PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

Protecting the age of innocence

Report of the inquiry into age verification for online wagering and online pornography

House of Representatives Standing Committee on
Social Policy and Legal Affairs

February 2020
CANBERRA

ISBN 978-1-76092-068-5 (Printed Version)

ISBN 978-1-76092-069-2 (HTML Version)

Contents

Executive summary

The Committee's inquiry considered the potential role for online age verification in protecting children and young people in Australia from exposure to online wagering and online pornography.

Evidence to the inquiry revealed widespread and genuine concern among the community about the serious impacts on the welfare of children and young people associated with exposure to certain online content, particularly pornography.

The Committee heard that young people are increasingly accessing or being exposed to pornography on the internet, and that this is associated with a range of harms to young people's health, education, relationships, and wellbeing. Similarly, the Committee heard about the potential for exposure to online wagering at a young age to lead to problem gambling later in life.

Online age verification is not a new concept. However, the Committee heard that as governments have sought to strengthen age restrictions on online content, the technology for online age verification has become more sophisticated, and there are now a range of age-verification services available which seek to balance effectiveness and ease-of-use with privacy, safety, and security.

In considering these issues, the Committee was concerned to see that, in so much as possible, age restrictions that apply in the physical world are also applied in the online world.

The Committee recognised that age verification is not a silver bullet, and that protecting children and young people from online harms requires government, industry, and the community to work together across a range of fronts. However, the Committee also concluded that age verification can create a significant barrier to prevent young people—and particularly young children—from exposure to harmful online content.

The Committee's recommendations therefore seek to support the implementation of online age verification in Australia.

The Committee recommended that the Digital Transformation Agency lead the development of standards for online age verification. These standards will help to ensure that online age verification is accurate and effective, and that the process for legitimate consumers is easy, safe, and secure.

The Committee also recommended that the Digital Transformation Agency develop an age-verification exchange to support a competitive ecosystem for third-party age verification in Australia.

In relation to pornography, the Committee recommended that the eSafety Commissioner lead the development of a roadmap for the implementation of a regime of mandatory age verification for online pornographic material, and that this be part of a broader, holistic approach to address the risks and harms associated with online pornography.

In relation to wagering, the Committee recommended that the Australian Government implement a regime of mandatory age verification, alongside the existing identity verification requirements. The Committee also recommended the development of educational resources for parents, and consideration of options for restricting access to loot boxes in video games, including though the use of age verification.

The Committee hopes that together these recommendations will contribute to a safer online environment for children and young people.

Lastly, the Committee acknowledges the strong public interest in the inquiry and expresses its appreciation to the individuals and organisations that shared their views with the Committee.

Membership of the Committee

Chair

Mr Andrew Wallace MP

Deputy Chair

Ms Sharon Claydon MP

Members

Dr Mike Freelander MP

Mr Andrew Laming MP

Ms Peta Murphy MP

Mr Rowan Ramsey MP

Mr Julian Simmonds MP

Dr Anne Webster MP

Terms of reference

The House of Representatives Standing Committee on Social Policy and Legal Affairs will inquire into and report on age verification for online wagering and online pornography.

The inquiry will have particular regard to:

1. its potential as a mechanism for protecting minors online;
2. requirements of Commonwealth, state and territory government laws, policies and practices (including technical and privacy requirements) that relate to, and enable improved age verification requirements;
3. the potential benefits of further online age verification requirements, including to protect children from potential harm, and business and non-government organisations from reputation, operational and legal risks;
4. the potential risks and unintended consequences in further restricting age verification requirements, including, but not limited to:
    a. pushing adult consumers into unregulated/illegal environments or to other legal forms of these activities;
    b. privacy breaches;
    c. providing false assurance to parents and carers; and
    d. freedom of expression;
5. best practice age verification requirements internationally, including standards, verification and implementation timeframes, and particularly the likely effectiveness of the proposed age verification for access to online pornography in the United Kingdom's Digital Economy Act 2017;

6 barriers to achieving stronger age verification requirements, including but not limited to:

   a. capabilities of existing technology of business and verification providers;

   b. access, adequacy and security of third-party and government databases; and

   c. accurate and standardised capture of customer information;

7 education and warning messages associated with age verification;

8 the economic impact of placing further restrictions on age verification on business, including small business, and the potential financial and administrative burden of such changes;

9 the impact of placing further restrictions on age verification on other eSafety resourcing, education and messaging; and

10 Australia 's international obligations.

List of abbreviations

ACC	Australian Christian Churches
AIFS	Australian Institute of Family Studies
AML-CTF	Anti-Money Laundering and Counter-Terrorism Financing
AVC	Age Verification Certificate
AVPA	Age Verification Providers Association
BBFC	British Board of Film Classification
DEA	United Kingdom *Digital Economy Act 2017*
DTA	Digital Transformation Agency
DVS	Document Verification Service
EBT	Electronic Betting Terminal
FVS	Face Verification Service
GDPR	European Union General Data Protection Regulation
INHOPE	International Association of Internet Hotlines
ISP	Internet-service provider
NFC	Near-field-communication
PAS	Publicly Available Specification
RGF	NSW Responsible Gambling Fund
RWA	Responsible Wagering Australia
SbD	Safety by Design initiative
TDIF	Trusted Digital Identity Framework

UNSW	University of New South Wales
VACCA	Victorian Aboriginal Child Care Agency
VPN	Virtual private network
VRGF	Victorian Responsible Gambling Foundation
WACSS	WA Child Safety Services

List of recommendations

Recommendation 1

2.143 The Committee recommends that the Digital Transformation Agency, in consultation with the Australian Cyber Security Centre, develop standards for online age verification for age-restricted products and services.

a. These standards should specify minimum requirements for privacy, safety, security, data handling, usability, accessibility, and auditing of age-verification providers.

b. Consideration should be given to the existing technical standards in Australia and overseas, including but not limited to the UK Age Verification Certificate, the PAS 1296 Age Checking code of practice, the Trusted Digital Identity Framework, and the European Union General Data Protection Regulation.

c. Opportunities should also be provided for consultation with industry, including private age-verification providers, and members of the public.

Recommendation 2

2.148 The Committee recommends that the Digital Transformation Agency extend the Digital Identity program to include an age-verification exchange for the purpose of third-party online age verification.

Recommendation 3

3.184 The Committee recommends 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, setting out:

a. a suitable legislative and regulatory framework;

b. a program of consultation with community, industry, and government stakeholders;

c. activities for awareness raising and education for the public; and

d. recommendations for complementary measures to ensure that age verification is part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.

Recommendation 4

4.61 The Committee recommends that the Australian Government, through the National Consumer Protection Framework for Online Wagering, introduce a requirement that customers are not able to use an online wagering service prior to verification of their age as 18 years or over.

Recommendation 5

4.66 The Committee recommends that the Office of the eSafety Commissioner or other relevant government department report to the Australian Government on options for restricting access to loot boxes and other simulated gambling elements in computer and video games to adults aged 18 years or over, including through the use of mandatory age verification.

Recommendation 6

4.68 The Committee recommends that the Office of the eSafety Commissioner develop educational resources to inform parents of the risks and harms associated with online gambling and assist parents to reduce children and young people's exposure to online gambling.

1. Introduction

1.1 Children and young people are increasingly growing up in an online world.

1.2 According to the Australian Bureau of Statistics, in 2016-17, 97 per cent of Australian households with children under 15 years of age had access to the internet, and the highest proportion of internet users of any age group was among people aged 15 to 17.[1]

1.3 The internet has brought about new opportunities for children and young people to learn, play and connect with friends and family. However, while taking advantage of these new opportunities, it is also important that children and young people are protected online.

1.4 This includes ensuring that age restrictions that apply to content or services offline in the physical world are also applied in the online world.

1.5 This inquiry considered the potential role for age-verification technology in protecting children and young people in Australia from exposure to online wagering and online pornography.

Related inquiries

1.6 In December 2015, the Senate Environment and Communications References Committee adopted an inquiry into harm being done to Australian children through access to pornography on the internet. The inquiry lapsed at the dissolution of the Parliament in May 2016, and was adopted again in September 2016.[2]

---

[1] Australian Bureau of Statistics, *Household Use of Information Technology, Australia, 2016-17*, <https://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0>.

[2] Senate Environment and Communication References Committee, *Harm being done to Australian children through access to pornography on the Internet*, November 2016, p. 1.

1.7 The Committee presented its report in November 2016, making four recommendations. These recommendations included that the Australian Government commission dedicated research into the exposure of Australian children and young people to online pornography, and that, following this research, the Government commission an expert panel to make recommendations regarding possible policy measures.[3]

1.8 The Government response to the report was published in April 2017.[4]

1.9 The response stated that the Government had commissioned the Australian Institute of Family Studies to review evidence on the effects of pornography on children and young people. The review was subsequently published in December 2017. Key messages included that pornography use can shape sexual practices and is associated with unsafe sexual health practices, and that pornography may strengthen attitudes supportive of sexual violence and violence against women.[5]

1.10 The response also stated that the Government would ask the Online Safety Consultative Working Group, chaired by the eSafety Commissioner, to consider the issue and report back to Government on strategies to inform an effective policy response. The group made recommendations to Cabinet in December 2017.[6]

The current inquiry

1.11 The Minister for Families and Social Services, Senator the Hon. Anne Ruston, and the Minister for Communications, Cyber Safety and the Arts, the Hon. Paul Fletcher MP, wrote to the Committee requesting that it inquire into and report on age verification for online wagering and online pornography.

---

[3] Senate Environment and Communication References Committee, *Harm being done to Australian children through access to pornography on the Internet*, November 2016, p. vii.

[4] Department of Communications and the Arts, *Australian Government response to Senate References Committee on Environment and Communications report: Harm being done to Australian children through access to pornography on the Internet*, April 2017, <https://www.communications.gov.au/publications/australian-government-response-senate-references-committee-environment-and-communications-report>.

[5] Australian Institute of Family Studies, *The effects of pornography on children and young people – An evidence scan*, 2017.

[6] Office of the eSafety Commissioner, *Annual report 2017–18*, p. 136. See also: Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 11.

1.12 On 10 September 2019, the Committee adopted the terms of reference referred by the Ministers. The full terms of reference are provided in the front pages of this report.

Conduct of the inquiry

1.13 The inquiry was advertised on 11 September 2019. Submissions were invited from a range of government, industry and community organisations and from other relevant stakeholders, and opened to the public.

1.14 On 11 September 2019 the Committee published a statement outlining principles for its treatment of evidence received by the inquiry. The statement is included at Appendix A.

1.15 The Committee received 325 submissions and two supplementary submissions, which are listed at Appendix B. The Committee also received four exhibits, which are listed at Appendix C.

1.16 Submissions to the inquiry included a significant number of contributions from groups of individuals or campaigns, including:

- 219 contributions received via eChildhood;
- 87 identical and 50 similar contributions based on a form letter;
- 30 identical and 36 similar contributions based on another form letter;
- 2236 contributions received via the online advocacy organisation OneClickPolitics; and
- 707 short contributions in similar terms.

1.17 Consistent with the approach taken by other Parliamentary Committees, one example of each form letter was accepted as a submission and published on the inquiry web page. Where multiple submissions were sent to the Committee as a group or contained similar text, these were published as a compilation.

1.18 The Committee heard from witnesses at two public hearings in Canberra on 5 and 6 December 2019. Witnesses are listed at Appendix D.

1.19 The Committee also notes that it received some submissions addressing the issue of age verification for online alcohol sales. While this was outside the scope of the inquiry, the Committee carefully considered the matters raised in these submissions.

1.20 The Committee acknowledges the strong community interest in the inquiry and expresses its appreciation to the individuals and organisations that contributed evidence and shared their views with the Committee.

Structure of the report

1.21 Chapter 2 summarises evidence received on the attributes of an effective online age-verification model, and then reviews the current state-of-the-art methods for age verification.

1.22 Chapter 3 considers evidence on children and young people's exposure to online pornography. The chapter then considers how online pornography is currently regulated in Australia, approaches in other jurisdictions, and the possible implementation of a mandatory regime for age verification for online pornography in Australia.

1.23 Chapter 4 considers evidence on online wagering by children and young people. The chapter then examines Australia's current verification process for access to online wagering, the planned review of this process, approaches in other jurisdictions, and other possible measures.

2. Methods for online age verification

2.1 The terms of reference for the inquiry required the Committee to consider the potential of online age verification as a mechanism for protecting children and young people from exposure to certain forms of age-restricted content.

2.2 As such, the Committee was interested in evidence on how online age-verification works in practice to verify that an internet user is aged 18 years or above, and how this can be done easily, safely, and securely.

2.3 The Committee heard that while the concept of online age verification is not new, initial methods involved simply displaying an adults-only warning, requiring a user to input their date of birth, or requiring a user to scan or mail a copy of an identity document.[1]

2.4 The Age Verification Providers Association (AVPA) explained that these initial methods were easily evaded, and were not adequate in circumstances where legislation imposed age restrictions.[2]

2.5 Similarly, the eSafety Commissioner submitted that the 'digital ecosystem for third-party verification and in-person proofing was not sufficiently evolved' to proceed with a pilot of age verification attempted by Microsoft in Australia in 2008.[3]

[1] Age Verification Providers Association, *Submission 200*, p. 3.

[2] Age Verification Providers Association, *Submission 200*, p. 3.

[3] eSafety Commissioner, *Submission, 191*, p. 8.

2.6 However, more recently, as technology has developed and as some jurisdictions have sought to strengthen age restrictions on certain forms of online content, age verification has become an area of increased interest, leading to the development of more sophisticated methods.

2.7 This chapter summarises evidence received on the attributes of an effective online age-verification model, and then reviews the current state-of-the-art methods for age verification. Evidence in relation to the application of age verification to online pornography and online wagering is discussed in subsequent chapters of this report.

Attributes of an effective age-verification model

2.8 While the Committee heard about a range of age-verification methods (discussed later in this chapter), the Committee also received more general evidence on attributes or features that an effective online-age verification model should possess.

2.9 This evidence, which may serve to inform the implementation of any future regime for online age-verification in Australia, is summarised in three sections addressing the following themes:

- privacy and security;
- accuracy and effectiveness; and
- impact on business and users.

Privacy and security

2.10 A consistent theme in evidence to the inquiry was the importance of any system for online age verification having strong controls for the safety, security, and privacy of users.

2.11 For example, the eSafety Commissioner submitted:

> The importance of balancing privacy, security and safety considerations is essential. Any age verification proposal in Australia that mandates the use of technology should include and make explicit reference to data protection, privacy and safety.[4]

2.12 Similarly, consumer credit agency Equifax submitted that 'strong privacy controls will be critical'. Equifax offered the following points for consideration:

[4] eSafety Commissioner, *Submission 191*, p. 14.

- Minimise, or if possible, eliminate, the retention of any record of age-verification, including a prohibition on disclosure or reuse of any personal information relating to a request for age verification;
- 18+ sites should not know who a viewer is, only know that a person viewing or using the site has been verified as 18+;
- Similarly, the entity verifying age should not know what site the person wishes to view, only that age verification has been requested;
- The age verification process should be conducted using the minimum details required to achieve a match;
- In a more mature identity environment, people could choose to obtain a reusable age-verification token for them to provide when needed.[5]

2.13 The University of New South Wales (UNSW) Law Society raised concerns in relation to the collection and management of personal information and potential breaches of privacy:

> There are many questions that exist ... such as: whether users will be given notice around the storage of their information; to what extent can users consent to the manner in which their data is utilised; whether it is certain that unauthorised disclosure of personal information will not occur. ...the effectiveness of age verification is thus contingent upon the ability to safeguard [an] individual's security details.[6]

2.14 The eSafety Commissioner also highlighted the importance of requirements for data storage.[7]

2.15 The AVPA recommended that personal data should not be retained unless required:

> ... where there is no need to retain an audit trail of age verifications, then personal data should not be retained, thus vastly minimising the risk of a privacy breach.
>
> Where an audit trail is required by regulators or the law, still personal data need not be retained, rather only the pseudonimised record of the verification events themselves.[8]

[5] Equifax, *Submission 189*, pp. 2-3.

[6] UNSW Law Society, *Submission 58*, p. 7.

[7] eSafety Commissioner, *Submission 191*, p. 11.

[8] Age Verification Providers Association, *Submission 200*, pp. 4-5.

2.16 Mr Alastair MacGibbon, former eSafety Commissioner and former National Cyber Security Adviser, told the Committee that while 'there is no such thing as absolute security, safety or privacy online', technology was sufficient to provide services in the 'vast bulk of cases' involving age-restricted content.[9]

2.17 However, Mr MacGibbon also suggested that individuals with concerns about privacy 'will be forced into darker parts of the web to avoid verification'.[10] A similar suggestion was made by the UNSW Law Society.[11]

2.18 Dr Julia Fossi, Expert Advisor at the Office of the eSafety Commissioner, stressed the importance of independent auditing and monitoring of age-verification technologies and raising public awareness of safeguards that may be in place.[12]

Identity protection and third-party verification

2.19 The Committee was made aware of the distinction between age verification and identity verification.[13]

2.20 Several submitters noted that age verification only requires checking of one attribute of an individual's identity—age-related eligibility (that is, whether or not the individual is over a particular age).[14]

2.21 For example, Mr Iain Corby, Executive Director of the AVPA, explained:

> ... age verification is not identity verification. They're very separate. What we try to do is have the minimum amount of data used in the first place and then retained going forward. For quite a lot of uses, you wouldn't need to retain any personal data at all. All you need to know is that person X—and we only know them as 'X'—has at some point proved, to a certain standard, that they are over a particular age or within a particular age range or they have a particular date of birth.[15]

---

[9] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, p. 24.

[10] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, p. 26.

[11] UNSW Law Society, *Submission 58*, p. 8.

[12] Dr Julia Fossi, Expert Advisor, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 16. See also: eSafety Commissioner, *Submission 191*, p. 5.

[13] eSafety Commissioner, *Submission 191*, p. 5.

[14] See, for example: eChildhood, *Submission 192*, pp. 24-25; Equifax, *Submission 189*, p. 1.

[15] Mr Iain Corby, Executive Director, Age Verification Providers Association, *Committee Hansard*, Canberra, 5 December 2019, p. 7.

2.22 Similarly, online compliance provider TrustElevate submitted:

> Traditionally, to verify that an individual is, for example, 18+ years of age, the collection of a significant amount of personal data, including name, address, and date of birth, is required. In effect, age verification involves a full identity verification process. Recent technology and policy innovations in the electronic identity sector mean that it is now possible for age check services to check a single attribute of an individual's identity (i.e. age-related eligibility).[16]

2.23 The Committee heard that disclosure of personal information could be minimised through the use of third-party age verification, which involves verification being carried out by an entity that is separate from the age-restricted service.

2.24 Ms Amelia Erratt, Head of Age Verification at the British Board of Film Classification (BBFC), explained:

> In terms of the age verification solutions that we were looking at, for the most part age verification is provided by a third party, which means that you don't give your personal data to [an age-restricted] website; you leave the website and carry out your age verification separately.[17]

2.25 Mr Peter Alexander, Chief Digital Officer at the Digital Transformation Agency (DTA), likened third-party verification to the authentication process used in some online transactions:

> ... sometimes when you make a purchase online, before the sale is finalised you are referred to a banking institution or credit card domain to enter a two-factor authentication code. Once you've successfully verified the two-factor authentication code, you are returned to the retailer's website.[18]

2.26 Mr Matt Strassberg, General Manager of External Relations in Australia and New Zealand at Equifax, stated that it was his expectation that age-restricted sites would not be responsible for age verification:

> You'll be redirected by a third party, so that way there's separation between the verification and the [age-restricted] site.

---

[16] TrustElevate, *Submission 190*, p. 1.

[17] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 5.

[18] Mr Peter Alexander, Chief Digital Officer, Digital Transformation Agency, *Committee Hansard*, Canberra, 6 December 2019, p. 42.

> ... We don't want to know what site you're going to, nor should the [age-restricted] site know who you are.[19]

2.27 Representatives of the DTA described the process of third-party verification as 'privacy enhancing' as it involved the age-restricted site only receiving a 'yes/no answer' about whether the user was aged 18 years or above rather than providing documents directly to the age-restricted site.[20]

Accuracy and effectiveness

2.28 The Committee received limited evidence in relation to the accuracy and effectiveness of online age verification. (Evidence on compliance with age-verification requirements for age-restricted content is discussed in subsequent chapters.)

2.29 However, a consistent theme in evidence was that while age verification was not a 'silver bullet', with appropriate standards in place, the technology could provide a barrier to prevent young people—and particularly young children—from inappropriately accessing age-restricted content.

2.30 Mr Corby suggested that online age verification could be applied in a proportionate manner:

> For some things you would never want anybody to scrape through whereas for other things you might not be quite so concerned. ...You can scale up or down as appropriate, and that's important because you want to allow the wheels of commerce to keep turning without too much extra friction, so you only want to ask the questions you really need to.[21]

2.31 Ms Erratt told the Committee that the BBFC was aware of age-verification solutions that were 'very accurate', but that it was a matter of setting robust standards:

> For example, we required that the type of data be data that was only known by that person rather than broadly known. Age, name and address, for

---

[19] Mr Matt Strassberg, General Manager, External Relations Australia and New Zealand, Equifax, *Committee Hansard*, Canberra, 6 December 2019, pp. 39-40.

[20] Mr Peter Alexander, Chief Digital Officer, Digital Transformation Agency, *Committee Hansard*, Canberra, 6 December 2019, p. 42; Mr Jonathon Thorpe, Head of Identity, Digital Delivery Division, Digital Transformation Agency, *Committee Hansard*, Canberra, 6 December 2019, p. 42

[21] Mr Iain Corby, Executive Director, Age Verification Providers Association, *Committee Hansard*, Canberra, 5 December 2019, p. 7.

> example, could not be an acceptable dataset to age verify, because that is information that could be reasonably known by another person.[22]

2.32 As discussed later in this chapter, the Committee heard that age-estimation software could be configured to meet different accuracy thresholds.[23] The AVPA provided evidence on the accuracy of age estimation based on photos or videos:

> For a jurisdiction with legal age restriction of 18, and a threshold set to 25 years, the latest technology's current mean error rate is 0.31%. For a threshold of 23 years, the error rate is 0.75%. In other words, accuracy is over 99% if the system is set to allow only customers who its analytics conclude are over 23 based on their image. Even a solution reliant on a passport, identity card or driving licence might only offer a percentage level of accuracy, after accounting for the risks of forgery, impersonation or theft. This is no different from the offline world, where there are no systems which offer 100% verification – even passport checks at borders will miss some fake or recently stolen passports.[24]

2.33 Mr Robin Toombs, Chief Executive Officer of Yoti, submitted that it was 'quite difficult' for children nine to 13 years of age to fool Yoti's age-estimation system.[25]

2.34 The eSafety Commissioner, Ms Julie Inman-Grant, suggested that further work was required for automated facial recognition to be 'precisely accurate':

> I think we have a long way to go in terms of [artificial intelligence] and machine learning and also recognising different skin tones and ethnicities. There are a lot of complexities there.[26]

2.35 Some submitters note that online age verification may be circumvented using tools such as virtual private networks (VPNs), thereby limiting its

---

[22] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 5.

[23] Yoti, *Submission 172*, p. 11.

[24] Age Verification Providers Association, *Submission 200*, p. 4.

[25] Mr Robin Toombs, Chief Executive Officer, Yoti, *Committee Hansard*, Canberra, 6 December 2019, p. 30.

[26] Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 18. See also: Yoti, *Submission 172*, p. 11.

effectiveness. For example, Mr Chern Eu Kuan, Student Contributor at the UNSW Law Society, explained:

> Several factors suggest that the effectiveness of age verification is limited, the biggest concern being the various techniques that minors can easily employ to circumvent verification. ... In a real-world implementation of age verification, the use of a VPN would allow internet users to virtually relocate to a country without age verification and access a website as easily as they would be able to outside of Australia.[27]

2.36 Mr Kuan cited a study of 13- to 15-year-olds undertaken by Family Zone:

> ... they installed internet filters on children's devices and found that nearly two-thirds of 13- to 15-year-olds were trying to use VPN services to access pornography.[28]

2.37 However, Ms Erratt said the BBFC's research indicated that a smaller percentage of 11- to 13-year-olds claimed to know how to circumvent age verification:

> We know that there are going to be tech-savvy teenagers who find ways to circumvent the legislation. From our research, though, we've found that only 14 per cent of 11- to 13-year-olds claim that they know a workaround like the dark web or like VPN.[29]

2.38 The Alliance for Gambling Reform suggested that further research was required to understand the extent to which children are circumventing age verification.[30]

2.39 Ms Erratt suggested that age verification should not be seen as a 'silver bullet':

> We have always acknowledged that age verification is not a silver bullet, but without a doubt it can prevent young children from stumbling across

---

[27] Mr Chern Eu Kuan, Student Contributor, UNSW Law Society, *Committee Hansard*, Canberra, 6 December 2019, p. 47.

[28] Mr Chern Eu Kuan, Student Contributor, UNSW Law Society, *Committee Hansard*, Canberra, 6 December 2019, p. 47. See also: UNSW Law Society, *Submission 58*, p. 6; Family Zone, *Submission 202*, p. 2.

[29] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 4.

[30] Alliance for Gambling Reform, *Submission 179*, p. 2.

> commercial pornography online. With online regulation, no single solution will be perfect, but that shouldn't prevent action being undertaken.[31]

2.40 This sentiment was shared by a number of other stakeholders, who argued that age verification would create a significant barrier and prevent inadvertent access to age-restricted sites.[32] This evidence, particularly as it relates to online pornography, is discussed in further detail in the following chapter.

2.41 Speaking more generally, Mr MacGibbon emphasised that approaches to regulation on online activity should not be expected to be perfect:

> ... when it comes to solutions online, you'll often hear where they'll fail. Yet offline we accept the fact that there are edge cases and people who will be unintended victims ...of regulation or of activities. We accept the fact that seatbelts save lives but not every life, but we still mandate the wearing of seatbelts. When it comes to online regulation or online intervention or online behaviours, there is a prevailing philosophy that says that everything needs to be perfect or you should do nothing, and that, if you do try to do something, it will be completely ineffective anyway...I think we see the consequences of that market failure today in a whole range of things whether it is online safety, online security or privacy.[33]

Impact on business and users

2.42 The Committee heard a range of views on the impact on businesses and users of implementing online age verification for age-restricted content or services. Evidence highlighted the importance of minimising the burden for businesses and giving users a choice of age-verification methods.

2.43 The BBFC submitted that age verification was a 'simple and affordable option' for online platforms:

> ... in order to ensure that these solutions were not prohibitively expensive, age-verification providers have developed products which have significantly reduced the cost of age-verification. In fact, a number of age-verification providers were planning to offer age-verification free to online commercial pornographic services and most have services which are completely free to

---

[31] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, pp. 2, 4.

[32] For example, see: Collective Shout, *Submission 178*, pp. 10-11; British Board of Film Classification, *Submission 187*, p. 1; eChildhood, *Submission 192*, p. 22; Age Verification Providers Association, *Submission 200*, p. 5.

[33] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, pp. 23-24.

> consumers. The reason that this is possible is because age-verification services online can drive uptake for services offline which can be monetised such as age-verification for restricted products such as alcohol and cigarettes or entry to nightclubs.[34]

2.44 Similarly, TrustElevate submitted that business could perform age verification for free or at low cost:

> The commercial models that underpin an identity ecosystem can be flexible enough to enable businesses that are not generating sufficient revenue, to run checks at a lower cost, or free, which mitigates concerns around stifling innovation or the imposition of overly burdensome costs.[35]

2.45 However, Eros Association expressed concern about the 'red-tape burden' on producers of age-restricted content associated with mandatory age-verification controls.[36]

2.46 The Committee received further evidence in relation to the regulatory burden of identity verification for online wagering, which is discussed in Chapter 4.

2.47 In relation to users, Dr David Sandifer suggested that online age verification was 'minimally inconvenient':

> Those adults who wish to access online [age-restricted content] are not prevented from doing so: they merely need to confirm their adult status, as they would when buying alcohol or cigarettes.[37]

2.48 Several witnesses stressed the importance of making available a range of options for age verification. For example, Ms Erratt told the Committee:

> It's ...important that consumers trust age verification systems. They need to be aware that they have a choice of options available to them and know how to age-verify safely.[38]

---

[34] British Board of Film Classification, *Submission 187*, p. 12.

[35] TrustElevate, *Submission 190*, p. 3.

[36] Eros Association, *Submission 65*, p. 3.

[37] Dr David Sandifer, *Submission 171*, p. 3.

[38] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 1.

2.49 Similarly, Mrs Liz Walker, Deputy Chair of eChildhood, argued that user choice, as well as assurances about safety, security, and privacy, would 'lead to less resistance' to age verification.[39]

2.50 Mr Strassberg suggested that having a range of options for age verification would dissipate risks to security and empower users. Mr Strassberg also noted that there may be reluctance about using government-issued identity documents.[40]

2.51 Similarly, Mr Toombs told the Committee that choice was 'very important':

> I think there will be some people who are comfortable putting a photo ID into an age verification system, whether that be a government checking system or a private age verification provider. I think there will be lots of other people who feel they would rather find another way ... to prove their age...[41]

Technical standards for age verification

2.52 In evidence to the inquiry, there was general support for a standards-based approach to the implementation of online age verification.

2.53 For example, the eSafety Commissioner submitted that one of the 'main preconditions' for implementing a mandatory age verification scheme was 'the establishment of a trusted age verification framework for implementation, that sets out robust technical standards, requirements and conditions for age verification mechanisms that fully address privacy, data protection, security, safety, usability, and accessibility considerations'.[42]

2.54 The AVPA argued that there are a range of benefits to establishing a common standard for age verification, including that such a standard would:

- provide a basis for a competitive, interoperable marketplace, improving choice and quality for consumers while keeping prices down;
- provide a basis for educating the public about age verification and its effectiveness; and

---

[39] Mrs Liz Walker, Deputy Chair, eChildhood, *Committee Hansard*, Canberra, 6 December 2019, p. 56.

[40] Mr Matt Strassberg, General Manager, External Relations Australia and New Zealand, Equifax, *Committee Hansard*, Canberra, 6 December 2019, p. 39.

[41] Mr Robin Toombs, Chief Executive Officer, Yoti, *Committee Hansard*, Canberra, 6 December 2019, pp. 28-29.

[42] eSafety Commissioner, *Submission 191*, p. 5.

- enable a proportionate response depending on the risks associated with each age-restricted product or service, where the industry can provide standardised solutions to meet a given level of assurance and audit.[43]

2.55 Evidence received by the Committee relating to different approaches to establishing technical standards for online age verification is outlined in this section.

Guidance provided under the UK Digital Economy Act

2.56 The Committee heard about the approach of the BBFC as the designated age-verification regulator for online pornography under the Digital Economy Act in the United Kingdom. The Digital Economy Act is discussed in further detail in the following chapter.

2.57 Under section 14(1) of the Act:

> ... all providers of online commercial pornographic material accessible from the UK would have been required to carry age-verification arrangements for UK consumers to ensure that their content is not normally accessible to children.[44]

2.58 As the age-verification regulator, the BBFC was required to publish 'guidance about the types of arrangements for making pornographic material available that the regulator will treat as complying with section 14(1).'[45]

2.59 In its submission to the inquiry, the BBFC set out criteria against which age-verification providers would have been assessed for compliance with the Act, including:

> a) an effective control mechanism at the point of registration or access to pornographic content by the end-user which verifies that the user is aged 18 or over at the point of registration or access
>
> b) use of age-verification data that cannot be reasonably known by another person, without theft or fraudulent use of data or identification documents nor readily obtained or predicted by another person
>
> c) a requirement that either a user age-verify each visit or access is restricted by controls, manual or electronic, such as, but not limited to, password or

[43] Age Verification Providers Association, *Submission 200*, pp. 3-4.

[44] British Board of Film Classification, *Submission 187*, pp. 6-7.

[45] British Board of Film Classification, *Submission 187*, pp. 6-7.

personal identification numbers. A consumer must be logged out by default unless they positively opt-in for their log-in information to be remembered

d) the inclusion of measures which authenticate age-verification data and measures which are effective at preventing use by non-human operators including algorithms.[46]

2.60 The BBFC described this as a 'principles-based approach':

> We opted for a principle-based approach rather than specifying a finite number of "approved" solutions, to allow for and encourage technological innovation within the age-verification industry. In the years we worked on the project, we have seen significant advances in this area, notably the development of age estimation technology which had the potential to be both robust and easy to use for consumers.[47]

Age Verification Certificate

2.61 In addition to providing guidance to age-verification providers, the BBFC established a voluntary, non-statutory certification scheme—the Age Verification Certificate (AVC).[48]

2.62 The BBFC explained:

> The AVC Standard was developed by the BBFC and [cyber security and risk mitigation firm] NCC Group in cooperation with industry, with the support of Government, including the National Cyber Security Centre at GCHQ and Chief Scientific Advisors, and in consultation with the [Information Commissioner's Office]. Under the AVC, age-verification providers may choose to be independently audited by NCC, who are experts in cyber security and data protection, and then certified by the BBFC.
>
> The third party audit by NCC includes an assessment of an age-verification provider's compliance with strict privacy and data security requirements. These are tailored specifically to address age-verification for online pornography, for example by ensuring there is no handover of personal data

[46] British Board of Film Classification, *Submission 187*, p. 7.

[47] British Board of Film Classification, *Submission 187*, p. 7. See also: Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 3.

[48] British Board of Film Classification, *Submission 187*, p. 11.

> used to verify an individual's age between AV providers and pornographic websites.[49]

2.63 Ms Erratt explained that age-verification providers would be able to display a symbol to confirm that they had been certified. Users would be able to click on the symbol, which would take them to the BBFC website where they could view a summary report on the provider:

> The purpose of the age verification certificate is really to provide that comfort to consumers and ensure that they're confident in using age verification. It also gives age verification providers an opportunity to demonstrate that their solutions meet robust data protection standards.[50]

2.64 Ms Erratt told the Committee that, while the AVC was voluntary, 'all of the major age verification providers wanted to be certified under that scheme'.[51] According to the BBFC website, one provider (Yoti) achieved certification on 1 July 2019 and others are undergoing assessment.[52]

2.65 eChildhood noted that, under the Digital Economy Act, the BBFC would have been required to review age verification on all pornography websites accessible in the UK to ensure compliance with BBFC guidance, independent of the voluntary certification process.[53]

PAS 1296 Age Checking code of practice

2.66 As another example of an effort to develop technical standards for age verification, the Committee heard evidence about the Publicly Available Specification (PAS) 1296 Age Checking code of practice. PAS 1296 was published by the British Standards Institute in March 2018.[54]

2.67 Dr Rachel O'Connell, author of PAS 1296 and also Co-founder of TrustElevate, submitted that the standard was written to assist age-verification providers to comply with legal requirements:

---

[49] British Board of Film Classification, *Submission 187*, p. 11.

[50] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, pp. 1, 3, 6.

[51] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 6.

[52] British Board of Film Classification, 'Age-verification Certificate', <https://bbfc.co.uk/about-classification/age-verification-certificate>.

[53] eChildhood, *Submission 192*, pp. 19-20.

[54] TrustElevate, *Submission 190*, p. 1.

> [PAS 1296] provides recommendations on the due diligence businesses can exercise to ensure that age check services deliver the kind of solution that meet a business's specific regulatory compliance needs.[55]

2.68 Dr O'Connell told the Committee that the challenge in developing PAS 1296 was how to 'enable age-related eligibility checks to be conducted in a privacy-preserving manner'.[56]

2.69 Dr O'Connell explained that PAS 1296 uses a 'vectors of trust' approach, comprised of four components:

1. identity proofing (how strongly the set of identity attributes has been verified and vetted);
2. primary credential usage (how strongly the primary credential can be verified);
3. primary credential management (the use and strength of policies, practices, and security controls used in managing the credential); and
4. assertion presentation (how well the given digital identity can be communicated across the network without information leaking to unintended parties, and whether the given digital identity was actually asserted by the given identity provider and not another party posing as such).[57]

Trusted Digital Identity Framework

2.70 Beyond age verification, the Committee also heard about privacy and security standards associated with the Australian Government's Digital Identity program, led by the DTA in partnership with other government agencies.[58]

2.71 The Digital Identity program is intended to give Australian people and businesses a single, secure way to authenticate their identity for the purpose of accessing government services online.[59]

---

[55] TrustElevate, *Submission 190*, p. 1.

[56] Dr Rachel O'Connell, Co-founder, TrustElevate, *Committee Hansard*, Canberra, 5 December 2019, p. 12.

[57] TrustElevate, *Submission 190*, pp. 2-3. See also: Dr Rachel O'Connell, Co-founder, TrustElevate, *Committee Hansard*, Canberra, 5 December 2019, pp. 12-13.

[58] Digital Transformation Agency, *Submission 188*, pp. 1-2.

[59] Digital Transformation Agency, 'Digital Identity', <https://www.dta.gov.au/our-projects/digital-identity>.

2.72 The DTA explained that identity providers wishing to participate in the Digital Identity system must meet 'strict privacy and security requirements' set out in the DTA's Trusted Digital Identity Framework (TDIF).[60]

2.73 Mr Alexander, Chief Digital Officer at the DTA, explained:

> [The TDIF] has been developed in close cooperation with industry, government, academia and privacy experts. It sets rules and requirements for accreditation under the digital identity program, while participants in the digital identity program must be compliant with the TDIF, it is also freely available as a framework for all Australian businesses today as a reference for best practice and how to verify identity online.[61]

2.74 According to the DTA's website, the TDIF is currently made up of a set of 19 policies, which outline rules and standards for:

- how personal information is handled by participating government agencies and organisations;
- the usability and accessibility of identity services;
- how the identity system is secured and protected against fraud;
- how identity services are managed and maintained; and
- how [the TDIF] will be managed.[62]

2.75 eChildhood suggested that the TDIF could be modified to support an online age-verification regime.[63] The Committee heard that Australia Post was already providing age-verification services for alcohol purchasing and entry to licensed venues in some jurisdictions with its Digital iD solution, which is accredited under the TDIF.[64]

2.76 The DTA submitted that Digital Identity could be used to verify identity attributes, including age, for the purpose of accessing age-restricted sites:

> Such sites would only receive the information required to confirm the user meets the age requirements of the service. Other information could potentially

[60] Digital Transformation Agency, *Submission 188*, p. 2.

[61] Mr Peter Alexander, Chief Digital Officer, Digital Transformation Agency, *Committee Hansard*, Canberra, 6 December 2019, p. 41.

[62] Digital Transformation Agency, 'Trusted Digital Identity Framework', <Trusted Digital Identity Framework>.

[63] eChildhood, *Submission 192*, pp. 22-27.

[64] Australia Post, *Submission 199*, pp. 2-4.

> be provided, but this would be consent based to ensure the [user's] privacy is protected.[65]

2.77 However, Mr Alexander told the Committee that while there would be some benefits to using the Digital Identity program for online age verification, the DTA would need legislative authority for the program to connect directly to services in the private sector, and further investment would be required as age verification was not in the original scope of the program.[66]

2.78 The DTA recommended that if Digital Identity is used for age verification, it should be an optional choice:

> We would expect that [Digital Identity] would only be one of a number of potential pathways that individuals may use to undertake age verification.[67]

European Union General Data Protection Regulation

2.79 Some submitters noted that age-verification providers in the United Kingdom have been required to comply with the European Union General Data Protection Regulation (GDPR).[68]

2.80 The eSafety Commissioner explained that under the GDPR, when collecting and processing personal information, age-verification providers must comply with a range of data protection and data minimisation requirements, including:

- individuals must be told why, when, where and how their personal data is being processed, and by which organisations;
- providers must process the minimum personal data necessary to achieve the intended outcome of confirming age; additional personal data should not be collected, irrespective of whether it is subsequently securely deleted;
- providers must facilitate individuals' rights (including the rights of access, erasure and rectification); and

[65] Digital Transformation Agency, *Submission 188*, p. 2.

[66] Mr Peter Alexander, Chief Digital Officer, Digital Transformation Agency, *Committee Hansard*, Canberra, 6 December 2019, pp. 42-43.

[67] Digital Transformation Agency, *Submission 188*, p. 2.

[68] British Board of Film Classification, *Submission 187*, p. 10; eSafety Commissioner, *Submission 191*, pp. 10, 12-13; Age Verification Providers Association, *Submission 200*, p. 4.

- providers must ensure that personal data is not retained for longer than is necessary to achieve the purposes for which it was originally collected (sometimes referred to as individuals' 'right to be forgotten').[69]

Overview of methods for online age verification

2.81 As noted at the beginning of this chapter, the Committee heard that online age verification had become an area of increased interest and technological development as some jurisdictions had sought to enforce age restrictions for online content.

2.82 The eSafety Commissioner explained that age-verification technology is evolving quickly:

> There has been increased investment in the development of online age verification, age-assurance, age checking and e-identification systems over the last few years, and a broad suite of technologies now currently exist.[70]

2.83 The eSafety Commissioner went on:

> ... a number of third-party information and analytics companies exist to provide identity and age verification checks on consumers, as well as credit checks and fraud assessments.[71]

2.84 A number of commercial age- and identity-verification providers gave evidence to the inquiry, in addition to a number of government agencies involved in developing age- and identity-verification platforms.[72]

2.85 This section summarises the main methods of online age verification discussed in evidence to the inquiry, which involve verification based on:

- government-issued identity documents;
- consumer information and other databases; and
- biometric data.

2.86 Age estimation and age screening are also discussed in this section.

---

[69] eSafety Commissioner, *Submission 191*, pp. 12-13.

[70] eSafety Commissioner, *Submission 191*, p. 4.

[71] eSafety Commissioner, *Submission 191*, p. 6.

[72] For example, see: AVSecure LLC, *Submission 74;* Department of Home Affairs, *Submission 146*; Yoti, *Submission 172*; Digital Transformation Agency, *Submission 188;* Equifax, *Submission 189*; TrustElevate, *Submission 190*; Australia Post, *Submission 199*; Age Verification Providers Association, *Submission 200*.

2.87 While these methods are discussed individually, the Committee heard that providers may use a combination of methods depending on the level of assurance required.[73] For example, age verification could use a combination of biometric data and a government-issued identity document.

2.88 While not the focus of the inquiry, the Committee also notes evidence received on a number of alternative or complementary technologies, including filtering and ISP [internet-service provider] blocking.[74] This evidence is discussed in more detail in the following chapter.

Verification based on identity documents

2.89 The Committee heard that age verification could involve the use of a government-issued identity document, such as a driver licence or passport. As an individual's date of birth is verified in the initial process of obtaining the identity document, the document then provides a reference against which the individual's age can be verified at a later time.

2.90 For example, a simple method could involve a user submitting details from an identity document (for example, a driver licence number), which could then be verified with reference to an online government register or other database to confirm that the document (and therefore the user's date of birth) is valid.[75]

2.91 However, the Committee also heard about more sophisticated methods for validating identity documents, such as matching a photo on the document with an image submitted online in real-time by the user, or, in the case of a passport, reading the near-field-communication (or NFC) chip embedded in the document.[76]

Document Verification Service

2.92 As an example of a possible approach to online age verification based on government-issued identity documents, several submitters referred to the Document Verification Service (DVS), which was established by the Australian Government in partnership with state and territory governments.

---

[73] eSafety Commissioner, *Submission 191*, p. 7.

[74] For example, see: eSafety Commissioner, *Submission 191*, pp. 15-17; eChildhood, *Submission 192*, pp. 29-32; Family Zone, *Submission 202*, pp. 2-3.

[75] For example, see: Department of Home Affairs, *Submission 146*, p. 2.

[76] For example, see: Yoti, *Submission 172*, p. 10; Australia Post, *Submission 199*, p. 3.

2.93 The DVS enables checks of biographic information (including date of birth) against government-issued identity documents, including birth certificates, driver licences, passports, and visas.[77]

2.94 The Department of Home Affairs, which administers the DVS, confirmed that the service could be used for the purpose of age verification:

> The Document Verification Service checks whether the personal information on an identity document matches the original record. Importantly this includes verification of the date of birth on Australian passports, driver licences and birth certificates. The Document Verification Service conducted about 48 million transactions in 2018-19 and has been available to government agencies for over 10 years, and to the private sector since 2014.[78]

2.95 Private-sector organisations can only use the DVS to check a person's identity with their consent, and only where this is permitted by the *Privacy Act 1988*.[79] The DVS does not check facial images.[80] However, a service for this purpose is in development (see discussion later in this chapter).

2.96 The Department submitted that the DVS 'makes it harder for people to use fake identity documents, which could otherwise be used to circumvent age verification processes'.[81]

2.97 Responsible Wagering Australia submitted that there is a 'high level of confidence' in the integrity of the DVS, but also noted concerns about its usability by the private sector and some technical limitations:

> Some technical limitations of the DVS we have identified include a lack of consistency between data fields of the databases, queries being restricted to name and document number as opposed to a name and address, and affirmative matches requiring an absolute match (meaning that common typographical issues increase failure rates).[82]

---

[77] Australian Government, 'Identity Matching Services - what are they?', <https://beta.idmatch.gov.au/our-services>.

[78] Department of Home Affairs, *Submission 146*, p. 2.

[79] Department of Home Affairs, *Submission 146*, p. 2.

[80] Australian Government, 'Identity Matching Services - what are they?', <https://beta.idmatch.gov.au/our-services>.

[81] Department of Home Affairs, *Submission 146*, p. 2.

[82] Responsible Wagering Australia, *Submission 174*, p. 4.

Retail card

2.98 The Committee heard that online age verification could involve the use of a retail card, which would be obtained in a face-to-face transaction where the user's age would be verified by sighting a government-issued document such as a driver licence.[83]

2.99 Ms Erratt, Head of Age Verification at the BBFC, explained that a user would obtain the retail card from a shop in the same way as other age-restricted goods, such as cigarettes or alcohol. The card would include an anonymous code that could be submitted online to complete the age-verification process.[84]

2.100 Ms Erratt explained that age-verification providers had developed a range of safeguards to mitigate the misuse of a retail card by a person under the age of 18 years, such as requiring the code associated with the retail card to be used within a certain period of time.[85]

2.101 Ms Erratt suggested this was an example of an age-verification method that did not involve the retention of any personal information.[86]

Verification based on consumer information or other databases

2.102 The Committee heard that online age verification could involve the use of consumer information or other databases that incorporate age-related information or are restricted to individuals aged 18 years or above.

2.103 For example, Equifax submitted that age verification could involve confirmation that a user is listed on the Commonwealth electoral roll or has credit reporting information retained on Equifax's consumer credit bureau, either of which indicates that the user is aged 18 years or above.[87]

---

[83] For example, see: AVSecure LLC, *Submission 74*, p. 2; British Board of Film Classification, *Submission 187*, p. 10.

[84] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 5.

[85] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 5.

[86] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 5.

[87] Equifax, *Submission 189*, p. 2.

2.104 Equifax submitted that 96 per cent of eligible Australians are listed on the Commonwealth electoral roll and approximately 18 million of an estimated 18.9 million Australian adults are listed on the consumer credit bureau.[88]

2.105 According to Equifax, currently both the Commonwealth electoral roll and credit reporting information can be used for anti-money laundering and counter-terrorism financing purposes, but not for other identity- or age-verification purposes.[89]

2.106 Dr O'Connell gave a similar example of online age verification involving a user submitting their mobile phone number. As mobile phone contracts are restricted to individuals aged 18 years or above, age verification would then involve determining that a contract is associated with the phone number.[90]

Verification based on biometric data

2.107 Another possible method of online age verification involves the use of biometric data, such as a facial image of an individual user.

2.108 As noted above, this method could involve a user submitting a live photo from the camera on their phone, which is validated against a government-issued identity document, either automatically using facial-recognition technology or manually by a trained operator.[91]

2.109 The Committee heard that a so-called 'liveness test' could be used to ensure that user is a real person presenting genuine biometric data.[92] For example, Mrs Julie Dawson, representing Yoti, an age-verification provider, explained:

> We want to prove that it's actually you, so we're going to do what we called a 'liveness test', which is a quick 3D scan of your face where we're checking that you're a real human being, not a robot, a 3D image or a hologram of some sort.

[88] Equifax, *Submission 189*, pp. 1-2; Mr Matt Strassberg, General Manager, External Relations Australia and New Zealand, Equifax, *Committee Hansard*, Canberra, 6 December 2019, pp. 37-38.

[89] Equifax, *Submission 189*, p. 2.

[90] Dr Rachel O'Connell, Co-founder, TrustElevate, *Committee Hansard*, Canberra, 5 December 2019, p. 13.

[91] Yoti, *Submission 172*, pp. 10-11; Department of Home Affairs, *Submission 146*, p. 2.

[92] Yoti, *Submission 172*, p. 3; Australia Post, *Submission 199*, p. 3.

> Sometimes we might get you to read a couple of words off the screen, like 'dog', 'cat' or 'mother'. That helps us detect that that is a real human.[93]

2.110 The eSafety Commissioner provided two other examples of this approach:

> For example, individuals must blink when taking a selfie to prove they are live and not merely a static photo. To combat pre-recorded voices, the system prompts individuals to repeat randomly generated phrases or a sequence of numbers to prove that they are human and not a recording.[94]

Face Verification Service

2.111 The Department of Home Affairs submitted that it was developing a Face Verification Service (FVS), which it proposed could assist in age verification.[95]

2.112 The FVS is intended to enable checks of facial images against government-issued identity documents.[96]

2.113 The Department explained that the FVS would complement the DVS (see discussion earlier in this chapter):

> ... The Face Verification Service complements the Document Verification Service by preventing the use of stolen as well as fake identity information. This could assist in age verification, for example by preventing a minor from using their parent's driver licence to circumvent age verification controls.[97]

2.114 However, the Department also explained that the service was not yet fully operational:

> Whilst it is intended to be made available to private sector organisations in future, this will be subject to the passage of the Identity-matching Services Bill 2019 which is currently before Parliament. The use of driver licence images through the Face Verification Service is also subject to the agreement of the states and territories.[98]

---

[93] Mrs Julie Dawson, Director, Regulatory and Policy, Yoti, *Committee Hansard*, Canberra, 6 December 2019, p. 31.

[94] eSafety Commissioner, *Submission 191*, p. 9.

[95] Department of Home Affairs, *Submission 146*, p. 2.

[96] Australian Government, 'Identity Matching Services - what are they?', <https://beta.idmatch.gov.au/our-services>.

[97] Department of Home Affairs, *Submission 146*, p. 2.

[98] Department of Home Affairs, *Submission 146*, p. 2.

2.115 The *Identity-matching Services Bill 2019* was introduced into Parliament on 31 July 2019. The bill was subsequently referred to the Parliamentary Joint Committee on Intelligence and Security for review. In its report on the bill, the Committee recommended that the bill be re-drafted taking into account principles relating to privacy, transparency, oversight, and user obligations.[99]

Age estimation

2.116 The Committee heard about the recent development of more sophisticated approaches that involved estimating or predicting a user's age without reference to government-issued identity documents or other databases.

2.117 The eSafety Commissioner submitted that there is growing research into the use of age prediction, particularly in jurisdictions where identity documentation is rare or non-existent.[100]

2.118 Yoti referred the Committee to its Age Scan product, which involves a user submitting a facial image from the camera on their phone:

> Yoti Age Scan is a secure age-checking service that can estimate a person's age by looking at their face. ... The user does not have to register to use the service, and does not have to provide any information about themselves. Therefore, no identity document need be presented. The user simply presents their face in front of the camera.
>
> ... Yoti Age Scan works quickly, returning an age estimate in around 1 to 1½ seconds.[101]

2.119 Yoti submitted that the software is configurable to meet whatever accuracy threshold is required by the business or regulator:

> With a threshold set at 25, the average false positive rate across 14 to 17 year olds is 0.31%. This figure continues to decline as our training data increases in size.[102]

---

[99] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Identity-matching Services Bill 2019 and the Australian Passports Amendment (Identity-matching Services) Bill 2019*, October 2019.

[100] eSafety Commissioner, *Submission 191*, p. 7.

[101] Yoti, *Submission 172*, pp. 10-11.

[102] Yoti, *Submission 172*, p. 11.

2.120 Yoti submitted that the product had been used in a variety of settings, including live-streaming services, retail self-checkouts, and dating and pornography platforms, and that approximately 200 million checks had been performed in the nine months that the product had been available.[103]

2.121 Mr Corby, Executive Director of the AVPA, told the Committee that age-estimation software could also use social and behavioural information from a social media account.[104]

2.122 Similarly, the eSafety Commissioner explained that advances in technology were enabling platforms and services to identify users from behavioural and online signals:

> How an individual interacts and engages online leaves traces that can be utilised to identify whether they are an adult or a child. For example, a handle or username, image tags, hashtag usage, gesture patterns, web history, content interaction, IP address, location data, device serial number, contacts – all can be used to measure what age-bracket that you might fall under.
>
> These signals are sometimes used by social media platforms, alongside third-party verification systems, to flag users who might be underage on their site. There are a few examples of technology that utilise these signals for automatic age-gating purposes.[105]

Age screening

2.123 As noted above, the Committee heard evidence about earlier, less sophisticated methods such as age screening and age gating, which may involve a user self-declaring their age, often at the point of access or registration.[106]

2.124 The eSafety Commissioner explained that age gating allowed online services and providers to restrict access to content to people over a particular age:

> Age gating can simply restrict access to the content, providing users with an error message or re-directing them to more age-appropriate content.

---

[103] Yoti, *Submission 172*, p. 11; Mr Robin Tombs, Chief Executive Officer, Yoti, *Committee Hansard*, Canberra, 6 December 2019, p. 28.

[104] Mr Iain Corby, Executive Director, Age Verification Providers Association, *Committee Hansard*, Canberra, 5 December 2019, p. 10.

[105] eSafety Commissioner, *Submission 191*, p. 8.

[106] eSafety Commissioner, *Submission 191*, p. 6; Age Verification Providers Association, *Submission 200*, p. 3.

> Alternatively, content can be locked for access and only released once a PIN code or other type of age verification process has taken place.[107]

2.125 However, the eSafety Commissioner also noted that basic forms of age gating, which trust the user to declare their correct age, are easily circumvented.[108]

Online and physical-world rights and obligations

2.126 Lastly, in addition to the principles relating to age verification discussed earlier in this chapter, the argument was put to the Committee that there should be stronger alignment between individuals' rights and obligations in the physical world and corresponding rights and obligations in the online world.

2.127 Mr MacGibbon explained:

> One of the observations I would make is that we have somehow separated our online lives and our expectation for what occurs online from our offline lives. Yet now it would be trite to say that the connectivity between our online and offline activities is such that they're one single entity, and we should aspire as a nation to create the concept of an online civil society, one which reflects our offline society. To do that we do need to take action. We do need to consider regulations, and we do need to consider what roles and responsibilities governments have, as well as the companies that provide services online, and the role of individuals in that online civil society.
>
> ... I believe there are ways we can improve the online environment. I am not going to say they are perfect but I certainly would say that we owe it to the people of Australia to reflect Australian values online, just as every nation should reflect its values in the online space of its community.[109]

2.128 Mr Corby made a similar point, suggesting that a good starting point would be to consider '[w]hat happens in the real world, and are we trying to at least do as well as that?'[110]

---

[107] eSafety Commissioner, *Submission 191*, p. 6.

[108] eSafety Commissioner, *Submission 191*, p. 6.

[109] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, p. 23.

[110] Mr Iain Corby, Executive Director, Age Verification Providers Association, *Committee Hansard*, Canberra, 5 December 2019, p. 8.

2.129 Mr MacGibbon went on to relate this idea to the issue of age verification for age-restricted products and services:

> If I was to walk into a restricted premises today where I could gain access to legal yet restricted pornography, no-one would question who I was and my identity would not be known.
>
> ... Any system that we create online needs to somehow respect people's privacy for lawful access to materials. If society says it is lawful offline, it should be lawful online. And any system that you create which has to involve some form of technology should reflect as closely as possible our offline lives.[111]

2.130 Mr MacGibbon argued that, at present, online privacy, safety, and security are 'much less assured' than in the physical world:

> ... we think we're anonymous and ...we think that what we do online doesn't matter. ...while there might be technical and legal solutions to this, there is a broader social question about how society views its online activities, and we're very immature when it comes to that.[112]

2.131 In relation to children and young people in particular, both Mr MacGibbon and Ms Inman-Grant emphasised that parents need to be engaged in their children's online lives in the same way they are in their everyday lives.[113]

Committee comment

2.132 Australians are increasingly accessing a wide range of products and services online.

2.133 The Committee accepts the proposition that what is legal in the physical world should be legal in the online world. In the same way, the Committee is concerned to see that age restrictions that apply in the physical world are also applied online.

2.134 In face-to-face commerce, children and young people are restricted from accessing a range of adult products and services at the point of sale. This

---

[111] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, p. 23.

[112] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, pp. 24, 26.

[113] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, pp. 25-26; Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 11

includes alcohol, tobacco, and mobile phone services. Here, potential consumers are required to show appropriate personal identification before accessing these products.

2.135 The Committee considers that the same principle should apply to access online pornography and online wagering. This is discussed in further detail in the following chapters. While outside the scope of this inquiry, it was also put to the Committee that online sales of alcohol should similarly be restricted to individuals whose age has been verified using an effective method. As a matter of principle, the Committee accepts this proposition.

2.136 Evidence to the inquiry suggests that methods for online age-verification have advanced significantly in recent years. The Committee is confident that suitable technology exists to support a regime of mandatory age verification for age-restricted products and services.

2.137 However, it is the Committee's view that a prerequisite for the implementation of any system of mandatory age-verification is the establishment of robust technical standards, particularly in relation to the privacy of users' personal information.

2.138 As such, the Committee recommends that the Australian Government develop appropriate technical standards to underpin online age verification. The Committee considers that it is important for this work to begin now in order to support future policy decisions in relation to age verification. This work would also underpin the Committee's recommendations in relation to online pornography and online wagering later in this report.

2.139 The Committee recognises the benefit in users having a range of options available to verify their age. It is apparent that the various methods on offer have different strengths and weaknesses in relation to the key attributes identified above for an effective age-verification model. Any single method may involve a trade-off, for example, between its accuracy and effectiveness, and protecting the privacy of users' information. Some may offer high levels of accuracy and protection but at greater cost to the business and/or individual user.

2.140 As such, the Committee's expectation is that these standards would not seek to prescribe particular age-verification methods.

2.141 Instead, the standards would establish a baseline that all age-verification methods offered to customers in Australia would be required to meet. For example, with respect to privacy and security, based on evidence to

the inquiry, the Committee believes that at a minimum all age-verification methods should be required to:

- preserve a user's privacy such that no personal information other than the user's age-related eligibility is shared between the age-verification provider and the age-restricted site; and
- minimise retention of, and if possible eliminate the storage of personal information, so as not to create a 'honeypot' of sensitive data, and if some necessary data must be stored, it must be stored in a secure way.

2.142 The Committee's aim is to ensure that, whichever method a customer chooses to use to verify their age, they can be assured that the process will be easy, safe, and secure.

Recommendation 1

2.143 The Committee recommends that the Digital Transformation Agency, in consultation with the Australian Cyber Security Centre, develop standards for online age verification for age-restricted products and services.

a. These standards should specify minimum requirements for privacy, safety, security, data handling, usability, accessibility, and auditing of age-verification providers.

b. Consideration should be given to the existing technical standards in Australia and overseas, including but not limited to the UK Age Verification Certificate, the PAS 1296 Age Checking code of practice, the Trusted Digital Identity Framework, and the European Union General Data Protection Regulation.

c. Opportunities should also be provided for consultation with industry, including private age-verification providers, and members of the public.

2.144 In developing these standards, the Committee also encourages the Digital Transformation Agency to consult with ID Care, an Australian not-for-profit organisation which provides specialist advice and support to individuals and organisations in relation to online identity and cyber security. The Committee expects that consulting with ID Care and similar organisations will help to ensure that any standards adequately address security and privacy concerns and are fit-for-purpose in the Australian context.

2.145 As noted above, the Committee envisages that these standards would be mandated as part of any policy decision in relation to mandatory age-verification for particular products or services. These standards may also assist in educating and providing assurance to the public in the implementation of any such regime.

2.146 At the same time, the Committee recommends that the Australian Government develop an age-verification exchange for the purpose of third-party online age verification. Similar to the existing identity exchange (a component of the government's Digital Identity program) the age-verification exchange would enable users wishing to access an age-restricted site to choose from a range of age-verification providers.

2.147 To avoid duplication, the Committee recommends the age-verification exchange be developed as an extension of the Digital Identity program.

Recommendation 2

2.148 The Committee recommends that the Digital Transformation Agency extend the Digital Identity program to include an age-verification exchange for the purpose of third-party online age verification.

2.149 The Committee anticipates that such a system would support the development of a competitive ecosystem for third-party age verification in Australia, including public and private sector age-verification providers. This would ensure that users have a choice about how they wish to verify their age, and would also protect users' privacy by ensuring that age verification is carried out by a third party.

2.150 Age-verification providers wishing to participate in the system should be required to meet appropriate technical standards (see Recommendation 1).

2.151 The Committee also expects that the system would enable free or low-cost age verification by leveraging existing government verification services. This would assist in minimising compliance costs for small businesses required to implement mandatory age verification.

2.152 The Committee also encourages the Australian Government to consider measures to educate users—particularly children and young people and their parents and guardians—about online privacy. In this regard, the Committee acknowledges the ongoing work of the Office of the eSafety Commissioner and congratulates both Ms Inman-Grant and her staff for their important work in this area.

3. Age verification for online pornography

3.1 According to the eSafety Commissioner, research conducted in 2018 found that one third of parents of children aged 2 to 17 years reported that they were concerned about their children accessing or being exposed to pornography.[1]

3.2 This concern was reflected in a large number of submissions to the inquiry—many from parents, carers, and others responsible for the welfare of children and young people.

3.3 This chapter considers evidence in relation to the nature and effect of children and young people's exposure to pornography.

3.4 The chapter then considers how online pornography is currently regulated in Australia, and how age verification for online pornography has been pursued in other jurisdictions.

3.5 The chapter concludes with evidence about the possible implementation of a mandatory regime for age verification for online pornography in Australia.

Nature of children's exposure to pornography

3.6 The Committee received a large number of submissions and other correspondence expressing concern about the ease with which children and young people are able to access online pornography.

3.7 The Committee notes that evidence on this subject was also considered by the Senate Environment and Communications References Committee in its

[1] eSafety Commissioner, *Submission 191*, p. 2.

2016 report, *Harm being done to Australian children through access to pornography on the Internet*.[2]

3.8 eChildhood, a charity seeking to address the impacts of exposure to pornography on children and young people, submitted that children are 'increasingly accessing or being accidentally exposed to pornography on the internet':

> Whilst exact statistics vary due to the inherent research limitations on this topic, studies have shown that high percentages of children and young persons above the age of 10 have been exposed to pornographic material, with males being at a significantly greater risk of exposure.[3]

3.9 A number of submissions referred to research attempting to quantify the nature of children's exposure to online pornography at different age groups. For example, eChildhood submitted:

> According to recent data from an internet filtering software company used in schools, a third of students aged eight and under attempted to access online pornography in the past six months. This includes accidental access through unwanted pop-up ads and banners as well as deliberate searches for explicit material.[4]

3.10 Advocacy group Collective Shout referred to UK research which found that 28 per cent of children aged 11 to 12 years had seen pornography online. The same study found that 65 per cent of children aged 15 to 16 years had seen pornography online, with 94 per cent of those having first seen pornography by age 14 years.[5]

3.11 Collective Shout also cited Australian research which indicated that 69 per cent of males and 23 per cent of females had first viewed pornography at age 13 years or younger.[6]

3.12 The Victorian Aboriginal Child Care Agency (VACCA) referred to a survey undertaken in Australia in 2010 which found that nearly 1 in 4 children aged between 9 to 16 years had viewed sexually explicit images online. VACCA

---

[2] Senate Environment and Communication References Committee, *Harm being done to Australian children through access to pornography on the Internet*, November 2016, pp. 7-11.

[3] eChildhood, *Submission 192*, p. 9.

[4] eChildhood, *Submission 192*, p. 9.

[5] Collective Shout, *Submission 178*, p. 3.

[6] Collective Shout, *Submission 178*, pp. 4-5.

noted that these figures were higher than the average for the 25 other countries included in the survey as a reference point.[7]

3.13 The Committee heard that smartphones and other handheld devices were associated with an increase in children's exposure to pornographic material. For example, VACCA explained:

> Australian and international research and expert consensus shows that with the growing use of tablets and smartphones, children and young people are being exposed to online pornography at an ever-increasing rate. According to two studies in the UK, the average age of first exposure to online pornography is 11 years of age...[8]

3.14 Similarly, Collective Shout suggested that children's ability to access pornography was becoming easier 'due to the proliferation of handheld devices, including smartphones, as well as the availability of unfiltered public wifi'.[9] Ms Melinda Liszewski, Campaigns Manager for Collective Shout, told the Committee:

> Our take-up of technology has been rapid, and our safeguarding of children who are connected to the internet at the earliest of ages has been very slow.[10]

3.15 This point was echoed by WA Child Safety Services (WACSS), a not-for-profit provider of child safety education:

> Children and young people with access to the internet on any device - at home, at a friend's place, at school or in any of our community spaces with Wi-Fi - are at risk of exposure. It's now not a matter of 'if' a child will see pornography but 'when' and the when is getting younger and younger. In Australia the average age of first exposure is being reported at between 8 and 10 years of age. While pornography is not new, the nature and accessibility of today's pornography has changed considerably.[11]

---

[7] Victorian Aboriginal Child Care Agency, *Submission 185*, p. 3.

[8] Victorian Aboriginal Child Care Agency, *Submission 185*, p. 3.

[9] Collective Shout, *Submission 178*, p. 3.

[10] Ms Melinda Liszewski, Campaigns Manager, Collective Shout, *Committee Hansard*, Canberra, 6 December 2019, p. 60.

[11] WA Child Safety Services, *Submission 170*, p. 2.

3.16 Ms Tamara Newlands, Executive Director of eChildhood, characterised the situation as children having 'unfettered access to hard-core pornography at their fingertips 24/7'.[12]

3.17 A common theme in evidence was that children's exposure to pornographic material could be not only deliberate but also inadvertent.[13] While exposure due to 'pop-up' advertisements was raised, Collective Shout also submitted that 'innocuous activities like key-stroke errors and searches for cartoon characters' could inadvertently direct children to pornographic websites:

> Our children don't need to be looking for porn, but porn will find them. It's simply not a fair fight.[14]

3.18 Many of the individual submissions received by the Committee came from parents, teachers and others recounting first-hand experiences of children in their care encountering pornography online through friends or schoolmates, unintended results of innocuous web searches, or the appearance of unsolicited 'pop-up' material.

3.19 Another strong theme in evidence was that the nature of pornography had changed such that children are exposed to pornographic material that is more extreme. Ms Julie Inman-Grant, the eSafety Commissioner, told the Committee that pornographic material is today much more extreme and, in some cases, more violent than in the past.[15]

3.20 Ms Inman-Grant went on:

> Most of the parents we've talked to and done research with have no idea what kind of pornography is readily accessible and available online: ...it can be very violent, very confronting...[16]

3.21 WACSS submitted that pornography is 'often violent, graphic and portrays distorted gender roles'.[17] Similarly, Melinda Tankard-Reist told the

---

[12] Ms Tamara Newlands, Executive Director, eChildhood, *Committee Hansard*, Canberra, 6 December 2019, p. 51.

[13] For example, see: eChildhood, *Submission 192*, pp. 9-10; Collective Shout, *Submission 178*, p. 3; Dr Elizabeth Taylor, *Submission 196*, p. 3.

[14] Collective Shout, *Submission 178*, pp. 1-2.

[15] Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 10.

[16] Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 11.

[17] WA Child Safety Services, *Submission 170*, p. 2.

Committee that 'children are frequently seeing violent depictions of sex, torture, rape and incest porn'.[18]

3.22 VACCA also raised this issue in its submission, explaining:

> A great deal of the pornography that children view – whether accidentally or intentionally – contains violent imagery and themes. In a UK study it was found that 100 per cent of 15-year-old boys and 80 per cent of 15-year-old girls in 2013 had viewed "violent, degrading online pornography, usually before they have had a sexual experience themselves."[19]

3.23 In a recent analysis of pornographic videos commonly watched in New Zealand, the Office of Film and Literature Classification found that 10 per cent of videos showed physical aggression and 35 per cent showed some non-consensual behaviour.[20]

Effect of children's exposure to pornography

3.24 Many submissions to the inquiry expressed concern about a range of possible consequences associated with the increased exposure of children and young people to online pornography.

3.25 As noted above, evidence on this subject was also considered in the 2016 report of the Senate Environment and Communications References Committee,[21] and several submissions referred to evidence included in this report.

3.26 In its submission, eChildhood provided a summary of research into outcomes associated with children's exposure to pornography:

> Access to pornography at a young age, when the child is still developing, can have extensive negative impacts on the child. The literature reveals links between children's access to pornography and the following non-exhaustive list of outcomes:

---

[18] Ms Melinda Tankard Reist, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, p. 61. See also: Ms Melinda Liszewski, Campaigns Manager, Collective Shout, *Committee Hansard*, Canberra, 6 December 2019, p. 60.

[19] Victorian Aboriginal Child Care Agency, *Submission 185*, p. 3.

[20] New Zealand Office of Film and Literature Classification, 'Breaking Down Porn – An analysis of commonly viewed porn in NZ', <https://www.classificationoffice.govt.nz/news/latest-news/breaking-down-porn-an-analysis-of-commonly-viewed-porn-in-nz/>.

[21] Senate Environment and Communication References Committee, *Harm being done to Australian children through access to pornography on the Internet*, November 2016, pp. 12-23.

1 Poor mental health – including, but not limited to, being distressed and upset by the images, self-objectification and body image concerns, sexual conditioning and developing an addiction to pornography;

2 Sexism and objectification – such as reinforcing gender roles that women are 'sex objects' and men should be dominant while women should be submissive;

3 Sexual aggression and violence – consistently, there is a demonstrated association between regular viewing of online pornography and the perpetration of sexual harassment, sexual coercion and sexual abuse by boys;

4 Child-on-child and peer-on-peer sexual abuse; and

5 Shaping sexual behaviours, such as engaging in younger sexual behaviour, more frequent premarital and casual sexual behaviour and more 'risky' sexual behaviour.[22]

3.27 Similarly, summarising research on the effects of pornography on children and young people, the Australian Institute of Family Studies (AIFS) found:

> The available studies suggest that the effects of frequent and routine viewing of pornography and other sexualised images may:
>
> - reinforce harmful gender stereotypes;
> - contribute to young people forming unhealthy and sexist views of women and sex; and
> - contribute to condoning violence against women.
>
> There is also evidence to suggest an association between frequent viewing of online pornography and sexually coercive behaviour exhibited by young men.
>
> Pornography consumption by young people may also normalise sexual violence and contribute to unrealistic understandings of sex and sexuality.
>
> ...Pornography consumption has also been associated with the practice of "sexting", and young women have reported being coerced or feeling pressured to share naked images of themselves online.[23]

[22] eChildhood, *Submission 192*, p. 10.

[23] Australian Institute of Family Studies, *Children and young people's exposure to pornography*, <https://aifs.gov.au/cfca/2016/05/04/children-and-young-peoples-exposure-pornography>. See also: Australian Institute of Family Studies, *The effects of pornography on children and young people - An evidence scan*, 2017.

3.28 Speaking to the Committee, Ms Julie Inman-Grant, the eSafety Commissioner, outlined a range of concerns about the negative effects of pornography on young people:

> This includes harmful effects of online pornography on young people's mental health and wellbeing and negatively altering their knowledge, attitudes, beliefs and expectations about sex, gender and respectful relationships and what they should look like. There are deep and legitimate concerns about how ready access to online pornography might impact the social sexualisation of an entire generation. We are right to worry about whether this conditioning might heighten involvement in risky, violent or harmful sexual practices and behaviours. In short, I don't think anyone here would disagree that this is a pressing and urgent social concern.[24]

3.29 These issues were discussed in further detail in a number of submissions to the inquiry.[25]

3.30 Several submissions referred to the *Final Report of the Royal Commission into Institutional Responses to Child Sexual Abuse*, which found that exposure to pornography had been identified in cohorts of children displaying harmful sexual behaviours.[26]

3.31 Similarly, some submissions referred to *Prevent. Support. Believe. Queensland's Framework to address Sexual Violence*, which states that exposure to pornography is a potential driver of sexual violence and problematic sexual behaviour between young people.[27]

3.32 The Committee heard that Aboriginal children in care or experiencing vulnerability in their family setting are especially vulnerable to the impacts of exposure to pornography.[28]

---

[24] Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 10.

[25] For example, see: University of New South Wales Law Society, *Submission 58*, pp. 2-3; ChildSafe, *Submission 124*, pp. 1-5; WA Child Safety Services, *Submission 170*, pp. 1-2; Marshall Ballantine-Jones, *Submission 175*, pp. 1-2; Melinda Tankard Reist, *Submission 177*, pp. 2-7; Collective Shout, *Submission 178*, pp. 5-7; Bravehearts, *Submission 182*, pp. 2-3; Senator Amanda Stoker, *Submission 184*, pp. 1-3; Victorian Aboriginal Child Care Agency, *Submission 185*, pp. 3-4; eChildhood, *Submission 192*, pp. 9-11, 43-46.

[26] Royal Commission into Institutional Responses to Child Sexual Abuse, *Final Report*, Volume 10, Children with harmful sexual behaviours.

[27] Queensland Department of Child Safety, Youth and Women, *Prevent. Support. Believe. Queensland's Framework to address Sexual Violence*, 2019, p. 11.

[28] Victorian Aboriginal Child Care Agency, *Submission 185*, p. 4.

3.33 Concern was also expressed that due to real or perceived inadequacies in sex education and the limited availability of age-appropriate educational material, children and young people were turning to pornography for education.[29] For example, Mr Chern Eu Kuan, Student Contributor at the University of New South Wales (UNSW) Law Society, told the Committee:

> The most detrimental harm caused by exposing minors to pornography is the normalisation of unsafe sex. Since sex education in school is generally underwhelming. Minors often derive their understanding of sex from online pornography. This can be detrimental to their development as pornography depicts acts of unsafe sex, misogyny, physical aggression and verbal aggression.[30]

3.34 Further evidence on education is discussed later in this chapter.

Social impacts

3.35 The Committee also received evidence about broader social impacts that may be associated with exposure to pornography, such as anxiety about body image, broader mental health issues, reduced academic performance, erectile dysfunction, and systemic issues such as violence against women.[31]

3.36 For example, eChildhood noted a link between children's access to pornography and self-objectification and concerns about body image. Mrs Liz Walker, Deputy Chair of eChildhood, told the Committee:

> What we know from the literature is that there's certainly a correlation between a hypersexualised media in general, hypersexualised advertising and then of course pornography as well in body image issues. ...we do know that an increasing number of young women are seeking out plastic surgery, labiaplasties, which is trimming of the labia, to meet some sort of porn perfection representation. There are young men who are insecure about the size of their penis.[32]

3.37 More broadly, the eSafety Commissioner noted that there is evidence to suggest that exposure to pornography can negatively impact the mental

---

[29] For example, see: WA Child Safety Services, *Submission 170*, p. 2; Ms Tamara Newlands, Executive Director, eChildhood, *Committee Hansard*, Canberra, 6 December 2019, pp. 51, 55.

[30] Mr Chern Eu Kuan, Student Contributor, UNSW Law Society, *Committee Hansard*, Canberra, 6 December 2019, p. 47.

[31] For example, see: eChildhood, *Submission 192*, p. 44; eChildhood, *Submission 192.1*, pp. 1-4.

[32] Mrs Liz Walker, Deputy Chair, eChildhood, *Committee Hansard*, Canberra, 6 December 2019, p. 56.

health and wellbeing of young people.[33] Summarising research on the relationship between pornography use and mental health, eChildhood submitted that porn users experience higher incidence of depressive symptoms and lower degrees of social integration.[34]

3.38 eChildhood cited research that found a link between use of pornography and declining academic performance among 12- to 15-year old boys:

> ... the more boys used sexually explicit Internet content, the poorer their school grades were 6 months later. Boys' use of sexually explicit websites significantly predicted their school performance.[35]

3.39 eChildhood also cited a study of college-aged students with similar findings, along with research on the impact on a range of cognitive abilities associated with frequent use of online pornography.[36]

3.40 The Committee also heard about the association between pornography use and erectile dysfunction. Mrs Walker told the Committee:

> This is something that the average teen boy wouldn't consider. He'd be thinking, 'Well, if I watch pornography I'm going to become a great lover.' In actual fact, by the time he's 20 he might be discovering that he's actually unable to be aroused by the person he's with because he's watched so much pornography.[37]

3.41 Mrs Walker went on to explain that studies show an increase in the number of young men experiencing 'porn induced erectile dysfunction':

> The literature indicates that, pre-internet, we were seeing around three to five per cent of men under the age of 40 experiencing erectile dysfunction, and that was usually due to some sort of physiological condition... Now the literature is indicating that around one-third of men under the age of 40 are experiencing erectile dysfunction, and a large percentage of that looks like it's due to internet pornography.[38]

---

[33] eSafety Commissioner, *Submission 191*, p. 2.

[34] eChildhood, *Submission 192*, p. 44.

[35] eChildhood, *Submission 192.1*, p. 2.

[36] eChildhood, *Submission 192.1*, pp. 2-3. See also: eChildhood, *Research: academic and concentration impacts of pornography*, <https://www.echildhood.org/research_academic_impacts>; Marshall Ballantine-Jones, *Submission 175*, pp. 1-2.

[37] Mrs Liz Walker, Deputy Chair, eChildhood, *Committee Hansard*, Canberra, 6 December 2019, p. 56.

[38] Mrs Liz Walker, Deputy Chair, eChildhood, *Committee Hansard*, Canberra, 6 December 2019, p. 56.

3.42 The Committee is also aware of the findings of a survey conducted by researchers at Monash University that indicate that in many cases young women's experience of sex is unsatisfying and associated with feelings of guilt, embarrassment, and stress, and that this may be due to them being pressured by their partners to live up to unrealistic expectations of sex encouraged by online pornography.[39]

3.43 A number of submitters raised a link between exposure to online pornography and sexual aggression and violence.[40] eChildhood cited a meta-analysis on the relationship between pornography and sexual aggression, which found that:

> ... on the average, individuals who consume pornography more frequently are more likely to hold attitudes conducive to sexual aggression and engage in actual acts of sexual aggression than individuals who do not consume pornography or who consume pornography less frequently.[41]

3.44 Ms Newlands from eChildhood elaborated on this point:

> Minors who have been exposed to pornography are more likely to view women as sex objects. Minors who view pornography and other sexualised media are more accepting of sexual violence and more likely to believe rape myths. Adolescents who are exposed to pornography are more likely to engage in sexual violence. In addition, a correlation has been shown between a child being exposed to pornography and their likelihood of being a victim of sexual violence.[42]

3.45 In relation to violence against women, eChildhood noted that the *Third Action Plan of the National Plan to Reduce Violence against Women and their Children* has a focus on 'better understanding and countering the impact of pornography given increasing evidence showing a correlation between exposure to online pornography and the sexual objectification of women and girls, the development of rape cultures and the proliferation of sexual assault'.[43]

---

[39] Sue Dunlevy, *'Women feeling guilty in bedroom'*, The Courier-Mail, Brisbane, Queensland, 24 February 2020, p. 7.

[40] For example, see: Melinda Tankard Reist, *Submission 177*, pp. 3-5; Dads4Kids, *Submission 181*, p. 7; Bravehearts, *Submission 182*, p. 2; eChildhood, *Submission 192*, p. 45.

[41] eChildhood, *Submission 192*, p. 45.

[42] Ms Tamara Newlands, Executive Director, eChildhood, *Committee Hansard*, Canberra, 6 December 2019, p. 52.

[43] eChildhood, *Submission 192*, p. 10.

3.46 Ms Liszewski from Collective Shout told the Committee that 'harmful attitudes and behaviours' associated with viewing pornography 'are widely recognised as underpinning the epidemic of violence against women in Australia'.[44]

United Nations Convention on the Rights of the Child

3.47 Given concern about the potential harms caused to children from exposure to pornography, a number of submitters referred to Australia's obligations under the United Nations Convention on the Rights of the Child.[45]

3.48 eChildhood submitted that under the Child Convention, Australia 'has an obligation to protect children, and this obligation is extended to children's use of the internet'.[46]

Regulation of online pornography in Australia

3.49 Online content (content accessed through the internet, mobile phones, content services, and live-streaming) is regulated under the *Broadcasting Services Act 1992*. Under Schedule 7 of the Act, prohibited content includes content that has been, or is likely to be, classified as:

- RC (refused classification);
- X18+;
- R18+ unless it is subject to a restricted access system; and
- MA15+ and is provided on a commercial basis unless it is subject to a restricted access system.[47]

3.50 Material that contains 'real depictions of actual sexual activity between consenting adults' and is 'unsuitable for a minor to see' falls within the X18+ classification.[48]

---

[44] Ms Melinda Liszewski, Campaigns Manager, Collective Shout, *Committee Hansard*, Canberra, 6 December 2019, p. 60.

[45] For example, see: Ms Jane Munro, *Submission 144*, p. 2; Collective Shout, *Submission 178*, pp. 12-13; Canberra Declaration, *Submission 180*, pp. 9-12; Dads4Kids, *Submission 181*, pp. 9-11; TrustElevate, *Submission 190*, p. 7; eChildhood, *Submission 192*, p. 18.

[46] eChildhood, *Submission 192*, p. 18.

[47] eSafety Commissioner, *Submission 191*, pp. 3-4; Department of Communications and the Arts, 'Online content regulation', <https://www.communications.gov.au/policy/policy-listing/online-content-regulation>.

[48] National Classification Code (May 2005), <https://www.legislation.gov.au/Details/F2013C00006>. See also: eSafety Commissioner, *Submission 191*, pp. 3-4.

3.51 Where prohibited content is hosted in Australia, the eSafety Commissioner has the authority to direct the relevant content service provider to remove the content from its service.[49]

3.52 Where prohibited content is hosted overseas, the eSafety Commissioner will notify the content to the suppliers of approved filters under the Family Friendly Filter scheme, so that access to the content is blocked.[50]

3.53 Regardless of where content is hosted, if the content is of a sufficiently serious nature (for example, child sexual abuse material), the eSafety Commissioner can take additional measures, including referring the content to law enforcement and to the International Association of Internet Hotlines (INHOPE), a global network to facilitate the removal of child sexual abuse material from the internet.[51]

3.54 Mr Toby Dagg, Manager of Cyber Report at the Office of the eSafety Commissioner, confirmed to the Committee that it is prohibited for any X18+ material 'showing explicit sexual activity between consenting adults' to be hosted in Australia. However, Mr Dagg explained that 'very little of that content' is hosted in Australia and was instead 'overwhelmingly' hosted overseas.[52]

Age verification for online pornography in other jurisdictions

3.55 This section summarises evidence received on age verification for online pornography in international jurisdictions, which predominantly considered the proposed regime for mandatory age verification in the United Kingdom.

UK Digital Economy Act

3.56 The terms of reference for the inquiry required the Committee to consider the proposed regime for mandatory age verification for access to online pornography in the United Kingdom.

[49] eSafety Commissioner, *Submission 191*, pp. 3-4.

[50] eSafety Commissioner, *Submission 191*, pp. 3-4.

[51] eSafety Commissioner, *Submission 191*, pp. 3-4.

[52] Mr Toby Dagg, Manager, Cyber Report, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 14.

3.57 The regime was set out in Part 3 of the *Digital Economy Act 2017* (DEA) and would have made the distribution of online pornography in the UK without age verification controls an offence.[53] The DEA is discussed in further detail later in this section.

3.58 However, in October 2019, following the establishment of the present inquiry, the UK Government announced that it would not commence age verification under the DEA.[54] The Government stated that it had concluded that a coherent agenda on these issues 'will be best achieved through our wider online harms proposals', which 'will give the regulator discretion on the most effective means for companies to meet their duty of care'.[55]

3.59 Nevertheless, as outlined in this section, the Committee received a range of evidence on the DEA and the proposed regime which may inform the consideration of age verification for online pornography in Australia.

Scope and requirements

3.60 Under section 14(1) of the DEA, pornographic material may not be made available on the internet to persons in the UK on a commercial basis unless controls are in place to ensure that the material is not normally accessible by persons under the age of 18.[56] In addition, section 23 of the DEA provides powers to block access to extreme pornographic material.[57]

3.61 Pornographic material is defined in Section 15 of the DEA to include:

- video works issued with an R18 certificate by the British Board of Film Classification (BBFC); and
- any other material that could be assumed from its nature was produced solely or principally for the purposes of sexual arousal.[58]

3.62 According to the BBFC, the R18 category is 'primarily explicit works of consenting sex or strong fetish material involving adults'.[59]

---

[53] eChildhood, *Submission 192*, p. 19.

[54] British Board of Film Classification, *Submission 187*, p. 1.

[55] Secretary of State for Digital, Culture, Media and Sport, 'ONLINE HARMS: Written statement – HCWS13', <https://www.parliament.uk/written-questions-answers-statements/written-statement/Commons/2019-10-16/HCWS13>.

[56] *Digital Economy Act 2017* (United Kingdom), section 14(1).

[57] *Digital Economy Act 2017* (United Kingdom), section 23. See also: British Board of Film Classification, *Submission 187*, p. 2.

[58] *Digital Economy Act 2017* (United Kingdom), section 15.

3.63 The circumstances in which pornographic material would be regarded as made available on a commercial basis are defined in the *Online Pornography (Commercial Basis) Regulations 2018* to include:

- if access to that material is available only upon payment; or
- if that material is made available free of charge and the person who makes it available receives (or reasonably expects to receive) a payment, reward or other benefit in connection with making it available on the internet.[60]

3.64 The regulations exclude circumstances where it is reasonable for the regulator to assume that pornographic material makes up less than one-third of the content made available on a site. However, this exclusion does not apply if the site is marketed as a site by means of which pornographic material is made available.[61] This definition includes websites 'which offer pornographic content for free, but which generate revenue through advertising or premium content', but excludes social media platforms.[62]

3.65 In February 2018, under section 16 of the DEA, the Secretary of State appointed the BBFC as the age-verification regulator. The BBFC is the non-governmental, not-for-profit independent regulator of film and video in the UK.[63]

3.66 The BBFC would be responsible for determining whether arrangements for making pornographic material available complied with section 14(1) of the DEA.[64] The DEA requires the BBFC to publish guidance on compliant age-verification arrangements (the published guidance is discussed in the previous chapter of this report).[65]

3.67 The DEA also gives the BBFC powers to:

- issue notices requiring information;[66]

---

[59] British Board of Film Classification, 'R18', <https://bbfc.co.uk/about-classification/r18>. See also: British Board of Film Classification, *Submission 187*, p. 8.

[60] *Online Pornography (Commercial Basis) Regulations 2018*.

[61] *Online Pornography (Commercial Basis) Regulations 2018*.

[62] British Board of Film Classification, *Submission 187*, p. 6.

[63] British Board of Film Classification, *Submission 187*, p. 2.

[64] British Board of Film Classification, *Submission 187*, pp. 2, 7.

[65] *Digital Economy Act 2017* (United Kingdom), section 25(1)(a); British Board of Film Classification, *Submission 187*, pp. 7-8.

[66] *Digital Economy Act 2017* (United Kingdom), section 18(1).

- issue enforcement notices and/or impose financial penalties where a person contravened section 14(1);[67]
- issue notices to payment-services providers and ancillary service providers where a person contravened section 14(1);[68] and
- issue notices to internet-service providers (ISPs) where a person had contravened section 14(1) requiring them to prevent access to the offending material.[69]

3.68 Guidance published by the BBFC sets out the BBFC's considerations in terms of enforcement action, in addition to a list of classes of ancillary service providers included under section 21 of the DEA, 'such as social media platforms, search engines and advertising networks'.[70]

3.69 Speaking to the Committee via teleconference, Ms Amelia Erratt, Head of Age Verification at the BBFC, confirmed that the BBFC would have the ability to block non-compliant websites and request that service providers withdraw their services from non-compliant websites.[71] Ms Erratt submitted that these powers would give the BBFC 'international reach':

> Obviously, with ISP blocking you would block a website from being accessible in the UK, but what we had understood from the payment service provider power is that, if you cut off a website's payment services, that can have a 'global impact on their business. Given that these websites are quite financially focused, the threat of having their payments cut off was enough to make them want to comply with the legislation.[72]

3.70 The BBFC submitted that VISA and Mastercard had 'confirmed a willingness to cooperate with the regime'.[73]

---

[67] *Digital Economy Act 2017* (United Kingdom), section 19(1)-(2).

[68] *Digital Economy Act 2017* (United Kingdom), section 21(1).

[69] *Digital Economy Act 2017* (United Kingdom), section 23(1)-(2).

[70] British Board of Film Classification, *Submission 187*, p. 8.

[71] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, pp. 1, 4.

[72] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 4.

[73] British Board of Film Classification, *Submission 187*, p. 6.

Implementation status

3.71 As noted above, in October 2019 the UK Government announced that it would not commence the age verification provisions of the DEA. This followed an earlier announcement in June that the date of entry into force of the scheme would be postponed 'due to the failure of officials to notify the BBFC's Guidance on Age-verification Arrangements to the European Commission as required by the Technical Standards and Regulations Directive'.[74]

3.72 Despite electing not to commence the age-verification scheme, the UK Government stated that it expected age verification tools 'to continue to play a key role in protecting children online' as part of its broader online harms regulatory regime.[75] The Under-Secretary of State for Digital, Culture, Media and Sport elaborated in Parliament that the Government wanted to take more time to review the regulatory regime, including its definition of pornographic material and coverage of social media platforms. He stated that:

> Age verification will be a key part of the online harms agenda. It will be a key tool in the box, but the toolbox will, through the online harms agenda, be bigger…we will be bringing it forward for pre-legislative scrutiny so that we can get it right. I hope that the BBFC will be a key part of the future of this process, because its expertise is in the classification of content…We look forward to working together with the BBFC.[76]

3.73 The BBFC submitted that it had been ready to implement the scheme:

> The BBFC had all systems in place ready to undertake our role, to ensure all commercial pornographic websites accessible from the UK would have age-verification controls in place or face swift enforcement action. The adult industry was similarly prepared to implement age-verification, and age-verification providers were undergoing a robust certification process to

[74] British Board of Film Classification, *Submission 187*, p. 2.

[75] Secretary of State for Digital, Culture, Media and Sport, 'ONLINE HARMS: Written statement – HCWS13', <https://www.parliament.uk/written-questions-answers-statements/written-statement/Commons/2019-10-16/HCWS13>.

[76] United Kingdom House of Commons *Hansard*, 17 October 2019, Volume 666, <https://hansard.parliament.uk/commons/2019-10-17/debates/C743945F-9F9F-48E5-9064-707189D07846/OnlinePornographyAgeVerification>.

> ensure they too were ready for entry into force. The Government has acknowledged our preparedness...[77]

3.74 The BBFC submitted that it was required under the DEA to act proportionately and had prioritised the most popular pornographic websites:

> As 70% of UK traffic visit just the top 50 sites - and these sites are owned by an even smaller number of companies - we were confident our efforts would have made a significant impact in a relatively brief period of time.[78]

3.75 The BBFC explained that its engagement with the adult industry had been positive and that it was confident that these large companies would have complied with the requirements of the DEA.[79] Ms Erratt expanded on this point:

> The adult industry believed the new regime would work and saw regulation as inevitable given the international consensus that children should not have unrestricted access to pornography. The BBFC engaged directly with the adult industry, and we anticipated that over 80 per cent of pornographic websites were set to comply with age verification from day one.[80]

3.76 Ms Erratt said there was 'no pushback' from the industry as far as she was aware.[81]

3.77 The eSafety Commissioner submitted that the UK Government had estimated the cost to date of implementing the scheme was approximately $4.15 million, and that the UK Government had requested indemnity of up to approximately $18.84 million for the BBFC in its first year of operation.[82]

Lessons for Australia

3.78 Reflecting on the experience to date in the UK, and in particular criticisms of the proposed age-verification regime, a number of witnesses put forward

---

[77] British Board of Film Classification, *Submission 187*, p. 2.

[78] British Board of Film Classification, *Submission 187*, p. 7.

[79] British Board of Film Classification, *Submission 187*, p. 1.

[80] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 1.

[81] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 4.

[82] eSafety Commissioner, *Submission 191*, pp. 11-12.

lessons for Australia in any consideration of age verification for online pornography.

3.79 Speaking on behalf of the BBFC about the UK experience, Ms Erratt suggested that there were three 'crucial factors' for Australia to consider:

- ensuring there is a level playing field in terms of regulation;
- ensuring age verification is both robust and easy for consumers to use; and
- raising public awareness of age verification, so that consumers understand that age verification is a child protection measure and so that they trust and understand how to use age-verification systems in place.[83]

3.80 A common theme in evidence was the importance of raising awareness and addressing concerns among members of the public. For example, the eSafety Commissioner explained:

> A number of concerns about age verification were raised, including: concerns about data security and privacy; freedom of expression; ease of circumnavigation; and difficulties of enforcement (particularly against non-UK companies). Whilst a number of these concerns were subsequently addressed by the age verification regulator, these were not necessarily adequately explained or communicated to the general public or media. It is imperative that public concerns are addressed head-on, and that there is full transparency over effectiveness and measures taken to address concerns, so that the community and media is brought along.[84]

3.81 Similarly, the Age Verification Providers Association (AVPA) submitted that while 'no significant, valid criticisms' in relation to privacy or technology were put forward by its members, there were clear lessons to be learnt in relation to 'raising public awareness and maintaining credibility that policies will be enforced to drive adoption by content publishers'.[85]

---

[83] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, pp. 1-2.

[84] eSafety Commissioner, *Submission 191*, p. 14. See also: Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 11; Dr Julia Fossi, Expert Advisor, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 16.

[85] Age Verification Providers Association, *Submission 200*, p. 5.

3.82 Mr Iain Corby, Executive Director of the AVPA, told the Committee that there was a failure to explain to the public the rationale of the age-verification regime and the privacy protections that would be in place.[86]

3.83 Dr Julia Fossi, Expert Advisor at the Office of the eSafety Commissioner, suggested that a basis for criticism of the regime was the fact that data protection and privacy standards were not enshrined in the DEA:

> The BBFC put [data protection and privacy] into their certification and their guidance and it's in their standards. But the simple fact that that wasn't put into the legislation itself was an open door to the privacy rights cohort of people.[87]

3.84 Another criticism raised in evidence to the inquiry was that the age-verification regime did not include social media. For example, the eSafety Commissioner explained:

> One of the main criticisms of the DEA was that the legislation was limited to online commercial providers, and therefore did not address the plethora of online pornography that can be easily accessed on social media, gaming websites and search engines. As such, these services would not be required to carry age-verification.[88]

3.85 The eSafety Commissioner suggested that, given evidence about the exposure of young people to sexual and pornographic material on social media, this omission was a 'grave concern for many'. It argued that the UK Government's decision to pursue a wider regulatory regime 'highlights the importance of taking a broad harm-minimisation approach'.[89]

3.86 In its submission, the BBFC stated that the age-verification regime could have been expanded to include social media.[90] Ms Erratt expanded on this point:

> ... there were clauses in the [DEA] that required the regulator to report to government 12 months after entry into force on the effectiveness of the regime.

---

[86] Mr Iain Corby, Executive Director, Age Verification Providers Association, *Committee Hansard*, Canberra, 5 December 2019, p. 11.

[87] Dr Julia Fossi, Expert Advisor, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 12. See also: UK Children's Charities' Coalition on Internet Safety, *Submission 161*, p. 2.

[88] eSafety Commissioner, *Submission 191*, pp. 10-11.

[89] eSafety Commissioner, *Submission 191*, p. 14.

[90] British Board of Film Classification, *Submission 187*, pp. 8, 13.

> In that kind of report, we may have recommended that the government needed to look at social media.[91]

3.87 Evidence in relation to age-verification for social media is discussed in further detail later in this chapter.

3.88 Lastly, eChildhood submitted that a common criticism of the UK approach was 'that it was an imperfect solution that determined teenagers would be able to get around, such as through the use of VPNs [virtual private networks]'.[92]

3.89 In response to this criticism, eChildhood, the BBFC and the AVPA argued that age-verification would prevent many children from inadvertently accessing pornography.[93] Similarly, Collective Shout explained:

> For children, some may be sufficiently tech-savvy to use a free VPN to bypass age verification, or use a parent's VPN if this is not well protected. However, the goal of age verification is not the unrealistic prevention of any access by any child to online pornography but rather to create a significant barrier to access and in particular to prevent inadvertent and casual access.[94]

3.90 Evidence on the effectiveness of online age verification is discussed in further detail in the previous chapter.

Other international approaches

3.91 The Committee received limited evidence on approaches to restricting access to online pornography in other nations.

3.92 The eSafety Commissioner provided an overview which indicated that a range of approaches were in place or under consideration. For example, these approaches included:

- labelling content for certain age groups, authenticating users, and imposing scheduling restrictions on live streaming (in Germany);

---

[91] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 2.

[92] eChildhood, *Submission 192*, p. 22.

[93] eChildhood, *Submission 192*, p. 22; British Board of Film Classification, *Submission 187*, p. 10; Age Verification Providers Association, *Submission 200*, p. 5. See also: Senator Amanda Stoker, *Submission 184*, p. 4.

[94] Collective Shout, *Submission 178*, p. 11.

- mandating default settings to block adult content, which can only be uninstalled with valid identification proving that the user is over 18 (in South Africa); and
- national-level content filtering (in South Korea).[95]

3.93 New Zealand is monitoring the implementation of age verification in the UK and has indicated that it is an option for consideration.[96]

3.94 However, the Committee heard that no jurisdiction had implemented a mandatory scheme for age verification for online pornography.[97]

Evidence on implementation in Australia

3.95 Consistent with the widespread concern among submitters about the harms to children and young people due to exposure to pornography, there was strong support for the introduction of a regime of mandatory age verification for online pornography in Australia.

3.96 This section summarises evidence received during the inquiry on the implementation of such a regime. Evidence on the implementation of online age verification more generally is discussed in the previous chapter.

Possible scope

3.97 As outlined above, the proposed regime for age verification in the UK was intended to cover pornography made available on a commercial basis as defined under the DEA. In evidence to the inquiry, there was some discussion about the appropriate scope of any such scheme in Australia.

3.98 The UNSW Law Society argued that the 'narrow focus' of the UK scheme meant that children would be able to access pornographic material from free sites, through sharing on mobile phones, or from non-pornographic sites such as Twitter, Reddit, and Imgur.[98]

3.99 Again referring to the UK scheme, TrustElevate suggested there may be benefit in addressing the issue of pornographic material in a comprehensive

[95] eSafety Commissioner, *Submission 191*, pp. 23-27. See also: Communications Alliance Ltd, *Submission 186*, p. 4.

[96] eSafety Commissioner, *Submission 191*, pp. 25.

[97] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 3.

[98] UNSW Law Society, *Submission 58*, p. 6.

way, rather than pursuing 'incremental measures' which may disperse users to other, non-commercial sites.[99]

3.100 The eSafety Commissioner submitted that consultation would be required on the services to be incorporated and covered in any mandatory age-verification regime for online pornography.[100]

Free and ad-supported websites

3.101 A clear theme in evidence was that many pornographic websites are able to be accessed for free. Many submissions referred to the website Pornhub, which offers free content supported by advertising, in addition to paid content. Pornhub reported approximately 33 billion site views in 2018.[101]

3.102 The Committee heard that many free pornographic websites—including Pornhub—have a commercial aspect that would ensure they are captured under the broad definition of commerciality under the DEA.[102]

3.103 Mr Dagg from the Office of the eSafety Commissioner explained that the 'overwhelming rationale for operating free platforms is to drive customers into the premium platforms'. Mr Dagg noted that MindGeek, the parent company of Pornhub, also owns 'scores' of premium websites.[103]

3.104 Mr Dagg suggested that the definition of commercial in the DEA was 'a reasonably good place to start'.[104]

Social media services and search engines

3.105 Concern was also raised about the availability of pornographic material on social media websites and via search engines. As noted above, there was some criticism of the UK approach for its failure to include social media

[99] TrustElevate, *Submission 190*, p. 8.

[100] eSafety Commissioner, *Submission 191*, p. 5.

[101] Mr Toby Dagg, Manager, Cyber Report, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 14.

[102] Mr Toby Dagg, Manager, Cyber Report, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 13.

[103] Mr Toby Dagg, Manager, Cyber Report, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 13.

[104] Mr Toby Dagg, Manager, Cyber Report, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 13.

services, and this omission was cited in the UK Government's decision to pursue a wider regulatory regime.

3.106 Collective Shout expressed concern that, while working to improve their practices, social media services 'continue to host pornographic content that is easily accessed by children'.[105] Similarly, Mr Kuan told the Committee:

> Simply typing a pornographic term into a search engine like Google would ...display pornographic content without restriction.[106]

3.107 The Synod of Victoria and Tasmania, Uniting Church in Australia argued that search engines would need to be captured for age-verification to be effective:

> Unless the Government can require search engine corporations to do age verification on users to then not return results for searches for pornography to children, requiring commercial pornography sites to provide age verification would seem to be a limited safeguard.[107]

3.108 The eSafety Commissioner submitted that many social media services use age screening to ascertain whether or not a user is eligible, and that this may 'simply require users to self-declare their age'.[108] However, some submitters argued these measures were not effective.[109]

3.109 In a submission to the inquiry, DIGI, an industry association representing companies including Google, Facebook, and Twitter, outlined a range of measures used by its members to restrict access to pornographic content. These measures include age restrictions, human moderation, and automated technology to detect and remove prohibited content.[110] As an example:

---

[105] Collective Shout, *Submission 178*, p. 10.

[106] Mr Chern Eu Kuan, Student Contributor, UNSW Law Society, *Committee Hansard*, Canberra, 6 December 2019, p. 47.

[107] Synod of Victoria and Tasmania, Uniting Church in Australia, *Submission 183*, p. 6.

[108] eSafety Commissioner, *Submission 191*, p. 6.

[109] For example, see: Synod of Victoria and Tasmania, Uniting Church in Australia, *Submission 183*, pp. 2-3.

[110] DIGI, *Submission 269*, pp. 1-2.

> ... in the last quarter, Facebook removed 98.4% of adult nudity sexual activity content, and 99.5% of child nudity and sexual exploitation content, before it was flagged by users.[111]

3.110 In its submission, the BBFC discussed the question of age verification for social media services:

> Potentially harmful material on social media platforms needs to be addressed but a 'blanket ban' on users aged under 18 is unlikely to be viewed as a satisfactory solution to the problem, either by platforms or by the general public more broadly. Blocking an entire platform is unlikely to be a proportionate response. Perhaps the power to issue fines would be more appropriate.[112]

3.111 The BBFC went on to suggest a number of options:

> These range from voluntary measures to direct statutory intervention, though different enforcement powers would be required than those set out in the DEA. For example, age-verification could be applied at account level and could be monitored by the platform.[113]

3.112 eChildhood submitted that age verification for online platforms including social media services required further investigation, and that these platforms were the target of the Office of the eSafety Commissioner's Safety by Design initiative (see discussion later in this chapter).[114]

Mechanisms for enforcement

3.113 There was some discussion in evidence about the difficulty of enforcing a requirement for age verification given that—as noted above—pornographic material is generally hosted outside Australia.

3.114 eChildhood argued that any age-verification regime must be capable of restricting access to pornographic material, whether it is hosted in Australia or internationally. eChildhood also argued that there should be parity in the treatment of domestic and international websites.[115]

---

[111] DIGI, *Submission 269*, p. 1.

[112] British Board of Film Classification, *Submission 187*, p. 13.

[113] British Board of Film Classification, *Submission 187*, p. 13.

[114] eChildhood, *Submission 192*, p. 32.

[115] eChildhood, *Submission 192*, p. 36.

3.115 The UNSW Law Society submitted that enforcement would be 'incredibly difficult' due to the large number of adult websites, and that compliant sites could be at a competitive disadvantage as children may preferentially seek pornographic material from non-compliant sites.[116]

3.116 However, Ms Erratt told the Committee that the large number of adult websites are 'owned by a relatively small number of companies':

> If you engage with those companies, you can have quite a broad impact on compliance.[117]

3.117 The AVPA argued that extending jurisdiction beyond a country's borders was also a consideration in the physical world and was not necessarily a reason not to impose rules domestically:

> The risk of evading protections by going to offshore, unregulated websites has to be addressed through enforcement, be that through financial blocks on income streams to those websites from the domestic market or through more direct site blocking through internet service providers. ...And a standards based approach adopted globally will provide increased opportunity for international agreements and collaboration to raise standards internationally.[118]

3.118 A focus of discussion was the power under the DEA for the BBFC to issue notices to ancillary service providers, including payment providers such as Visa and MasterCard. Ms Erratt, representing the BBFC, argued that this power was an effective one:

> As you can imagine, the adult industry is financially driven, so the threat of losing income means that these are very effective enforcement powers for any regulator.[119]

3.119 Similarly, Mr Dagg told the Committee:

> ... that approach of targeting ancillary service providers is a good one. If you are undermining the economic viability of those sites then you are directly

---

[116] UNSW Law Society, *Submission 58*, p. 6.

[117] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 4.

[118] Age Verification Providers Association, *Submission 200*, p. 4.

[119] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 1. See also: Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 4.

> affecting the interests of those who run the sites and they are motivated to comply.[120]

3.120 Mr Dagg explained that the Office of the eSafety Commissioner had found that Visa and MasterCard had taken 'swift and absolute' action in instances where their services were being misused to facilitate access to child sexual abuse material:

> In previous investigations we have focused on contacting MasterCard and Visa where we've identified the use of those payment cards to facilitate access to child sexual abuse material. And in respect of the websites that we were targeting, as soon as we notified those card providers through our inquiries with the information that their services were being misused to access child sexual abuse material, we saw an immediate impact on the websites.[121]

3.121 Mr Alastair MacGibbon, former eSafety Commissioner and former National Cyber Security Adviser, also suggested that restricting payments was an important enforcement power, but noted that non-compliant websites might seek to use alternative payment methods.[122] However, Mr MacGibbon emphasised that any approach would involve 'edge cases' where it would fail.[123]

3.122 Mr MacGibbon said that there were other options for enforcement, including blocking non-compliant websites.[124] eChildhood also discussed 'forced blocks' implemented at the ISP level.[125]

3.123 eChildhood proposed that there should be provision for members of the public to report non-compliant sites and that there should be widespread awareness of this facility.[126]

---

[120] Mr Toby Dagg, Manager, Cyber Report, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 20.

[121] Mr Toby Dagg, Manager, Cyber Report, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 20.

[122] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, p. 24. See also: Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 20.

[123] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, p. 24.

[124] Mr Alastair MacGibbon, Private capacity, *Committee Hansard*, Canberra, 6 December 2019, p. 24.

[125] eChildhood, *Submission 192*, p. 31.

[126] eChildhood, *Submission 192*, p. 36.

Privacy regulation and auditing

3.124 It was put to the Committee that any regime for age verification for online pornography should include strong protections for the privacy of users' personal information.[127] Further evidence relating to privacy in the implementation of age verification more generally is discussed in the previous chapter.

3.125 Eros Association was concerned that implementation of an age-verification model similar to that proposed for the UK would create a 'honey pot' of personal information that may be hacked or leaked.[128]

3.126 As noted above, while the Committee heard that the regulator in the UK had attempted to address this concern through data protection and privacy standards, a criticism was that these standards were not enshrined in legislation. The eSafety Commissioner explained:

> The fact that the legislation itself did not contain any guidance, technical requirements or conditions for data storage expected of age verification solutions was considered inattentive, particularly given the sensitivities in relation to data security and privacy that age verification involve. Whilst the BBFC made clear in its own guidance and voluntary certification scheme of the expectations and obligations in relation to data protection and privacy, the fact that these details were not translated into the core of the DEA legislation itself was of concern.[129]

3.127 The Australian Christian Lobby suggested that it 'would be unacceptable for adult sites to retain any identification of users'.[130] Similarly, eChildhood submitted:

> For adults who wish to access pornography online, the fact that they are accessing pornography and information regarding their personal pornography preferences, is sensitive personal information that must not be misused.[131]

3.128 There was general agreement about the use of third-party age verification such that no personal information is passed between a pornographic website

---

[127] For example, see: UNSW Law Society, *Submission 58*, p. 8; eSafety Commissioner, *Submission 191*, p. 5.

[128] Eros Association, *Submission 65*, p. 3.

[129] eSafety Commissioner, *Submission 191*, p. 11.

[130] Australian Christian Lobby, *Submission 160*, p. 6.

[131] eChildhood, *Submission 192*, p. 21.

and an age-verification provider.[132] Third-party verification is discussed in detail in the previous chapter.

3.129 eChildhood and the UNSW Law Society noted that obligations under the *Privacy Act 1998* and the Australian Privacy Principles would apply to age-verification providers.[133] However, eChildhood argued that, 'due to the sensitive nature of access to and personal preferences with respect to online pornography', these obligations should be supplemented with more stringent privacy protections.[134]

3.130 eChildhood also recommended including in any age-verification legislation the individual's right to be forgotten, similar to the provision in the European Union General Data Protection Regulation (see discussion in the previous chapter).[135]

3.131 As discussed in the previous chapter, the BBFC established a voluntary scheme whereby age-verification providers could be audited for compliance with privacy and data security requirements.[136]

3.132 The eSafety Commissioner suggested that a prerequisite for the implementation of a mandatory age-verification regime would be the establishment of 'processes and procedures to test, monitor, audit and provide oversight on age verification technical solutions and tools'.[137]

Community and industry consultation

3.133 eChildhood submitted that in order to ensure any age-verification legislation is effective, 'thorough consultation with all key stakeholders and digital experts is imperative':

> This will enable a robust, flexible and researched outcome that includes safety, security and privacy.[138]

---

[132] For example, see: eChildhood, *Submission 192*, p. 21.

[133] eChildhood, *Submission 192*, p. 21; UNSW Law Society, *Submission 58*, p. 7.

[134] eChildhood, *Submission 192*, p. 21.

[135] eChildhood, *Submission 192*, p. 21.

[136] British Board of Film Classification, *Submission 187*, p. 11.

[137] eSafety Commissioner, *Submission 191*, p. 5.

[138] eChildhood, *Submission 192*, p. 33.

3.134 The eSafety Commissioner nominated several areas where consultation may be required prior to implementing a mandatory age-verification scheme for online pornography:

- consultation with the public (children and young people as well as adults), adult industry, internet service providers, social media platforms, mobile phone providers, civil rights groups, human rights groups, NGOs to ascertain views on, and support for, the use of age verification to protect children and young people from online pornography
- public consultations on any draft guidance to any regulatory approach to age verification, standards and classes or types of services to be incorporated and covered
- broad consultation with federal and state regulators to develop a national strategy and to ensure for harmonisation and interoperability across jurisdictions.[139]

3.135 eChildhood nominated several matters to be determined in a consultation process, including the appointment of an appropriate regulatory body (see discussion in the next section).[140]

3.136 Speaking to the Committee about work done in preparation for the proposed age-verification regime in the UK, Ms Erratt said that the BBFC engaged with industry and also carried out 'full-scale public consultation'. The BBFC was also planning a public engagement program to educate consumers about age verification:

> We really did understand the importance of ensuring that consumers understood why age verification was coming in, which was to protect children, and that they understood how to age verify safely.[141]

3.137 The eSafety Commissioner also noted the importance of awareness raising and education to inform the public about the rationale for age verification for online pornography and the safeguards in place to address privacy, security, and safety concerns.[142]

3.138 The Committee notes evidence from the eSafety Commissioner that additional resources may be required were her office to be tasked with

---

[139] eSafety Commissioner, *Submission 191*, p. 5.

[140] eChildhood, *Submission 192*, p. 28.

[141] Ms Amelia Erratt, Head, Age Verification, British Board of Film Classification, *Committee Hansard*, Canberra, 5 December 2019, p. 3.

[142] eSafety Commissioner, Submission 191, p. 5.

carrying out further work on age verification, such as reviewing and testing appropriate technologies and negotiating with industry bodies.[143]

Regulatory oversight

3.139 In its submission, eChildhood considered the appointment of a body to oversee an age-verification regime in Australia, suggesting that appropriate bodies may include the Office of the eSafety Commissioner, the Australian Classification Board, and the Australian Communications and Media Authority.[144]

3.140 In relation to the Office of the eSafety Commissioner, eChildhood noted its existing mandate to coordinate and lead online safety efforts:

> The [Office of the eSafety Commissioner] may be well-positioned to regulate and enforce an Age Verification regime for the purpose of providing online safety to children. It already has similar obligations and responsibilities, is well-known and respected within the industry and has both national and International support networks. It has a platform within schools and other online safety education arenas to promote the system and disseminate information about it.[145]

3.141 However, eChildhood suggested that a decision in relation to the appropriate regulator would be an important outcome of any consultation process, and that whichever body was appointed would need to be provided with adequate resources to ensure that effective implementation of the regime was maintained.[146]

Evidence on complementary measures

3.142 The Committee heard evidence about a range of technological and other measures that could complement age verification in order to minimise or address the harms associated with exposure of children and young people to online pornography.

---

[143] Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, pp. 16-17.

[144] eChildhood, *Submission 192*, pp. 28-29.

[145] eChildhood, *Submission 192*, p. 28.

[146] eChildhood, *Submission 192*, p. 28.

Filtering and blocking

3.143 The Committee heard about other technologies to protect children and young people from exposure to online pornography, including network- and device-level filtering and ISP blocking.[147]

3.144 For example, the Family Friendly Filter scheme, introduced in 2005, requires that ISPs make available approved filters for end users to install.[148] As noted above, the eSafety Commissioner refers adult and explicit overseas-hosted content to suppliers of filters under the scheme to ensure that this content is blocked.[149]

3.145 The eSafety Commissioner submitted that filtering services 'can be a useful tool to support those looking to moderate children's access to online content, particularly in relation to very young children'.[150]

3.146 The eSafety Commissioner explained that device-level filtering products were found to be the most effective, but that these did not offer complete protection for families and children.[151]

3.147 As an alternative, ISP blocking involves maintaining a blacklist of addresses for ISPs or internet infrastructure operators to block on their systems.

3.148 However, the eSafety Commissioner submitted that blocking systems suffer from a number of limitations, including over- and under-blocking, ease of circumvention, and high maintenance and administration costs. Further, blocking systems are unable to capture all internet traffic and there is 'very little publicly available information' on their effectiveness and accuracy.[152]

3.149 eChildhood discussed filtering and blocking in some detail in its submission, arguing that these solutions lack robustness and should not be relied on in isolation.[153]

---

[147] For example, see: eSafety Commissioner, *Submission 191*, pp. 15-17.

[148] Communications Alliance, *Submission 186*, p. 5; eSafety Commissioner, *Submission 191*, p. 15.

[149] eSafety Commissioner, *Submission 191*, pp. 3-4, 15.

[150] eSafety Commissioner, *Submission 191*, p. 15.

[151] eSafety Commissioner, *Submission 191*, p. 17; Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 11.

[152] eSafety Commissioner, *Submission 191*, p. 17.

[153] eChildhood, *Submission 192*, pp. 29-32.

3.150 The eSafety Commissioner recommended that an effective approach to minimising exposure to online pornography would involve a 'combination and layering of technological solutions'.[154]

Safety by Design initiative

3.151 The Committee heard about the Safety by Design initiative (SbD), which seeks to ensure that user safety is considered in the design and development of online products and services. The development of SbD is being led by the eSafety Commissioner.[155]

3.152 The eSafety Commissioner explained:

> At its core, [SbD] is about embedding the rights of users and user safety into the design, development and deployment of online and digital products and services.
>
> ... It recognises and responds to the intersectionality of risk and harm in the online world and acknowledges the potential of advancements in technology, machine-learning and artificial intelligence to radically transform user safety and our online experiences.[156]

3.153 The eSafety Commissioner emphasised the importance of considering online safety in a holistic manner 'rather than addressing issues in an ad hoc manner', and also proactively considering user safety 'rather than retrofitting safety considerations after online harms have occurred'.[157]

3.154 The Committee heard that age verification was one tool that could be used in incorporating user safety in the design of online platforms.[158]

3.155 Following consultation with industry, parents and carers, and children, the eSafety Commissioner developed a set of three SbD principles that 'provide online and digital interactive services with a universal and consistent set of realistic, actionable and achievable measures to better protect and safeguard citizens' safety online'. These principles are:

---

[154] eSafety Commissioner, *Submission 191*, p. 16.

[155] eSafety Commissioner, *Submission 191*, pp. 20-22. See also: eSafety Commissioner, 'Safety by Design', <https://www.esafety.gov.au/key-issues/safety-by-design>.

[156] eSafety Commissioner, *Submission 191*, p. 20.

[157] eSafety Commissioner, *Submission 191*, p. 20.

[158] Dr Julia Fossi, Expert Advisor, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 13.

- service provider responsibilities;
- user empowerment and autonomy; and
- transparency and accountability.[159]

3.156 The eSafety Commissioner explained that consultations also identified that young people expect industry to be proactive in identifying and minimising exposure to threats, risks, and harmful content.[160]

3.157 The eSafety Commissioner is in the process of creating a framework and resources to facilitate the adoption of SbD principles.[161]

Education

3.158 A clear theme in evidence to the inquiry was that education to address the harms associated with exposure to online pornography would complement technological measures such as age verification.

3.159 The eSafety Commissioner submitted that it is imperative that young people are assisted to navigate their digital environment:

> It is developmentally appropriate that young people are sexually curious and have an interest in what constitutes healthy sexual relationships. As such, young people will explore their sexual identities and search for information about relationships online.
>
> ... A child's educational journey therefore presents a critical opportunity for evidence-based education and awareness raising to address children's exposure to sexually explicit material and online pornography.[162]

3.160 Citing research that indicated that 94 per cent of parents with pre-schoolers reported that their child was using the internet by age four, the eSafety Commissioner suggested that such education 'needs to start early'.[163]

3.161 The eSafety Commissioner recommended that education about respectful relationships and online safety—including age-appropriate education on

---

[159] eSafety Commissioner, *Submission 191*, pp. 20-21.

[160] eSafety Commissioner, *Submission 191*, p. 21. See also: Dr Julia Fossi, Expert Advisor, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 16.

[161] eSafety Commissioner, *Submission 191*, pp. 21-22.

[162] eSafety Commissioner, *Submission 191*, p. 17.

[163] eSafety Commissioner, *Submission 191*, p. 18.

dealing with online pornography—should be embedded in the Australian Curriculum.[164]

3.162 Similarly, the child protection advocacy group Bravehearts, recommended 'developmentally appropriate sex education for schools, inclusive of positive and healthy relationships, consent issues and awareness of the online environment':

> ... one of the most important tools we have is education and ensuring that children have access to honest, developmentally appropriate sex education and personal safety programs.[165]

3.163 The UNSW Law Society submitted there are 'structural problems' with sex education programs and that these programs could be supplemented with 'information about how pornography can display unrealistic and harmful behaviours towards sex'.[166]

3.164 Ms Carol Ronken, Director of Research at Bravehearts, argued that education should aim to teach children to be 'critical consumers' of online material.[167]

3.165 This message was echoed by the eSafety Commissioner, who submitted that education should incorporate 'broad-based relationship, critical thinking and resilience skills that enable young people to critically interpret online media and cope with potential exposure to harmful content'.[168] Ms Inman-Grant explained:

> I often talk about the filter between our children's ears—their brains—and that's where the education and critical reasoning skills are really, really important.[169]

3.166 Concern was expressed about a lack of consistency across the country in relation to sex- and online safety education, and about competing priorities in the curriculum.[170] For example, Ms Inman-Grant told the Committee:

---

[164] eSafety Commissioner, *Submission 191*, p. 19.

[165] Bravehearts, *Submission 182*, pp. 3-4.

[166] UNSW Law Society, *Submission 58*, p. 9.

[167] Ms Carol Ronken, Director of Research, Bravehearts, *Committee Hansard*, Canberra, 6 December 2019, p. 57.

[168] eSafety Commissioner, *Submission 191*, p. 18.

[169] Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 18.

> We know, with our fragmented education system, that online safety education and respectful relationships education is not happening consistently and comprehensively across the public, independent and Catholic schools. It is a concern.[171]

3.167 Mr Marshall Ballantine-Jones, a PhD candidate undertaking research on reducing the negative effects of pornography and sexualised media on adolescents, submitted that there are 'only a handful' of education programs that address pornography and sexualised media, and that none of these have been empirically tested for effectiveness.[172]

3.168 The Department of Social Services advised that it provided the charity Our Watch with $3.129 million over four years from 2016-17 to deliver an 'evidence-based community awareness initiative to understand and counter the impact of pervasive pornography on young people'. However, the Department also advised that the campaign had yet to launch.[173]

3.169 Ms Elizabeth Hefren-Webb, Deputy Secretary of the Department, told the Committee:

> It's really tricky to develop a campaign about porn that doesn't breach community standards and parents' standards about what young people should be hearing. ...The materials that have been developed targeting parents, we think, are in good shape, but the materials targeting people under 18—we don't think we've got the right pitch yet.[174]

3.170 The eSafety Commissioner recommended further research into what constitutes effective education on online pornography, 'including content, pedagogy, professional learning and support for vulnerable cohorts':

> This should also include capacity building and support for educators to develop knowledge, skills, capacity and confidence to cover this content.[175]

---

[170] eSafety Commissioner, *Submission 191*, pp. 18-19; Ms Carol Ronken, Director of Research, Bravehearts, *Committee Hansard*, Canberra, 6 December 2019, p. 58.

[171] Ms Julie Inman-Grant, eSafety Commissioner, Office of the eSafety Commissioner, *Committee Hansard*, Canberra, 6 December 2019, p. 12.

[172] Marshall Ballantine-Jones, *Submission 175*, p. 2.

[173] Department of Social Services, *Submission 163*, pp. 6-7.

[174] Ms Elizabeth Hefren-Webb, Deputy Secretary, Families, Department of Social Services, *Committee Hansard*, Canberra, 6 December 2019, p. 7.

[175] eSafety Commissioner, *Submission 191*, p. 19.

3.171 As noted in the previous section, the Committee also heard about the role for education in informing the public about the rationale for age verification, and the safeguards in place, to allay fears about the privacy and safety of pornography users.

Integration with a wider eSafety approach

3.172 Consistent with the evidence outlined in this section, a key message of the eSafety Commissioner was that online harms should be addressed as part of a wider approach to online safety:

> It is clear that there are no quick-fix solutions to any online safety issue, but that long-term, sustained social and cultural change to protect children online requires the coordinated efforts of the global community and greater collaboration and consultation between industry, government and the general public. There is no silver bullet, and age verification will only ever be one part of the solution.[176]

3.173 Similarly, Bravehearts argued that age verification can only be effective as part of a holistic approach to addressing online threats, including research, education, and preventive measures.[177]

Committee comment

3.174 The Committee recognises that there is increasingly clear evidence that children and young people are being exposed to online pornography, and that this exposure is associated with a range of risks and harms.

3.175 Evidence given to the inquiry showed very clearly that there is widespread and genuine concern among the community about the negative impact of online pornography on the welfare of children and young people.

3.176 Based on the evidence to the inquiry, it is the Committee's strong view that age verification should be pursued as a measure to limit children and young people's exposure to online pornography.

3.177 The Committee acknowledges that age verification is not a silver bullet—some websites containing pornographic material may not be captured, and some determined young people may find ways to circumvent the system. However, when it comes to protecting children from the very real harms

[176] eSafety Commissioner, *Submission 191*, p. 22.

[177] Bravehearts, *Submission 182*, pp. 3-4.

associated with exposure to online pornography, the Committee's strong view is that we should not let the perfect be the enemy of the good.

3.178 It is the Committee's expectation that an effective age-verification regime will create a significant barrier to prevent young people—and particularly young children—from deliberately or, perhaps even more importantly, inadvertently gaining access to pornographic material. In doing so, age verification will work best to protect the most vulnerable from the harms associated with exposure to online pornography.

3.179 The Committee however notes the experience in the United Kingdom, where the implementation of age verification has stalled, and also the lack of precedent for a regime of mandatory age verification in any other jurisdiction. This is evidence of the challenge of implementing an effective regime, and an indication that there is still more work to do.

3.180 An effective regime will require robust standards for privacy, safety, and security, broad understanding and acceptance among the community, support from the adult industry and age-verification providers, and a well-resourced regulator with appropriate powers.

3.181 Consideration will also need to be given to the most appropriate legislative and regulatory regime, as well as to what extent the regime should seek to capture social media, search engines, and other online services. All of these issues will need to be worked through, but it is the Committee's view that these mediums should be caught by an age-verification regime.

3.182 Further to this, a clear message in evidence to the inquiry is that an effective response to the exposure of children and young people to online pornography will be broader than age verification. Other technical solutions, education, and a broader focus on e-safety will all contribute to minimising harms from online pornography and bringing about a safer online environment for our children.

3.183 In this context, the Committee recommends that the eSafety Commissioner lead the development of a roadmap for the implementation of age verification for online pornography.

Recommendation 3

3.184 The Committee recommends 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, setting out:

a. a suitable legislative and regulatory framework;

b. a program of consultation with community, industry, and government stakeholders;

c. activities for awareness raising and education for the public; and

d. recommendations for complementary measures to ensure that age verification is part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.

3.185 As a dedicated office with relevant expertise, industry knowledge, and an understanding of the broader issues associated with online safety, the Committee considers that the eSafety Commissioner is best placed to ensure that the issues set out above are addressed as part of a comprehensive set of measures involving age verification.

3.186 As a basis for consideration, the Committee offers the following principles based on evidence to the inquiry:

- at a minimum the regime should seek to capture pornographic material made available on a commercial basis, consistent with the definition established in the United Kingdom;
- the regime should also capture pornographic material accessed via and/or available on non-commercial websites as well as social media platforms, search engines, and other online services;
- enforcement powers should include the power to direct ancillary service providers (such as payment providers) to withhold services from non-compliant websites;
- appropriate standards relating to privacy, safety, and security should be incorporated in legislation; and
- consultation with industry and members of the community, and education and awareness raising about the purpose of age verification, should commence as early as possible in the process.

3.187 In carrying out this work, the Committee expects that the eSafety Commissioner would consult with regulators in other jurisdictions—including the British Board of Film Classification—to leverage existing work and to ensure consistency where this is appropriate.

3.188 The Committee also expects that the eSafety Commission would consult with the Digital Transformation Agency in relation to the development of

appropriate technical standards for age verification (see Recommendation 1) and an age-verification exchange (see Recommendation 2) to ensure that any regime for age verification for online pornography leverages these more general capabilities.

3.189 Lastly, the Committee is concerned to see this issue addressed as quickly as possible. As such, the Committee recommends that this work be completed and presented to government for decision within 12 months of the presentation of this report.

3.190 The Committee encourages the Australian Government to provide additional resources to the Office of the eSafety Commissioner as is required to complete this work without compromising the important existing work carried out by the office.

4. Age verification for online wagering

4.1 In contrast to online pornography, an identity verification regime, which provides for age verification, has been introduced for online wagering in Australia, as part of measures to combat money laundering and terrorist financing. The evidence received by the Committee about online gambling focused mainly on issues relating to this existing legal framework.

4.2 This chapter discusses recent research on the prevalence and risks of online gambling by young people. It examines Australia's current verification process for access to online wagering services, and the upcoming review of the requirements, as well as international comparisons. This chapter also notes evidence received on some related issues, including other proposed measures for protecting minors from online wagering.

Access to online wagering by children and young people

4.3 With the prevailing use of digital and smart technology, the availability of online products - such as gambling - has become more readily accessible to everyone, including children and young people. The Victorian Responsible Gambling Foundation (VRGF) states that:

> Adolescents today are increasingly exposed to gambling marketing through social media, online advertising and sports coverage, alongside increased

> accessibility and opportunities to gamble with the rise of internet and smart phone access.[1]

4.4 The New South Wales Responsible Gambling Fund (RGF) also identified accessibility as an issue, noting the link between accessibility and the potential for young people to experience problem gambling later in life. Specifically, the RGF cited recent research which indicates:

> …that increased availability of, and access to, gambling products for young people is associated with greater gambling participation; and as a result, a higher chance the users will experience gambling problems and gambling harm in later years.[2]

4.5 These problems are said to be compounded by a young person's limited capacity to assess risk. In particular, it has been found that 'compared to adults, adolescents may be even more vulnerable to the harmful effects of gambling as their ability to assess risks is still developing'.[3]

Estimates of gambling by children and young people

4.6 The Australian Institute of Family Studies (AIFS) has identified online gambling as the fastest growing segment of the Australian gambling market:

> The proportion of people who placed a bet on sports, racing or other events via the internet is estimated to have almost doubled between 2012 and 2018 – from 16% to 34%.[4]

4.7 There is little available research on the prevalence of online gambling by young people or the impact of this behaviour. However, research

---

[1] Victorian Responsible Gambling Foundation, *The prevalence and correlates of gambling in secondary school students in Victoria, Australia, 2017,* October 2019, p. 1.

[2] New South Wales Responsible Gambling Fund, *Submission 173*, p. 1.

[3] Australian Institute of Family Studies, *Gambling Activity Among Teenagers and their Parents*, <http://www3.aifs.gov.au/institute/media/docs/r1GpIwOaS7tS/LSAC-ASR-2018-Chap7-gambling.pdf>. Growing Up in Australia Longitudinal Study of Australian Children 2018 Annual Statistical Report.

[4] Australian Institute of Family Studies, *National Consumer Protection Framework for Online Wagering: Baseline Study, Final Report, June 2019,* p. 6, <https://www.dss.gov.au/sites/default/files/documents/11_2019/d19_887121_final_baseline_study_-_national_consumer.pdf>.

undertaken by the VRGF, which was cited in several submissions to the inquiry, does provide some insights into gambling by young people.[5]

4.8 In a recently published study of Victorian secondary school students, the VRGF found that:

- almost one in three students (31 per cent) reported that they had gambled at some time in the past;
- among students who had gambled at some time in the past, nearly one quarter (21 per cent) reported having gambled in the last 30 days. The median amount of money spent by those who had gambled in the last month was $9.30; and
- among students who had ever gambled, the most frequently reported modality was 'at home or at a friend's home' (52 per cent), followed by a parent or guardian purchasing or playing for them (51 per cent).[6]

4.9 Most relevant to this inquiry was the finding that online gambling by students (18 per cent) was reported to be relatively more common than gambling at a pub or club (10 per cent) or casino (1 per cent).[7]

4.10 The AIFS has also conducted research on gambling by young people aged 16-17 years. In its longitudinal study, it found that 16 per cent of 16–17 year olds reported spending money on at least one gambling activity in the past 12 months. In addition, just under five per cent (one in 20), or around 9,000 17 year old children reported spending money on gambling activities that are illegal due to age restrictions such as poker machines, poker, and casino table games.[8]

Social impacts

4.11 The negative impact of gambling by young people was succinctly described by the VRGF:

---

[5] See NSW Responsible Gambling Fund, *Submission 173*; Alliance for Gambling Reform, *Submission 179*; Department of Social Services, *Submission 163*; Australian Gambling Research Centre, *Submission 166*.

[6] Victorian Responsible Gambling Foundation, *The prevalence and correlates of gambling in secondary school students in Victoria, Australia, 2017*, October 2019, pp. 1-2.

[7] Victorian Responsible Gambling Foundation, *The prevalence and correlates of gambling in secondary school students in Victoria, Australia, 2017*, October 2019, p. 2.

[8] Australian Institute of Family Studies, *Gambling Activity Among Teenagers and their Parents*, <http://www3.aifs.gov.au/institute/media/docs/r1GpIwOaS7tS/LSAC-ASR-2018-Chap7-gambling.pdf>. Growing Up in Australia Longitudinal Study of Australian Children 2018 Annual Statistical Report, p. 79.

> Adolescent gambling has been associated with negative impacts on school performance and family and peer relationships, depression, and is also correlated with engagement in other risk behaviours such as alcohol and other drug use.[9]

4.12 In its submission, the Australian Christian Churches (ACC) listed some of the negative outcomes associated with gambling more generally. In addition to financial loss, these outcomes include:

- harm to the problem gambler and their family;
- mental and physical health problems;
- difficulty in maintaining employment, and struggling to maintain personal relationships; and
- loss of quality family time together.[10]

4.13 The ACC also noted that gamblers are six times more likely than non-gamblers to divorce, and four times more likely to suffer from alcohol abuse.[11]

4.14 While these latter impacts are not specific to children and young people, the ACC advocated for the protection of young people from the 'dangers of online addiction while they are still vulnerable'.[12] It was a sentiment shared by other submitters; that young people need to be prevented from accessing online wagering to minimise the potential harm associated with gambling products – now and in the future.

Regulation of online wagering in Australia

4.15 Wagering services, as defined in Section 4 of the *Interactive Gambling Act 2001* (Cth), are services for directly or indirectly placing, making, receiving or accepting bets. Wagering is a sub-set of gambling, generally relating to betting on sports or races—as distinct from 'gaming', which covers gambling in forms such as lotteries and video games.

4.16 To participate in online wagering in Australia, licensed operators must verify the identity of every customer who opens a wagering account. This regime is governed by the Commonwealth *Anti-Money Laundering and*

---

[9] Victorian Responsible Gambling Foundation, *The prevalence and correlates of gambling in secondary school students in Victoria, Australia, 2017*, October 2019, p. 1.

[10] Australian Christian Churches, *Submission 69*, p. 2.

[11] Australian Christian Churches, *Submission 69*, p. 2.

[12] Australian Christian Churches, *Submission 69*, p. 2.

Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (AML-CFT Rules), made under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (*AML-CFT Act).

4.17 The eSafety Commissioner told the Committee that verifying the identify of a customer means wagering operators need to verify a customer's full legal name, date of birth and current residential address within 14 days of depositing funds.[13]

4.18 Online wagering providers undertake identity verification by cross checking the information provided by customers with various government and non-government data sources. This includes, but is not limited to:

- driver licence;
- passport;
- Australian Electoral Roll;
- tenancy roll;
- the white pages;
- ASIC; and
- credit history records.[14]

4.19 Generally, online wagering providers will outsource these verification checks to third party providers. The options and methods used for such verification are discussed in Chapter 2 above.

4.20 The Department of Social Services noted that under the Rules, there is no exemption for online wagering providers to meet the customer verification time frame of 14 days. If there is a breach of the 14-day timeframe, a maximum penalty of $21 million may be applied.[15]

National Consumer Protection Framework

4.21 The National Consumer Protection Framework for Online Wagering (the National Framework) was developed by the Commonwealth and State and Territory governments to provide 'a set of standard minimum protections for online gamblers, which must be adhered to by all online wagering providers'.[16] The National Framework commenced on 26 November 2018,

---

[13] eSafety Commissioner, *Submission 191*, p. 8.

[14] eSafety Commissioner, *Submission 191*, p. 8.

[15] Department of Social Services, *Submission 163*, p. 3.

[16] Department of Social Services, *National Consumer Protection Framework for Online Wagering*, <https://www.dss.gov.au/sites/default/files/documents/11_2018/ncpfow-fact-sheet28-nov-2018-2.pdf>.

and consists of ten 'consumer protection measures which aim to minimise the harms to Australians gambling online'.[17]

4.22 A key element of the National Framework was the introduction of the 14 day customer verification period, which represented a significant reduction from the previous 90 day period. The 14 day verification period came into effect on 26 February 2019 under an amendment to the Rules.[18]

4.23 The Department of Social Services explained that this reduction was critical because:

- quicker age and identity verification processes were needed to better identify and reduce the potential harms associated with underage online wagering and any customers who may have self-excluded from online wagering activities;
- it better assisted online wagering providers to address any fraudulent activities, money laundering, and guard against reputational, operational and legal risks; and
- the 90 day timeframe did not reflect the current environment of advancing technology, or account for the speed and ease of completing a verification process online.[19]

4.24 While the 14 day customer verification period does not prevent an individual from opening a wagering account and gambling within this period, it does prevent a customer from being paid his or her winnings. In other words, a customer's age and identity must be verified before any money can be paid out. In addition, should a person be found to be under 18 years of age, online wagering providers must return all deposited funds and close the account immediately.[20]

Review of customer verification period.

4.25 The National Framework provided for the Commonwealth to commence a review of the 14-day customer verification period in February 2020, with a

[17] Department of Social Services, *Submission 163,* p. 3. See also: National Policy Statement, <https://www.dss.gov.au/sites/default/files/documents/11_2018/national-policy-statement.pdf>.

[18] Ms Elizabeth Hefren-Webb, Deputy Secretary, Families, Department of Social Services, *Committee Hansard*, Canberra, 6 December 2019, p. 1.

[19] Department of Social Services, *Submission 163,* p. 3.

[20] Department of Social Services, *Submission 163,* p. 4.

view to reducing it to 72 hours.[21] In its submission to the inquiry, the Department of Social Services advised the Committee that the review would involve consultation with industry and other critical stakeholders to ensure that any changes reflect current technological solutions and social changes.[22]

Customer verification and/or age verification for online wagering in other jurisdictions

4.26 Limited evidence was provided on the customer verification processes used in overseas jurisdictions. The Committee was advised that 'Australia now has one of the shorter maximum verification periods' for online wagering accounts compared to other countries. For example, in Gibraltar, Denmark, Italy and Nevada verification periods range from 72 hours to 30 days. [23]

4.27 Many submissions to the inquiry highlighted the United Kingdom as an example of best practice in customer verification for online gambling.

4.28 In May 2019, the UK Gambling Commission moved from a 72 hour age verification period to a mandatory verification rule.[24] This change, which followed a lengthy consultation process, requires online wagering licensees to verify the age and personal details (name and address) of any customer **before** the customer can:

- deposit funds into an account;
- access any free-to-play games the licensee may make available; or
- gamble with the licensee with either their own money or a free bet or bonus. [25]

Video games

4.29 Gambling or simulated gambling in video games does not fall within the definition of wagering under the *Interactive Gambling Act 2001*, as outlined in

---

[21] See National Policy Statement, *Customer Verification,* p. 8, <https://www.dss.gov.au/sites/default/files/documents/11_2018/national-policy-statement.pdf>.

[22] Department of Social Services, *Submission 163,* p. 4.

[23] Department of Social Services, *Submission 163,* p. 6.

[24] See <https://www.gamblingcommission.gov.uk/news-action-and-statistics/News/new-age-and-identity-verification-rules-changes-to-the-lccp-from-tuesday-7-may>.

[25] See <https://www.gamblingcommission.gov.uk/PDF/AV-CI-Consultation-responses-Feb-2019.pdf>.

paragraph 4.15. These matters therefore fall outside the scope of the present inquiry.

4.30 Nevertheless, the Committee noted that in the UK there have been calls for the regulation of betting features known as 'loot boxes' and 'skins' that feature in some video games. In particular, there is concern:

> …at how firmly embedded gambling-type features are in many of these games. The rise of loot boxes and skin betting have seen young people introduced to the same mechanisms that underpin gambling, through an industry that operates unchecked and unregulated on the back alleys of the internet, which young people can access from their bedrooms.[26]

4.31 The AIFS pointed out to the Committee that this issue was raised by its Australian Gambling Research Centre in its submission to a 2018 Senate Environment and Communications References Committee Inquiry into *Gaming Micro-Transactions for Chance Based Items.* The Centre recommended prohibiting micro-transactions for chance-based items in online games available in Australia.[27]

4.32 In its inquiry report, the Senate Committee recommended that the Australian Government undertake a comprehensive review of loot boxes in video games including further research into the potential for gambling-related harms, any regulatory or policy gaps, the adequacy of the classification scheme and existing customer protection frameworks, and consistency with international counterparts.[28]

4.33 The recommendations were noted by the Government.[29] In its response to the inquiry, the Government referred to research carried out in 2018 by the Department of Communications and the Arts on community views on loot boxes and simulated gambling in games. The research identified concern among parents and gamers about loot boxes that resemble gambling, such as

---

[26] 'Charity warns that betting features in video games harm young people', *The Guardian,* 20 December 2019, <www.theguardian.com/society/2019/dec/20/charity-warns-that-betting-features-in-video-games-harm-young-people>.

[27] Australian Institute of Family Studies, *Submission 166*, Appendix 1, p. 5.

[28] Senate Environment and Communications References Committee, *Gaming micro-transactions for chance-based items,* 27 November 2018.

[29] Australian Government, *Response to the Senate Environment and Communications References Committee report: Gaming micro-transactions for chance-based items*, March 2019, <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Gamingmicro-transactions/Government_Response>.

those that can be purchased with 'real world' money and those where items of substantial value to players are at stake.[30]

4.34 The Committee is also aware of the Australian Government's review of classification regulation, which is considering whether the criteria for classifying content, including video games, is appropriate and reflects community concerns.[31]

Views on further changes in Australia

4.35 The most consistent view put to the Committee was the need to reduce the customer verification period from the current 14 days to a mandatory verification system.[32] This would prevent any online gambling from occurring until a person's identity was verified, and also introduce consistency between on-line and on-premises gambling products.

4.36 For example, AIFS recommended that:

> …age (>=18 years) should be verified prior to any engagement in online wagering activity. This would bring online age verification in line with immediate age verification requirement for land-based gambling venues in Australia.[33]

4.37 Similar to the UK's age verification requirements, the AIFS proposed that age should be verified before a customer can access an online wagering account; deposit funds into an account; gamble either with their own money or a free bet or promotion; and access any free-to-air games hosted by online wagering providers.[34]

4.38 While acknowledging the intention of the National Framework review to reduce the customer verification timeframe from 14 days to 72 hours, some,

---

[30] Department of Communication and the Arts, *2018 classification survey report: loot boxes and simulated gambling in games*, <https://www.classification.gov.au/sites/default/files/2019-10/classification-survey-report-loot-boxes-and-simulated-gambling-in-games-novemberanddecember2018.pdf>.

[31] Department of Infrastructure, Transport, Regional Development and Communications, *Review of Australian classification regulation*, <https://www.communications.gov.au/have-your-say/review-australian-classification-regulation>.

[32] See Australian Gambling Research Centre, *Submission 166*; Children's Charities Coalition on Internet Safety, *Submission 161*; Alliance for Gambling Reform, *Submission 179*; Responsible Gambling Fund Trust, *Submission 173*; Synod of Victoria and Tasmania Uniting Church, *Submission 183*.

[33] Australian Institute for Family Studies, *Submission 166,* p. [4].

[34] Australian Institute for Family Studies, *Submission 166,* p. [4].

such as the Responsible Gambling Fund, considered that the proposed change does not go far enough.[35] This is because people are still able to gamble while waiting for their verification.

4.39 The Alliance for Gambling Reform submitted that:

> the current 14 day requirement is an unreasonable delay that poses unnecessary dangers to children online. This window allows 14 days for a child to experiment with an adult product before their account is forcibly closed.[36]

4.40 In pressing its case for verification-first, the Alliance for Gambling Reform used the example of purchasing a mobile phone SIM card:

> Just as an individual is required to submit 100 points of identification upon purchasing a mobile phone SIM card in Australia, so too should they be required to be verified as over 18 years of age before depositing any money into an online wagering account, or placing a bet.[37]

4.41 Not all submissions to the inquiry supported further reductions in customer verification periods. For example, Responsible Wagering Australia (RWA) drew attention to the already-strong measures in place within the wagering industry:

> The Australian-licensed online wagering industry has the absolute strongest protections in place of any age-restricted product available in Australia to protect access by minors.[38]

4.42 Furthermore, the RWA stated that it is 'virtually impossible for a minor to operate an account with an Australian-licensed [wagering service provider] without concerted fraud'.[39]

4.43 The RWA did not support further changes to the time period. It noted that under the current arrangements, even if a minor managed to access an account, the account would be closed and any funds deposited would have to be returned after the 14 day period, because they would not be able to verify the account.[40]

---

[35] Responsible Gambling Fund, *Submission 173*, p. 2.

[36] Alliance for Gambling Reform, *Submission 179*, p. 1.

[37] Alliance for Gambling Reform, *Submission 179*, p. 2.

[38] Responsible Wagering Australia, *Submission 174*, p. 1.

[39] Responsible Wagering Australia, *Submission 174*, p. 1.

[40] Responsible Wagering Australia, *Submission 174*, p. 2.

4.44 Instead, the RWA called for the existing identify verification requirements for online wagering to be extended to Electronic Betting Terminals (EBTs) in retail venues. According to the RWA, EBTs provide the 'single greatest opportunity for a minor to gamble in Australia':

> These devices are essentially completely unmonitored and do not require any verification of age prior to a bet being placed…there is very little stopping a minor from walking into a retail venue with cash and gambling at an EBT.[41]

Unintended consequences

4.45 In its submission, the RWA outlined a number of unintended consequences that may follow further changes to customer verification requirements. Specifically it submitted that 'reducing the age verification period beyond what current technology and processes can effectively support' would:

- lead to a higher percentage of prospective customers failing to pass the verification process and having their accounts closed because they cannot have their identify verified in time;
- create a significant 'push factor' where Australians will opt for anonymous cash-based wagering; and
- drive otherwise law-abiding citizens to illegal off-shore operators.[42]

4.46 The Department of Social Services noted that concerns about the same unintended consequences had been raised by stakeholders during the National Framework consultation process. In addition, stakeholders raised concern about 'possible significant commercial impacts' on licensed online wagering operators.[43]

4.47 While acknowledging the potential for unintended consequences of reducing the customer verification period, the Department of Social Services highlighted measures already taken to mitigate these potential outcomes. For example, the Department noted 'a withdrawal of prominent offshore operators from Australia and [that] statistics point to a downward trend in offshore gambling expenditure' as a result of targeting by the Australian Communications and Media Authority.[44] Furthermore, the Department relayed that most of the large online wagering providers confirmed they had

---

[41] Responsible Wagering Australia, *Submission 174,* p. 2.

[42] Responsible Wagering Australia, *Submission 174,* p. 4.

[43] Department of Social Services, *Submission 163,* p. 5.

[44] Department of Social Services, *Submission 163,* p. 5.

already implemented a reduced verification timeframe ahead of the expected change to the Rules.[45]

Cost of changing the timeframe

4.48 The Government has estimated that reducing the customer verification timeframe will cost the online wagering industry approximately $900,000 annually or $9 million over 10 years.[46] These costs relate to the need to reconfigure internal systems to accommodate the reduced time frame.[47]

4.49 The Department of Social Services also identified three further possible regulatory impacts of reducing the customer verification timeframe (to a period between 72 hours and 14 days). These include:

- smaller online wagering operators may be competitively disadvantaged by lacking the technological capability to complete the verification process in a shorter time period;
- online wagering providers may require greater access to government systems and databases to verify documents more quickly; and
- additional subscription costs may be incurred to access third party verification systems.[48]

Other changes

4.50 In its evidence, the Department of Social Services told the Committee that customer verification 'cannot possibly stop all young people gambling online', particularly where fraud is involved. Rather, it must be part of a range of strategies. In particular, Deputy Secretary, Ms Elizabeth Hefren-Webb stated:

> Customer verification needs to be part of a multifaceted approach that encompasses further education of children and parents sitting alongside other

[45] Department of Social Services, *Submission 163*, p. 5.

[46] Department of Social Services, *Submission 163*, p. 5. See also: *A National Consumer Protection Framework for online wagering in Australia – Decision Regulation Impact Statement*, pp. 129-131, <https://ris.pmc.gov.au/2018/11/30/national-consumer-protection-framework-online-wagering-australia>.

[47] Department of Social Services, *Submission 163*, p. 5.

[48] Department of Social Services, *Submission 163*, p. 6.

government policies recently implemented, such as restrictions on advertising during children's viewing hours.[49]

4.51 The Alliance for Gambling Reform made a similar point, noting that age verification 'is not the only safeguard to protecting children online'. The Alliance highlighted the role of some parents and guardians in providing access for their children to gambling, and suggested greater education and further research into this issue. In particular, it suggested that further research be conducted into the extent to which children are circumventing age verification, and how this is occurring.[50]

4.52 Other suggestions put to the Committee for minimising the risks of children and young people engaging in online gambling included:

- requiring licensed online gambling businesses to register a customer in person at a physical location or by live webcam in Australia;[51]
- applying age and identity verification to all types of interactive wagering including telephone betting;[52] and
- introducing tighter restrictions and warnings on video games that include micro-transactions (such as 'loot boxes' and 'skins').[53]

4.53 The RGF suggested that the Committee consider whether a reliance on online verification actually increases the risk of young people gaining access to gambling services. In this respect the RGF noted some concern over young people using another person's identification to obtain verification online through third party providers, rather than being verified by the wagering provider in person. The RGF suggested that consideration be given to alternate verification processes.[54]

---

[49] Ms Elizabeth Hefren-Webb, Deputy Secretary, Families, Department of Social Services, *Committee Hansard*, Canberra, 6 December 2019, p. 2.

[50] Alliance for Gambling Reform, *Submission 179,* p. 2.

[51] Synod of Victoria and Tasmania Uniting Church, *Submission 183,* p. 5.

[52] Australian Institute of Family Studies, *Submission 166*, Appendix 1.

[53] Australian Institute of Family Studies, *Submission 166*, Appendix 1.

[54] Responsible Gambling Fund Trust, *Submission 173,* pp. 2-3.

Committee comment

4.54 The clear and consistent message received by the Committee is that strong identity and age verification processes are necessary to prevent young people potentially developing problem gambling behaviours and addiction.

4.55 The Committee recognises the distinction between young people who gain access to online gambling sites because their age is not screened and/or verified, and young people who gain access to online gambling sites because they have engaged in fraud and are purporting to be someone else. Age verification processes are unlikely to deter the latter.

4.56 As discussed in Chapter 2, the Committee is confident that technological advances are able to support quicker and more robust verification processes to provide a balance between allowing legitimate online customers to engage in legal wagering activities, and protecting children and young people from the potential harm associated with these activities.

4.57 The Committee notes that the National Consumer Protection Framework for Online Wagering is currently under review with a view to reducing the timeframe for customers' identity verification from 14 days to 72 hours.

4.58 While the Committee would support such a stricter requirement for a customer's *identity* to be verified prior to them opening an online wagering account, at a minimum the Committee recommends that a customer's *age* must be verified prior to engaging in online wagering.

4.59 Consistent with the Committee's view in relation to online pornography, the Committee considers that it is reasonable to expect that customers wishing to open an online wagering account be required to verify that they are 18 years or over, and that this happen before they can engage in online wagering.

Recommendation 4

4.60 The Committee recommends that the Australian Government, through the National Consumer Protection Framework for Online Wagering, introduce a requirement that customers are not able to use an online wagering service prior to verification of their age as 18 years or over.

4.61 The Committee notes the potential for duplication in having different age- and identity verification systems and/or timeframes, but leaves this as a matter for the Government to consider as part of the review.

4.62 While gaming is not captured by the definition of wagering under the *Interactive Gambling Act 2001* and was therefore outside the scope of the inquiry, in the course of the inquiry it came to the Committee's attention that there is concern in the community about children and young people being exposed to simulated gambling through 'loot boxes' in video games.

4.63 The Committee shares this concern, and notes the potential for loot boxes to act as a gateway to problem gambling and associated harms later in life.

4.64 Given their resemblance to gambling, the Committee considers that loot boxes and other simulated gambling elements in video games should be subject to appropriate age restrictions, including through the use of mandatory age verification.

Recommendation 5

4.65 The Committee recommends that the Office of the eSafety Commissioner or other relevant government department report to the Australian Government on options for restricting access to loot boxes and other simulated gambling elements in computer and video games to adults aged 18 years or over, including through the use of mandatory age verification.

4.66 Lastly, the Committee notes with concern evidence that indicates that young people are often exposed to online gambling by their parents or guardians. The Committee would like to see more resources made available to inform parents about the risks and harms associated with online gambling, and to assist parents to create safer online environments for their children.

Recommendation 6

4.67 The Committee recommends that the Office of the eSafety Commissioner develop educational resources to inform parents of the risks and harms associated with online gambling and assist parents to reduce children and young people's exposure to online gambling.

4.68 The Committee expects that these educational resources would also seek to raise awareness among parents of the potential for children and young people to be exposed to simulated gambling through video games.

Mr Andrew Wallace MP
Chair
25 February 2020

Labor Members' Additional Comments

1.1 Labor members of the Committee share concerns about children and young people's exposure to harmful online content and services.

1.2 We strongly support the objective of ensuring that Australians younger than 18 years should not have access to online wagering and pornography sites and acknowledge the harms that can flow if efforts are not made to prevent such access.

1.3 Labor has a strong track record when it comes to promoting online safety.

1.4 In 2008, the Labor Government delivered $125.8 million towards a cybersafety plan to combat online risks to children and help parents and educators protect children from inappropriate material and contacts while online. In 2010, the Labor Government established the Joint Select Committee on Cyber-Safety as part of its commitment to investigate and improve cyber-safety measures, releasing a report with 32 recommendations each of which was endorsed and responded to by the Labor Government.

1.5 Since 2013, Labor has supported Government eSafety and online wagering initiatives in Parliament and the Government has acknowledged the strong bipartisan support in this area. Further, Labor Senators supported the recommendations of the Senate Environment and Communications References Committee Inquiry into *harm being done to Australian children through access to pornography on the internet* (November 2016) and the Inquiry into *gaming micro-transactions for chance-based items* ('loot boxes') (November 2018).

1.6 Labor members of the Committee understand that we live in an era where many children have greater facility with technology than their parents and

carers and that a holistic, multi-faceted and layered approach to protect children online, including safety-by-design, adult supervision, technological access-prevention measures and the education of children and adults, is of ongoing necessity.

1.7 Labor members of the Committee acknowledge that there is 'no silver bullet' for addressing online harm, that no control mechanism is 100 per cent effective and that age verification should not be seen as a panacea.

1.8 We appreciate that technological measures are designed to limit children and young people's access to harmful online content but that technological interventions will never be able to completely eliminate the risk of children and young people being exposed to harmful content.

Age verification

1.9 Labor members of the Committee support the implementation of age verification technology, as well as the legislative framework that would support it, subject to further research and review. This position is consistent with that of Australia's eSafety Commissioner.

1.10 We note that in a 9 December 2019 blog, available on the website of the Office of the eSafety Commissioner, the eSafety Commissioner states that:

> eSafety has supported the implementation of age verification technology, as well as the legislative framework that would support it – **subject to further research and review**.[1] [emphasis added]

1.11 In its submission to the review, the eSafety Commissioner states that:

> Should the Australian Government wish to progress on developing and implementing age verification solutions or regulations, eSafety would advise that a review should be undertaken first.[2]

1.12 Labor members of the Committee accept that age verification requires further review, research and development in order to be implemented effectively as part of a multi-faceted and layered approach to online safety. Without adequate review and research, any new system may fail to win public trust and support and increase risks and unintended consequences

---

[1] Julie Inman-Grant, eSafety Commissioner, 'Can age verification help protect our kids from online pornography?', 9 December 2019 at <https://www.esafety.gov.au/about-us/blog/can-age-verification-help-protect-our-kids-online-pornography>.

[2] Office of the eSafety Commissioner, *Submission 191*, p. 14.

around data security, trust, privacy and freedom of expression as well as fail to provide an effective measure for online access minimisation.

1.13 We note the Office of the eSafety Commissioner submission that:

> Age verification is a nascent field, and if it is to be leveraged to protect children and young people from accessing online pornography, then we need to develop a supportive ecosystem, develop robust technical standards and requirements for this type of technology, and better understand the effectiveness and impact of age verification solutions in addressing this policy concern.[3]

and

> As highlighted in the inquiry's terms of reference, it is also vital to identify and mitigate the risks associated with the use of age verification before it is rolled out.[4]

1.14 We note the Communications Alliance submission that:

> The failure of widespread and successful age verification systems to emerge … was further underlined in mid-October 2019, when the UK Government announced that its planned age verification regime, to prevent under-18s from accessing commercially offered online pornography, would not go ahead. The Government reported that the system, which was originally scheduled to commence in July 2019, had experienced numerous technical issues relating to its implementation.[5]

and

> Translating this objective [of ensuring that Australians younger than 18 years should not have access to online wagering and pornography sites] into a robust and practicable framework that also protects the privacy and cyber security of individual users of an age verification system is, however, a complex task that must be approached carefully and methodically.[6]

1.15 Labor members of the Committee note that after years of work and millions of pounds expended on its proposal to introduce age verification for online pornography, the UK Government announced that it will not be proceeding.

---

[3] Office of the eSafety Commissioner, *Submission 191*, p. 22.

[4] Office of the eSafety Commissioner, *Submission 191*, p. 2.

[5] Communications Alliance, *Submission 189*, p. 1.

[6] Communications Alliance, *Submission 189*, p. 1.

This is a recent cautionary tale that demonstrates how complicated it is to get age verification right.

1.16 We understand that the UK government estimates that approximately £2.2m (approximately $4.15m) was spent on the proposal to introduce age verification for online pornography; that the costs for implementation (not proceeding) were estimated at £4.45m (approximately $8.38m); and that the UK government requested that HM Treasury provide indemnity of up to £10m (approximately $18.84m) to protect the British Board of Film Classification against legal challenges in its first year of operation.[7]

1.17 Labor members of the Committee acknowledge that the necessary review and research requires time, expertise and resources to properly examine the complex range of issues that age verification gives rise to, across data security, trust, privacy and freedom of expression.

1.18 We note that the necessary review and research would require adequate resourcing to be successful. Without adequate resourcing, any new system may fail to win public trust and support, fail to address the risk of unintended consequences, and fail to operate as an effective access prevention measure.

1.19 We further note that a range of relevant Government Departments and Agencies would need to be involved in the necessary review, research and policy development in order to strike the right balance between safety, security and privacy across online wagering and online pornography, including the Office of the Australian Information Commissioner, the Australian Cyber Security Centre, the Australian Signals Directorate, the Australian Communications and Media Authority (ACMA) and the eSafety Commissioner.

Loot boxes

1.20 Labor members of the Committee note that the Terms of Reference to this Inquiry do not reference "loot boxes" and that key stakeholders (such as the Interactive Games and Entertainment Association (IGEA)) have not had the opportunity to provide written submissions or oral evidence to the inquiry, or respond to evidence, in relation to loot boxes. The Committee has not had the benefit of this exchange.

[7] Office of the eSafety Commissioner, *Submission 191*, pp. 11-12.

1.21 We note that the recent Senate inquiry into loot boxes didn't recommend any further regulatory action, and that the Government's response (March 2019) did not support the inquiry's recommendation for further research or even a review of loot boxes, rather it merely noted these recommendations.

1.22 Labor members of the Committee note that any work on options to restrict access to elements of computer and video games should be done in consultation with industry and done with reference to the classification scheme. We note there is a current classification review process on foot and we consider the Department of Infrastructure, Transport, Regional Development and Communications (the Classification branch) and the ACMA (the interactive gambling team) would also be well placed to conduct work around the restriction of loot boxes, which may require regulatory impact assessment.

Conclusion

1.23 Labor members of the Committee support further research and review to inform the development of a roadmap for the implementation of age verification for online wagering and online pornography to support the efficacy of this mechanism for protecting minors.

1.24 We regard further research and review as intrinsic to Recommendation 3, which recommends the development of a roadmap setting out a suitable legislative and regulatory framework; a program of consultation with community, industry and government stakeholders; activities for awareness raising and education for the public; and recommendations for complementary measures to ensure that age verification is part of a broader, holistic approach.

1.25 Labor members of the Committee consider that, given the time needed to inform and develop work for age verification for online wagering and pornography, it is imperative that work on other initiatives to strengthen online safety is done in tandem. To that end, we thank submitters for providing suggestions for other measures and initiatives to improve online safety.

1.26 We note that the Government has the benefit of a report of an expert working group, convened by the eSafety Commissioner and participated in by industry, which remains Cabinet-in-confidence. We encourage the Government to reclassify the report and make it public, so the broad range of stakeholders supportive of online safety may have the benefit of the work.

Ms Sharon Claydon MP
Deputy Chair

Dr Mike Freelander MP
Member

Ms Peta Murphy MP
Member

A. Statement on the principles for the treatment of evidence

The House of Representatives Standing Committee on Social Policy and Legal Affairs is inquiring into age verification for online wagering and online pornography to prevent children and young people from accessing harmful products.

The Committee will consider the aspects of online wagering and online pornography detailed in the terms of reference.

The Committee acknowledges that accessing online wagering from operators licensed in Australia and online pornography from appropriately classified websites is a legal activity for people aged over 18. The focus of this inquiry is not the legitimate use of online wagering and online pornography.

Online wagering is the placing or making of bets on an external event that takes place, such as on a sports field or a racetrack, or other contingency such as novelty betting, using the internet through any interactive media including computers, mobile phones, tablets and other similar electronic devices. The Committee is not considering other forms of online betting such as lotteries, electronic gaming and casino games including poker; or illegal online gambling products, such as online casino games and online poker.

The Committee will carefully consider each of the written contributions made by members of the community. While the Committee welcomes submissions sharing personal experiences, it is very mindful of the potential issues in publishing submitters' details under these circumstances. Where there is potential for any parties to be identified (including people connected with the author), the Committee may authorise publication with identifying information removed (possibly including the name of the submitter).

Please note that the Committee may also authorise publication of submissions with images, personal details, private information, and unnecessary adverse reflections on individuals, removed.

We thank all contributors for assisting the Committee with its inquiry.

B. List of submissions

1 *Name Withheld*

2 *Name Withheld*

3 Mrs Anne Weeks

4 *Name Withheld*

5 *Confidential*

6 *Name Withheld*

7 *Name Withheld*

8 Ms Megan Knight

9 Mr Costante Conte

10 Mr Scott Berry

11 Monique Pringle

12 Miss Katie Brown

13 *Name Withheld*

14 *Confidential*

15 Mr George Rigby

16 *Name Withheld*

17 Ms Kath Ryan

18 *Name Withheld*

19 *Confidential*

20 *Name Withheld*

21 Ms Jas Rowlinson

22 Ms Joanne Cox

23 Ms Violeta Buljubasic

24 *Name Withheld*

25 *Name Withheld*

26 *Name Withheld*

27 *Name Withheld*

28 *Name Withheld*

29 Professor Rikki Watts

30 *Name Withheld*

31 *Name Withheld*

32 *Name Withheld*

33 Mr Gerald Pilon

34 *Name Withheld*

35 Ms Glynis Simpson

36 *Name Withheld*

37 Dr Dean O'Keefe

38 Mrs Samantha Bryan

39 Mrs Laura Barrie

40 Ms Sophie York

41 *Name Withheld*

42 *Name Withheld*

43 *Name Withheld*

44 Reinier Bouman

45 *Name Withheld*

46 Ms Franca Calorio

47 Ms Sarah Antoniw

48 Ms Melinda Rau-Wig

49 *Confidential*

50 Infuse Church

51 *Name Withheld*

52 *Name Withheld*

53 Miss Janet Cowden

54 *Name Withheld*

55 *Name Withheld*

56 *Name Withheld*

57 FamilyVoice Australia

58 UNSW Law Society

59 *Confidential*

60 *Name Withheld*

61 Mr Matthew Roebuck

62 *Name Withheld*

63 *Name Withheld*

64 Mrs Anne-Maree Choi

65 Eros Association

- 65.1 Supplementary to submission 65

66 Mrs Dorothy Long

67 *Name Withheld*

68 Ms Naomi Bonanno

69 Australian Christian Churches

70 Ms Angela Thomas

71 Mr Ben Bishop

72 Goombungee Assembly of God

73 Brave Foundation

74 AVSecure LLC

75 *Confidential*

76 Mr Ronald Edwards

77 *Name Withheld*

78 Mr Ian Moncrieff

79 *Name Withheld*

80 *Name Withheld*

81 *Name Withheld*

82 Mr Tim Nitschke

83 *Name Withheld*

84 *Name Withheld*

85 *Name Withheld*

86 Dr Gavin Riches

87 Dr Graham Joseph Hill

88 *Name Withheld*

89 *Name Withheld*

90 *Name Withheld*

91 Thornleigh Community Baptist Church

92 Mr Costantino Di Biase

93 Ashok and Mary Jalalabadi

94 Ms Valma Dean

95 Mrs Vickie Janson

96 *Name Withheld*

97 *Name Withheld*

98 Safe4Kids Pty Ltd

99 *Name Withheld*

100 *Name Withheld*

101 Ms Deborah Lamour

102 *Name Withheld*

103 *Name Withheld*

104 Mr Michael Janson

105 *Name Withheld*

106 *Name Withheld*

107 Ms Julie Cornish

108 Mrs Linda Ramnath

109 Ms Andrea Wilk

110 Mr Narendra Ramnath

111 *Name Withheld*

112 *Name Withheld*

113 *Name Withheld*

114 Dr James Twelves

115 *Name Withheld*

116 Dr Haydn Nelson

117 Mr Allen Yam

118 BUZ Nurture Works

119 *Name Withheld*

120 *Name Withheld*

121 *Name Withheld*

122 *Name Withheld*

123 Presbyterian Church in NSW

124 ChildSafe

125 *Name Withheld*

126 SECASA

127 Ms Rachel Fisher

128 *Name Withheld*

129 Ms Dawn Allen

130 Glasshouse Christian College

131 *Name Withheld*

132 *Name Withheld*

133 *Confidential*

134 Mr Stephen Brinton

135 Mrs Patricia McInnes

136 *Name Withheld*

137 *Name Withheld*

138 *Name Withheld*

139 *Name Withheld*

140 Real Talk International Ltd

141 Dr Kristy Goodwin

142 *Name Withheld*

143 *Name Withheld*

144 Ms Jane Munro

145 Mr Ronald Bower

146 Department of Home Affairs

147 *Name Withheld*

148 Mrs Imelda Gilmore

149 *Name Withheld*

150 Ps Arthur Shepherd

151 Mrs Shelley Cassidy

152 *Name Withheld*

153 *Name Withheld*

154 Mrs Frances Evans

155 *Name Withheld*

156 *Name Withheld*

157 *Name Withheld*

158 Newcastle Autism Treatment Services

159 Mr John Miller

160 Australian Christian Lobby

161 UK Children's Charities' Coalition on Internet Safety

162 Christian Schools Australia

163 Department of Social Services

164 The Salvation Army, Australia

165 PartnerSPEAK

166 Australian Institute of Family Studies

167 NAPCAN

168 Civic Church

169 Hillsong Church Australia

170 WA Child Safety Services

171 Dr David Sandifer

172 Yoti Australia Pty Limited

173 NSW Responsible Gambling Fund Trust

174 Responsible Wagering Australia

175 Marshall Ballantine-Jones

176 Fr Mark De Battista B.Th., S.T.B., S.S.B., S.T.L. (Bib. Theol.)

177 Melinda Tankard Reist

178 Collective Shout

179 Alliance for Gambling Reform

180 Canberra Declaration

181 Dads4Kids Fatherhood Foundation

182 Bravehearts

183 Uniting Church in Australia

184 Senator Amanda Stoker

185 Victorian Aboriginal Child Care Agency (VACCA)

186 Communications Alliance Ltd

187 British Board of Film Classification (BBFC)

188 Digital Transformation Agency

189 Equifax

190 TrustElevate

191 eSafety Commissioner

192 eChildhood

- 192.1 Supplementary to submission 192

193 *Confidential*

194 *Confidential*

195 Alcohol Programs Team, Public Health Advocacy Institute of WA, Curtin University

196 Dr Elisabeth Taylor PhD (Cantab)

197 National Alliance for Action on Alcohol

198 Foundation for Alcohol Research and Education (FARE)

199 Australia Post

200 The Age Verification Providers Association

201 219 contributions via eChildhood

202 Family Zone

203 Example of 87 identical contributions received

204 Compilation of 50 similar contributions received

205 Example of 30 identical contributions received

206 Compilation of 36 similar contributions received

207 Examples of 2236 contributions via OneClickPolitics

208 Jan Lonsdale

209 *Name Withheld*

210 Robin Kentley

211 Kylie & Rob Clarke

212 *Name Withheld*

213 Catherine Goulding

214 *Name Withheld*

215 Mr Allen Cox

216 Miss Naomi Clements

217 Mr Peter Lombard

218 Mrs Jennifer Kellaway

219 *Name Withheld*

220 *Name Withheld*

221 Annette Hill and 35 other individuals

222 Child Abuse Prevention Service

223 Mrs Patricia Anderson

224 Mrs Donna Crouch

225 Mrs Lucy Rooney and 47 other individuals

226 Owen Butt and 43 other individuals

227 Mr Graham Stitz and 45 other individuals

228 Jeremy and Rachel Hopwood and 45 other individuals

229 *Name Withheld*

230 Mr Christopher Harkness

231 Mrs Shane Hamilton

232 Mr David Senescall

233 Mr Russell Gray

234 *Name Withheld*

235 *Name Withheld*

236 *Name Withheld*

237 Dr Paul Scully

238 FamilyVoice Australia

239 Mrs Carlee Egan

240 *Name Withheld*

241 *Name Withheld*

242 Ms Joy Tekinay

243 *Name Withheld*

244 *Name Withheld*

245 Karen Dobby

246 Mrs Kay Djoeandy

247 *Name Withheld*

248 Rev Wayne Alcorn

249 *Name Withheld*

250 *Name Withheld*

251 *Name Withheld*

252 Mrs Emma Argall

253 *Name Withheld*

254 *Name Withheld*

255 *Name Withheld*

256 Mr James Browne

257 *Name Withheld*

258 Miss Leanne Schulte

259 *Name Withheld*

260 Mrs Robyn Graham

261 *Name Withheld*

262 *Name Withheld*

263 Mrs Shirley Cambitzi

264 *Name Withheld*

265 *Name Withheld*

266 *Name Withheld*

267 *Name Withheld*

268 *Name Withheld*

269 Digital Industry Group Inc (DIGI)

270 Warwick & Kathy Vincent

271 Mrs Roslyn McMillan

272 Damien Torti

273 Mr Rex Frazer

274 David Pellowe

275 John Coverdale

276 *Name Withheld*

277 *Name Withheld*

278 Caroline Minshull

279 *Name Withheld*

280 Dr Sandra Lyne

281 Mrs Astrid Pendersen

282 *Name Withheld*

283 Alan Baker

284 Rajindran Hensman

285 Luke Fletcher

286 Tom Muir

287 Mrs Irene Mary June Sultana

288 Dr Robyn Hessin

289 F McGillivray

290 Joel Delaney

291 Dorothy Stephen

292 Wayne Phillips

293 Lisa Phillips

294 Jon & Susan Kirk

295 Wendy McClenaghan

296 Don and Dawn Goldney

297 Graham John Back

298 Mrs Pat Gartlan

299 Sharline Bahr

300 Mailanel Ilao

301 Maria Birchley

302 Krystal Hadfield

303 *Name Withheld*

304 *Name Withheld*

305 *Name Withheld*

306 *Name Withheld*

307 *Name Withheld*

308 *Name Withheld*

309 *Confidential*

310 Mouy Te

311 *Name Withheld*

312 *Name Withheld*

313 *Confidential*

314 *Confidential*

315 *Name Withheld*

316 *Confidential*

317 *Confidential*

318 *Name Withheld*

319 *Name Withheld*

320 *Name Withheld*

321 *Confidential*

322 *Confidential*

323 *Name Withheld*

324 *Name Withheld*

325 40 examples of 707 similar contributions received

C. List of exhibits

1	Yoti, *Yoti age checking solutions*
2	Yoti, *White paper: Age Scan 'Powered by Yoti' – Public version*, September 2019
3	Liz Walker, *Statement*
4	eChildhood, *Kids and Pornography in Australia: Mobilising a Public Health Response*, November 2019

D. List of public hearings

Thursday, 5 December 2019 – Canberra

British Board of Film Classification

- Ms Amelia Erratt, Head of Age Verification - via Skype

Age Verification Providers Association

- Mr Iain Corby, Executive Director

TrustElevate

- Dr Rachel O'Connell, Co-founder - via teleconference
- Ms Aebha Curtis, Policy Analyst - via teleconference

Friday, 6 December 2019 – Canberra

Department of Social Services

- Ms Elizabeth Hefren-Webb, Deputy Secretary, Families
- Ms Teena Blewitt, Group Manager, Communities
- Ms Chantelle Stratford, Branch Manager, Family Safety Branch

Office of the eSafety Commissioner

- Ms Julie Inman-Grant, eSafety Commissioner
- Dr Julia Fossi, Expert Advisor
- Mr Toby Dagg, Manager, Cyber Report

Mr Alastair MacGibbon, Private capacity - via teleconference

Yoti

- Mr Robin Tombs, Chief Executive Officer - via Skype
- Mrs Julie Dawson, Director, Regulatory and Policy - via Skype
- Mr Darren Pollard, Commercial Director, Australia and New Zealand

Alliance for Gambling Reform

- Ms Margaret Quixley, Campaigns Director - via teleconference

Equifax

- Mr Matt Strassberg, General Manager, External Relations Australia and New Zealand

Digital Transformation Agency

- Mr Peter Alexander, Chief Digital Officer
- Mr Jonathon Thorpe, Head of Identity, Digital Delivery Division

UNSW Law Society

- Mr Chern Eu Kuan, Student Contributor

eChildhood

- Ms Tamara Newlands, Executive Director
- Mrs Liz Walker, Deputy Chair

Bravehearts

- Ms Carol Ronken, Director of Research - via teleconference

Collective Shout

- Ms Melinda Liszewski, Campaigns Manager

Melinda Tankard Reist, Private capacity

Australian Christian Lobby

- Mrs Wendy Francis, State and Territory Director, Spokesperson for Women and Children
- Mrs Clara Geoghegan, Research Officer