws 'requiring social media platforms to verify that users are over either age 16 or 18 and require parental consent from users under that age limit', while Arkansas, Louisiana, Mississippi, Montana, North Carolina, Texas, Utah, and Virginia have all passed laws 'requiring online services with a certain amount of adult content to verify that users are over 18 or risk fines'.¹⁰²

Representative laws from Utah – one of the first states to legislate in the area – are detailed below as an example of state legislation.¹⁰³ Orrick's '[Online Safety Resource Center](#)' provides an overview of the rapidly developing state laws across the country.

Children's Online Privacy Protection Rule

The [Children's Online Privacy Protection Rule \(COPPA\)](#), issued in 1999 and effective since 21 April 2000, requires that operators of certain websites and online services must, among other things, 'obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children'.¹⁰⁴ A child is defined as an individual aged under 13, and personal information includes a child's first and last name and IP address.¹⁰⁵

In order to comply with the rule, many platforms – such as Facebook, Instagram and Discord – have set terms of service that restrict accounts to those over 13.¹⁰⁶ Others – such as YouTube and TikTok – provide modified accounts for users under 13, with parental consent.¹⁰⁷ However, COPPA's restrictions also apply in instances where account creation is not needed to access a platform's content. In 2019, the US Federal Trade Commission fined YouTube USD\$136 million for violating COPPA. The platform was found to knowingly collect data

100 Federal Trade Commission, '[New Rule Will Protect Privacy of Children Online](#)', media release, 20 October 1999. Natasha Singer, '[U.S. Regulators Propose New Online Privacy Safeguards for Children](#)', *The New York Times*, 20 December 2023.

101 An overview of these bills is available at '[Youth Online Safety Laws: U.S. State Law Tracker](#)', Orrick, 16 May 2024; and '[Age Verification Bill Tracker](#)', FSC Action Centre.

102 Ash Johnson, '[How to Address Children's Online Safety in the United States](#)', *Information Technology & Innovation Foundation*, 3 June 2024.

103 Bryan Schott, '[Utah first state to pass social media regulations aimed at protecting minors](#)', *The Salt Lake Tribune*, 24 March 2023;

104 Federal Trade Commission, '[New Rule Will Protect Privacy of Children Online](#)'. [Children's Online Privacy Protection Rule](#) (US), section 312.3 (b).

105 See definitions at [Children's Online Privacy Protection Rule](#) (US), section 312.2.

106 Natasha Singer, '[U.S. Regulators Propose New Online Privacy Safeguards for Children](#)', *The New York Times*, 20 December 2023. Discord, '[Answering parents' and educators' top questions](#)', Discord Safety Centre, 12 May 2022. '[Continuing to Make Instagram Safer for the Youngest Members of Our Community](#)', Instagram, 17 March 2021. '[How do I report a child under the age of 13 on Facebook?](#)', Facebook Help Centre.

107 TikTok, '[Guardian's Guide](#)', TikTok Safety Centre, updated 17 July 2024. '[YouTube Kids, YouTube & your child's Google Account](#)', YouTube For Families Help.

through cookies from viewers of child-directed channels without first obtaining parental consent.¹⁰⁸

Kids Online Safety Act

At the federal level, a proposed Kids Online Safety Act has been introduced in both the [Senate](#) and the [House of Representatives](#) with bipartisan support.¹⁰⁹ While the two bills do differ in some respects, they share common core features including that ‘covered platforms’ – including online platforms, messaging applications, online video games, and video streaming services – be designed in a way to prevent harm to minors; that minors be provided with modified accounts with protections regarding recommender systems, addictive design features and communications with strangers; that parental tools be available for minor’s accounts; reporting requirements; and the commissioning of a study into age verification technology. Minors are defined as those under the age of 17. Reporting suggests that the Senate bill may have the required support to pass.¹¹⁰

Utah Minor Protection in Social Media Act

[Utah Senate Bill 194](#) (Social Media Regulations Amendments) enacts the *Utah Minor Protection in Social Media Act* (the Utah Act), which will be effective from 1 October 2024. Under the Utah Act, social media platforms must implement an age assurance system to determine whether a current or prospective Utah account holder is under the age of 18.¹¹¹ Platforms must provide modified accounts for minors, with modifications regarding privacy, data collection, ability to message strangers, and addictive design features.¹¹²

The Utah Act also mandates that social media companies offer supervisory tools for minors’ accounts. These tools must include capabilities for an individual selected by the minor to set time limits on account usage, and to view data and settings related to the minor’s account. Minors must not be able to change their default privacy settings without first obtaining verifiable parental consent.¹¹³

[Utah House Bill 464](#) (Social Media Amendments) addresses potential harms to minors caused by social media platforms.

Section 1 (effective 1 May 2024) amends the offence of electronic communication harassment to include the electronic publishing of personal identifying information of a minor by a non-relative, if they are aware that such an action will result in a substantial risk that the minor will be the victim of an offense against the individual as outlined in the Utah Criminal

108 Federal Trade Commission, ‘[Google and YouTube Will Pay Record \\$170 Million for Alleged Violations of Children’s Privacy Law](#)’, press release, 4 September 2019.

109 Natasha Singer, ‘[Kids Online Safety Act Is a Bipartisan Push to Protect Children on Social Media](#)’, *The New York Times*, 31 January 2024.

110 Cristiano Lima-Strong, ‘[Senate poised to pass biggest piece of tech regulation in decades](#)’, *The Washington Post*, 15 February 2024.

111 Those who are under the age of 18 and are married or emancipated are not treated as minors for the sake of the act, see definitions of a ‘minor’ at [Utah Minor Protection in Social Media Act](#) (Utah), subsection 13-71-101 (8).

112 [Utah Minor Protection in Social Media Act](#) (Utah), Section 13-71-202.

113 [Utah Minor Protection in Social Media Act](#) (Utah), Sections 13-71-203 and 13-71-204.

Code.¹¹⁴ Section 2 (effective 1 October 2024) acknowledges potential harms of excessive social media use by minors — including by providing that ‘a Utah minor account holder or a Utah minor account holder's parent may bring a cause of action against a social media company in court for an adverse mental health outcome arising, in whole or in part, from the minor's excessive use of the social media company's algorithmically curated social media service’.¹¹⁵

Together, Utah Senate Bill 194 and Utah House Bill 464 repealed and replaced [Utah Senate Bill 152](#) and [Utah House Bill 311](#), which were passed in 2023 to together form the Utah Social Media Regulation Act (2023 Utah Act).¹¹⁶ At the time, the Utah Social Media Regulation Act was regarded as the first of its kind in the United States.¹¹⁷

However, the 2023 Utah Act was the subject of a complaint by a trade association for internet companies, which argued that it was unconstitutional.¹¹⁸ Notable provisions of the 2023 Utah Act have been removed from the 2024 Bills, including those requiring that:

- social media platforms may not permit a Utah minor to be an account holder unless the minor has the express consent of a parent or guardian¹¹⁹
- minors' accounts may not display advertising¹²⁰
- platforms must prohibit minors from signing in between the hours of 10:30pm – 6:30am, unless a parent authorises access¹²¹
- platforms must not use a design or feature that the company should know causes a minor to have an addiction to the platform.¹²²

Despite these changes, new complaints have been raised about the 2024 Bills.¹²³ The complaints again argue that the bills violate the constitution, and that they block the flow of information and the exercising of free speech.

Other jurisdictions

European Union

[Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC \(Digital Services](#)

¹¹⁴ *Utah Criminal Code* (Utah), [Chapter 5](#).

¹¹⁵ [Utah Social Media Amendments](#) (Utah), Section 78B-3-1103 (1).

¹¹⁶ [Social Media Amendments \(H.B.464\)](#) (Utah) repeals the 2023 Bills.

¹¹⁷ Bryan Schott, ‘[Utah first state to pass social media regulations aimed at protecting minors](#)’, *The Salt Lake Tribune*, 24 March 2023; Maanvi Singh, ‘[Utah bans under-18s from using social media unless parents consent](#)’, *The Guardian*, 24 March 2023.

¹¹⁸ Heather Kelly and Simone Seikaly, ‘[Legal expert questions Utah's social media restrictions](#)’, *KSL News Radio*, 19 December 2023; David Stauss and Shelby Dolen, ‘[Utah Legislature Repeals and Replaces Utah Social Media Regulations Act](#)’, *Byte Back*, Husch Blackwell, 11 March 2024.

¹¹⁹ [Social Media Regulation Amendments \(S.B.152\)](#) (Utah), 13-63-102 (3).

¹²⁰ [Social Media Regulation Amendments \(S.B.152\)](#) (Utah), 13-63-103 (3).

¹²¹ [Social Media Regulation Amendments \(S.B.152\)](#) (Utah), 13-63-105 (1).

¹²² [Social Media Usage Amendments \(H.B.311\)](#) (Utah), 13-63-201 (2).

¹²³ Kyle Dunphey, ‘[Utah changed its social media laws to avoid constitutional issues, but legal challenges persist](#)’, *Daily Herald*, 13 June 2024.

[Act](#)) (the Digital Services Act) was enacted on 16 November 2022. The Digital Services Act aims to 'contribute to the proper functioning of the internal market for intermediary services by setting out harmonised rules for a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected'.¹²⁴

The Digital Services Act predominantly applies to providers of 'very large online platforms' (VLOPs) and 'very large online search engines' (VLOSEs) that are designated by the European Commission. The first large platforms designated by the European Commission were required to meet requirements by August 2023 and all other platforms from February 2024.¹²⁵ Designated platforms include YouTube, LinkedIn, Facebook, Instagram, Pinterest, Snapchat, TikTok, and X, as well as Wikipedia, and several pornography sites, search engines, retail and app stores, and travel booking sites.¹²⁶

Online protection of minors

[Article 28](#) of the Digital Services Act states that:

providers of online platforms accessible to minors shall put in place appropriate and proportionate measures to ensure a high level of privacy, safety, and security of minors, on their service.

The article also restricts advertising based on the profiling of users known to be minors.

Providers of VLOPs and VLOSEs are required to annually identify and assess potential risks caused by their service, including those that may negatively affect the protection of minors.¹²⁷ Platforms must put in place measures to mitigate these risks, including 'taking targeted measures to protect the rights of the child, **including age verification and parental control tools**, tools aimed at helping minors signal abuse or obtain support, as appropriate'.¹²⁸ Article 44 (1)(j) provides that the Commission 'shall support and promote the development and implementation of voluntary standards' for targeted measures to protect minors online.

The Digital Services Act also provides that services must be designed to be understood by children. This includes requiring that the terms and conditions of services primarily directed at or predominantly used by minors be written in a way that minors can understand, and that complaints mechanisms be organised in a way that is child friendly.¹²⁹

¹²⁴ [Regulation \(EU\) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC](#) (Digital Services Act) (European Union), Article 1.

¹²⁵ European Commission, [The Digital Services Act \(DSA\) explained: Measures to protect children and young people online](#), (Luxembourg: Publications Office of the European Union, 2023), 6. See '[Supervision of the designated very large online platforms and search engines under DSA](#)', European Commission, updated 12 July 2024, for information on designated platforms.

¹²⁶ '[Supervision of the designated very large online platforms and search engines under DSA](#)', European Commission.

¹²⁷ [Digital Services Act](#), Articles 33 and 34. The kinds of potential risks that may impose on the rights of the child are outlined at [paragraph 81](#) of the Act's preamble.

¹²⁸ [Digital Services Act](#), Article 35(1)(j). Emphasis added.

¹²⁹ [Digital Services Act](#), Article 14 (3) and paragraph 89 of preamble.

Compliance and penalties

Providers of VLOPs and VLOSEs have various responsibilities under the Digital Services Act, including reporting compliance. The reporting obligations include undertaking an annual independent audit, providing the enforcement authority with access to data necessary to monitor compliance, the establishment of an in-house 'compliance function', and transparency reporting obligations.¹³⁰

The EU and Member States are responsible for ensuring that online providers comply with the Digital Services Act.¹³¹ EU Member States are required to set rules for penalties applicable to infringements under the DSA. The maximum fine that may be imposed for failure to comply with an obligation under the DSA is 6% of the annual global turnover of the provider of intermediary services. The maximum periodic penalty payment is 5% of the average daily global turnover of the provider of intermediary services per day.¹³² [The European Commission](#) can also impose fines where a provider of a VLOP or VLOSE intentionally or negligently infringes the DSA, or fails to comply with a direction or binding commitment made under the DSA.¹³³ Fines cannot exceed 6% of the provider's annual global turnover in the preceding financial year.¹³⁴

France

[French Law no. 2023-566 of July 7th 2023 implementing a digital age of majority and preventing online hate](#) (the French Law) was enacted on 7 July 2023. The French Law amends Law No. 2004-575 of June 21, 2004, on Confidence in the Digital Economy 'and implements a digital age of majority and reinforces the obligations of social networks, especially regarding registration of minors'.¹³⁵

Digital age of majority

Article 4 of the French Law stipulates that social media services operating in France shall refuse the registration of people under the age of 15, unless authorised by a parent. This applies to new and existing accounts. If authority is granted and an account is registered for a minor, the platform must provide information to minors and their parent on the risks associated with digital use and the means of prevention, and clear and appropriate information on the conditions of use of their data and their rights relating to data processing, files and freedoms. The platform must also activate a device to monitor the user's time spent on their service and regularly notify the user of that duration. A parent may request that a social media service suspend the account of a minor.

A reference framework will be provided by the Regulatory Authority for Audiovisual and Digital Communication outlining the ways in which social media services may verify the age of users and parental authorisation.

¹³⁰ Outlined at [Digital Services Act](#), Articles 37, 40, 41 and 43.

¹³¹ See [Digital Services Act](#), Articles 49-51.

¹³² See [Digital Services Act](#), Article 52.

¹³³ 'The enforcement framework under the Digital Services Act', European Commission.

¹³⁴ [Digital Services Act](#), Article 74.

¹³⁵ Nomos, 'The introduction of a digital age of majority and new obligations for social networks', Lexology, 2 October 2023.

The French Law also introduces obligations for social media services to prevent online harassment by making anti-harassment messages visible to users, directing users to support structures, and enabling all users to report illicit content.¹³⁶

Penalties

Article 4 of the French Law outlines penalties for noncompliance. Failure to deliver a technical solution to verify the age of end-users and parental authorisation will result in a formal compliance notice being issued by the Audiovisual and Digital Communication Regulatory Authority. The provider has 15 days to respond. In the event of non-compliance, the Authority can refer the matter to the Paris Judicial Court for a court order. Failure to comply with the court order is punishable by a maximum fine of 1% of the provider's worldwide turnover for the preceding financial year.

Singapore

The [Online Safety \(Miscellaneous Amendments\) Act](#) (the Singapore Act) entered into force on 1 February 2023.¹³⁷

Code of Practice for Online Safety

Among other things, the Singapore Act empowers the Singaporean Info-communications Media Development Authority (IMDA) to designate social media services (SMSs) with significant reach or impact in Singapore to comply with online codes of practice. IMDA has issued a Code of Practice for Online Safety, which came into effect from 18 July 2023. Designated SMSs required to comply with the Code, are Facebook, HardwareZone, Instagram, TikTok, Twitter, and YouTube.¹³⁸ Subsection Aii of the [Code of Practice for Online Safety](#) outlines specific measures that designated SMSs must follow for the protection of children.

The code acknowledges that specific content is harmful to children and provides that services must develop, publish and follow community guidelines and standards which minimally address sexual content, violent content, suicide and self-harm content and cyberbullying content.¹³⁹ If children do search for high-risk content, the service must actively offer relevant safety information.¹⁴⁰ Further, children must not be targeted to receive content – including advertising and recommendations – that the services is 'reasonably aware to be detrimental to their physical or mental well-being'.¹⁴¹

136 [LOI n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne \(1\)](#) (French Law no. 2023-566 of July 7th 2023 implementing a digital age of majority and preventing online hate) (France), article 3.

137 Ministry of Communications and Information, '[Online Safety \(Miscellaneous Amendments\) Act Takes Effect on 1 February 2023](#)', media release, 31 January 2023.

138 Infocomm Media Development Authority, '[IMDA's Online Safety Code comes into effect](#)', media release, 17 July 2023.

139 Infocomm Media Development Authority, [Code of Practice for Online Safety](#), clause 17.

140 [Code of Practice for Online Safety](#), clause 22.

141 [Code of Practice for Online Safety](#), clause 18.

The code also provides that children or their guardians must be provided with tools and information to help manage their safety online.¹⁴² Significantly, child users must also be provided with differentiated accounts whereby:

the settings for the tools to minimise exposure and mitigate impact of harmful and/or inappropriate content and unwanted interactions are robust and set to more restrictive levels that are age appropriate by default.¹⁴³

Penalties

Where an online communication service (which includes SMSs) fails to satisfy its duty to take all reasonably practicable steps to comply with the Code of Practice, IMDA may impose a financial penalty of any amount it sees fit, up to S\$1 million, or may direct the provider to take certain steps within a specified time.¹⁴⁴ Failure to comply with such a direction is an offence subject to a possible fine of up to S\$1 million (and a further fine not exceeding S\$100,000 for every day or part-day which the offence continues after conviction).¹⁴⁵

Conclusion

Australia led the world with online safety regulation with the introduction of the *Enhancing Online Safety Act 2015* and the establishment of the eSafety Commissioner in 2015. Since then, many other countries have followed suit, introducing various laws aimed at protecting children online, specifically on social media platforms. A common feature among many international regulations is the use of age verification to provide modified accounts to children to protect them from harms, including age-inappropriate content, communication with strangers, addictive design features, recommender algorithms, and data collection.

While Australia's next step in online safety regulation – the development of industry codes for class 2 content – focusses on limiting children's access to pornography, the current trial of age verification technology for both pornography *and* general social media sites suggests that age restrictions on social media sites may also eventuate in Australia. The current review of the *Online Safety Act 2021*, due to report to the Minister by 31 October 2024, provides an opportunity for Australia to ensure its online regulation is up-to-speed in a fast-changing media landscape.¹⁴⁶

142 [Code of Practice for Online Safety](#), clauses 19–21.

143 [Code of Practice for Online Safety](#), clause 20.

144 [Online Safety \(Miscellaneous Amendments\) Act 2022](#) (Singapore), section 45N.

145 [Online Safety \(Miscellaneous Amendments\) Act 2022](#) (Singapore), section 45N(2).

146 '[Statutory Review of the Online Safety Act 2021](#)', Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

Licence

© Commonwealth of Australia



Creative Commons

With the exception of the Commonwealth Coat of Arms, and to the extent that copyright subsists in a third party, this publication, its logo and front page design are licensed under a [Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia](#) licence.

In essence, you are free to copy and communicate this work in its current form for all non-commercial purposes, as long as you attribute the work to the author and abide by the other licence terms. The work cannot be adapted or modified in any way. Content from this publication should be attributed in the following way: Author(s), Title of publication, Series Name and No, Publisher, Date.

To the extent that copyright subsists in third party quotes it remains with the original owner and permission may be required to reuse the material.

Inquiries regarding the licence and any use of the publication are welcome to webmanager@aph.gov.au.

Disclaimer

This work has been prepared to support the work of the Australian Parliament using information available at the time of production. The views expressed do not reflect an official position of the Parliamentary Library, nor do they constitute professional legal opinion.

For copyright reasons some linked items are only available to members of Parliament. All links are correct at the time of publication and are not subsequently updated.

Any concerns or complaints should be directed to the Parliamentary Librarian at webmanager@aph.gov.au. Parliamentary Library staff are available to discuss the contents of publications with Senators and Members and their staff. To access this service, clients may contact the author or the Library's Central Entry Point for referral.

Acknowledgement of Country

We acknowledge the traditional owners and custodians of country throughout Australia and acknowledge their continuing connection to land, waters and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

The Parliamentary Library of Australia was established in 1901 and serves as a trusted source of information, analysis and advice for the Australian Parliament. The Library is part of the Department of Parliamentary Services.

Our services are confidential, impartial, and offered on an equal basis to all parliamentarians, parliamentary committees, and to staff acting on their behalf.

Our published material is available to everyone at:



aph.gov.au/library



Australian Parliamentary Library



@ParlLibrary



Confidential, Impartial, Timely

ISSN 2203-5249