Australian Government | eSafetyCommissioner

Inquiry into age verification for online wagering and online pornography

Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs

November 2019

About eSafety

The eSafety Commissioner (eSafety) is as an independent statutory office established under the *Enhancing Online Safety Act 2015*. A key function under the Act is to promote online safety for Australians. It does this through a combination of both its prevention and regulatory work. eSafety has a strong suite of regulatory powers to facilitate the rapid removal of harmful content online. It currently operates three regulatory schemes which cover Cyberbullying, Image-Based Abuse and Offensive and Illegal Online Content. The Commissioner has also been empowered to issue notices to content and hosting services being used for abhorrent violent material. Further the Commissioner can formally direct Australian Internet Service Providers to block harmful content that promotes, incites or instructs in terrorists acts or violent crimes.

The eSafety Commissioner's prevention work focuses on education, research and awareness raising. This includes leading and coordinating online safety efforts across Commonwealth agencies to help safeguard Australians at risk from online harms and to promote safer, more positive online experiences.

Our submission

eSafety welcomes the opportunity to provide a submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs' inquiry (inquiry) into age verification for online wagering and online pornography.

eSafety's remit does not extend to online wagering, which is regulated by the Australian Communications and Media Authority.[1] Accordingly, we will offer only limited comments on this aspect of the inquiry. Our submission will instead focus on age verification for the purpose of limiting children's exposure to online pornography, the regulation of which falls within our mandate through the Online Content Scheme.

In addition to the Online Content Scheme, this submission will discuss age verification technologies, prerequisites for their application, and implementation in other countries; other multi-faceted initiatives to prevent and address harm caused by children's exposure to pornography; and our Safety by Design framework.

While eSafety has a leadership role in online safety, we also recognise the work of other regulatory bodies who contribute to keeping Australians safe online. We therefore encourage the Committee to consult closely with these relevant agencies[2], and draw upon on the work carried out internationally relating to the development of age verification standards, especially in the United Kingdom.

Lastly, eSafety notes that the nature of the harm and the regulatory interventions required to deal with child sexual abuse material are different to those required for dealing with online pornography. While reiterating how abhorrent child sexual abuse material is in all forms, eSafety notes that this submission is focused on limiting harm to children through their exposure to pornography.

Introduction

eSafety has an extensive research program to ensure its programs and resources are evidence based. This equips eSafety with the insights and knowledge needed to understand the nature of online safety issues and design, implement and evaluate best possible solutions. Research conducted in 2018 with over 3,500 parents of children aged 2-17, found that one third of parents and carers reported that they were concerned about their children accessing or being exposed to pornography.[3] Research conducted by the New Zealand Classification Office confirms that children and young people themselves are troubled by what they see in pornography.[4]

We share this concern, as there is evidence[5] to suggest that exposure to pornography can negatively impact a young person's mental health and wellbeing; [6] their knowledge, attitudes, beliefs and expectations about sex and gender; [7] and their involvement in risky or harmful sexual practices or behaviours.[8]

The effectiveness of age verification as a mechanism for preventing and addressing these risks and harms depends on a wide variety of technical, legal, policy and cultural factors that this submission will explore in more detail.

It is imperative to note, however, that while technological capabilities are emerging and continue to advance, there is no "out of the box technology solutions", therefore age verification should not be seen as a panacea. Technical interventions will never be able to completely eliminate the risk of children being exposed to online pornography, and it will certainly not prepare children to interpret and understand online pornography once they reach adulthood. eSafety considers that risk and harms will more effectively be minimised through a combination and layering of technological solutions and other responses which includes education.

Regulatory approach and activities

eSafety adopts a whole of community and multifaceted regulatory approach, which draws upon social, cultural, technological and regulatory initiatives and interventions.

Similarly, it is crucial to ensure that any technological measures aimed at protecting children form part of a multifaceted approach that includes education, guidance and support for parents, carers and others who work with children—as well as for children and young people themselves. Sadly, we know it is not a matter of *if* our children will come across online pornography or sexually explicit material (whether voluntarily or involuntarily), it is a matter of *when*, so we need to ensure that we are bolstering the digital resilience and critical reasoning skills of our children to better protect them from this inevitability. The skills we empower children to learn should form part of an inclusive and strengths-based approach, in which children's diversity, strengths and resilience are understood as important factors that can be leveraged and used to help them better navigate digital environments.

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. Accordingly, eSafety supports an approach that builds in privacy, security and safety imperatives at the front-end of development and implementation.

Key to this is eSafety's Safety by Design initiative, which takes a proactive approach to online harm minimisation, rather than focussing on any one type of threat. This approach promotes industry taking active measures to prevent and address all forms of harm to children—from exposure to harmful content such as pornography or abhorrent violent material, to experiences of harmful conduct such as sexual exploitation, cyberbullying or image-based abuse.

Modernising the Australian Online Safety Framework

Work is underway to modernise Australia's existing online safety legislation and the Government is committed to introducing a new fit-for-purpose Online Safety Act.

The establishment and strong support for eSafety reflects the Australian Government's significant commitment to protecting Australians online. eSafety is world-leading and remains the only regulatory agency of its kind in the world to date, and we know that other countries are looking to our model as they develop their own regulatory bodies.

eSafety is acutely aware that more needs to be done to assist children and young people to navigate the particular issues and risks which can cause them harm or prevent them from experiencing the full benefits of digital technology. The digital environment poses new and broad ranging challenges and we have an important role to play in: protecting children and young; driving up standards of user safety within the technology community; raising awareness and the capacity of the community to deal with risks; and putting in place safety nets to minimise harm when risks are realised.

eSafety has extensive experience on the topic of online pornography, given its work in removing illegal and harmful material online, its close collaboration with industry on its Safety by Design initiative, its involvement in the family friendly filter scheme, and the significant work that was carried out in 2017 following the Senate References Committee on Environments and Communications report into harms being done to Australian children through access to pornography on the internet. eSafety convened an expert committee (at the request of government at the time), and submitted a report for consideration., eSafety would like to draw the Committee's attention to this body of work as we consider the assessment and findings remain relevant.

Given eSafety's experience to date, we are well-placed to play a key role in the development of any solutions relating to online pornography. We note however that any solution to develop and implement an age verification system for online pornography would require adequate resourcing to be successful. See for example the costs incurred by the UK Government to date on this issue.

Online Content Scheme

eSafety administers Schedules 5 and 7 of the *Broadcasting Services Act 1992* (Cth) ('BSA') and covers prohibited content accessed through the internet, mobile phones, content services, and livestreaming. This Online Content Scheme is underpinned by the National Classification Scheme,[9] and aims to protect consumers, particularly children, from exposure to unsuitable or offensive material.[10]

The legislative scheme does not expressly use the term 'pornography', but rather refers to 'prohibited content' and 'potential prohibited content'.[11] Under schedule 7 of the BSA, this includes content that has been, or is likely to be, classified under the National Classification Code for films as:

- RC (refused classification): This includes films that depict, express or otherwise deal with matters of sex, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that they should not be classified.

- X18+: This includes films (except RC films) that contain real depictions of actual sexual activity between consenting adults in which there is no violence, sexual violence, sexualised violence, coercion, sexually assaultive language, or fetishes or depictions which purposefully demean anyone involved in that activity for the enjoyment of viewers, in a way that is likely to cause offence to a reasonable adult and are unsuitable for a minor to see.

- R18+ (where it is not subject to a restricted access system[12]): This includes films (except RC films and X 18+ films and R 18+ films) that are unsuitable for a minor to see.

Under the Online Content Scheme, eSafety has the power to investigate complaints and take action with regard to material found to be prohibited or potentially prohibited, depending on where the content is hosted.

Where prohibited content is hosted in Australia, the eSafety Commissioner has the power to issue take-down notices.[13] Given the scarcity of Australian-hosted content and the high levels of compliance among those operating in Australia, only 12 take-down notices have been issued to Australian content hosts, and that was in the 2015-16 financial year.[14]

Where prohibited content is hosted overseas,[15] eSafety notifies the content to the suppliers of approved device-level filters under the Family Friendly Filter scheme, so that access to the content is blocked for consumers who use these filters. eSafety also refers sufficiently serious content to law enforcement for investigation.[16] However, eSafety lacks the authority to issue notices to overseas content hosts unless the content falls within one of our other statutory schemes, such as image-based abuse[17] or abhorrent violent material.[18]

The Office prioritises complaints under the scheme that concern child sexual abuse material that is hosted overseas. Despite the jurisdictional limitations, eSafety is able to facilitate swift removal of this material through our membership with the International Association of Internet Hotlines (INHOPE).

Age Verification

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.

It is important to note that age verification is markedly different to identity verification, and that there are also differences between assessing age and verifying it.

This section of eSafety's submission examines international developments and lessons relating to age verification and the importance of having the right digital ecosystem that takes a proportionate and harms minimisation approach.

Preconditions for a digital ecosystem that can support effective age verification

To implement age verification or assurance successfully requires a robust digital ecosystem and infrastructure in which these solutions are housed. The following is a non-exhaustive list based on research on the extensive literature and work undertaken in both the UK and the EU on age verification to date. We have focused on the main preconditions of implementing a mandatory age verification scheme for online pornography, considered to be good or best practice:

- the need for a legislative and policy structure that carefully balances the fundamental rights of all citizens including privacy, security and safety of citizens online, and that expressly addresses requirements of legality, proportionality and necessity
- 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
- the establishment of processes and procedures to test, monitor, audit and provide oversight on age verification technical solutions and tools – including an assessment and determination as to the need for accreditation or certification schemes
- 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
- ongoing research and evaluation, to determine the perceived and actual effectiveness of age verification and to assess impact in terms of harm minimisation
- awareness raising and education for the public, in terms of the planned approach, safeguards and rationale for implementation, as well as full transparency and explicability of technical tools and age verification or assurance measures that explicitly address privacy, security and safety concerns
- clarity over the roles and responsibilities of all players in the internet ecosystem in relation to the administration, implementation and interoperability of age verification tools and measures
- measures or systems to allow the general public and industry to make reports, complaints and appeals

We would like to point the Committee to the work that has been carried out in the UK, as many of the above considerations have been addressed by the British Board of Film Classification (please see pages 10-11 for

more information). eSafety has been actively engaging with the BBFC for the past two years and they have indicated a continued willingness to discuss their work with the Australian government in more depth.

Additionally, there is a tranche of work being undertaken in the United States and other jurisdictions on age verification more broadly. It would be important to liaise with these other jurisdictions to ensure harmonisation, consistency and amplification of efforts.

Tools and methods

A brief overview of a range of age verification tools and methods, which are currently used to protect children and young people from exposure to online pornography and other content, is provided below.

Age screening

Age screening is a tool used by many social media services to ascertain whether an individual is eligible to access their services. Many services simply require users to self-declare their age either manually, through the use of a drop-down menu, or via a check/tick box. This tends to occur at point of registration or access. In order to prevent circumnavigation, some sites use session cookies or other such tracking tools in order to prevent users from being able to immediately go back and change the date of birth to gain access.

Age gating

Age gating is a specific feature that allows online services and providers to restrict access to content so that only people over the legal age, or who are within the age-range attributed as being appropriate to view the content, are allowed access or can view the content. In its basic form, age gating requires end users to simply enter their date of birth at point of access or point of registration. This ultimately relies on an honour system that assumes the end user is entering a truthful birthdate, and as such can easily be circumvented.

Whilst initially used to restrict advertising content, age gating is also applied to content that has been classified (i.e. films and games), and to user-generated content which is age-tagged on upload by users, by service/provider themselves, or utilising meta-tags (such as the restricted to adults label[19], as standardised by the Association of Sites Advocating Child Protection (ASACP)). The potential limitation with this form of labelling is that they are reliant upon end users (either general public or pornographic sites) to label their content accurately, to actually utilise the labelling or tagging scheme, and for filters to be activated on devices or on the platform/website itself.

Age gating can simply restrict access to the content, providing users with an error message or re-directing them to more age-appropriate content. Alternatively, content can be locked for access and only released once a PIN code[20] or other type of age verification process has taken place.

Third party verification

With regards to online wagering and “Know your Customer” (KYC) requirements, online wagering providers in Australia are required to collect and disclose customers full name, current residential address and date of birth when using electronic verification services for identity verification and validation. As such, 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.

Assessments are often made across a range of data sources or databases[21], and a variety of personal information can be collected (which are outlined in the privacy policies of these companies).

In relation to verification ***solely on age attributes***, the following third-party verification models exist:

- Age identity providers who verify age attributes and issue a reusable physical ID card, token, voucher code or app
- Age checking providers who verify age attributes on request on a transaction-by-transaction basis (usually under a pre-arranged contractual basis with the third party)
- Age verification providers who use consumer information databases and multiple data elements to determine the age of an individual
- Third-party exchange providers who provide an online gateway for age check providers to access verified age and identity attributes
- Age estimation providers that estimate the age of an individual based on their image, most often utilising liveness tests – whose biometric details are stored for live re-authentication purposes
    - Some systems[22] offer the capability to combine age estimation with identity attributes (such as a government issued ID) in order to create a secure digital ID.
        - This technology is advancing at pace, but given current accuracy rates, these systems would have to combined with identity attributes for cases which require full verification compliance
- Age check certification schemes that provide third-party independent audits, assessments and validation services to age identity, age checking and exchange providers

Most of the systems above will indicate to the third party (i.e. pornography website) that the user is over 18, and will not disclose any further information about the person at all. Hence, it is simply the age attribute (i.e. over 18) that is exchanged. The importance of third-party providers in this regard is essential.

Of note, many third-party verification providers use one of more of the models above in their solutions – with a graded approach from age assurances to full age verification, requiring different forms, types and grade of evidence to ascertain the age and/or identity of the individual in question.

Age prediction

Age prediction based on extractable biological, behavioural or physiological characteristics that are embedded in individuals biometric data, is a growing field. Two models currently exist: unimodal biometric systems that utilise a single biometric feature for identity authentication, and multi-modal biometric systems that combine two or more biometric features for authentication purposes. Whilst these systems are currently developing for identity verification and authentication purposes, there is growing research into their use for age prediction (particularly for jurisdictions where identity documentation is rare or non-existent).

Behavioural and online signals

Advances in artificial intelligence and machine learning are enabling platforms and services to identify users via 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.

National identity systems

Many international jurisdictions have designated electronic identification systems in place, whose purposes for age verification purposes are either in use, or being explored.

Age verification in Australia to date

Following the release of the Internet Technical Task Force's Report[23] on age verification and other online child safety technologies in 2008, Microsoft attempted to initiate the first-ever age verification pilot in Australia. This effort was driven by the current eSafety Commissioner, who at the time was APAC Regional Director of Safety, Privacy and Security at Microsoft.

However, the digital ecosystem for third-party verification and in-person proofing was not sufficiently evolved at that stage to proceed with the pilot. Australia currently does implement a range of age verification and restriction tools for physical products and online wagering.

In Australia, the sale of age restricted products, such as knives and alcohol are regulated by both federal and state/territory laws. Most jurisdictions require a form of 18+ identification to be provided by an individual at point of purchase in stores, and at the delivery address if bought online. Age verification requirements often reside with the online sales provider, using relatively weak age gating requirements such as entering a valid date of birth into an age calculating tool at the point of purchase.

In relation to online wagering and gambling, the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* requires licensed wagering operators to verify the identity of every customer who opens a wagering account. This means wagering operators need to verify customers full legal name, date of birth and current residential address within 14 days of depositing funds. This verification process relies upon the wagering operator collecting and disclosing identification details to a range of electronic verification services (E-IDV), who match these details against records held in various government and non-government databases, such as but not limited to:

- Driver licence;
- Passport;
- Australian Electoral Roll;
- Tenancy Roll;
- White Pages;

- ASIC; and
- Credit history records (noting this is not a credit check).

Many of the Australian wagering operators are currently using services that utilise multi- and hybrid verification processes that utilise document scanning, biometric capture, document upload, manual data entries, fraud detection and data matching to verify identities so as to meet legislative requirements globally. We understand that the online wagering community, in anticipation of the requirements as set out in the UK's Digital Economy Act 2017 being picked up in other jurisdictions, have been working to apply, develop and utilise tools that meet those standards.

Technical age verification tools currently relied on by many licensed wagering operators in Australia include Equifax IDMatrix[24] and Illion (formerly known as Dun & Bradstreet)[25] which collect and verify an individual's age through third-party data verification. greenID by Vixverify uses more robust and advanced technology in verifying the age of individuals. 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.[26]These tools look promising and we point the Committee to these solutions.

In addition, Australia is currently developing a digital identity ecosystem, under the Digital Transformation Agency. This is for the purposes of providing Australians with single and secure way to use government services online, removing the need for the public to have to verify who they are in person at a government office. The scheme is completely voluntary. The ecosystem and infrastructure that has been developed includes an accredited service provider (myGovId), multiple identity service providers[27], an Australian Government accredited identity exchange, attribute verification services, Govt digital services[28] and finally attribute service providers. Whilst identity verification is very different to age verification, we would point the Committee to this programme of work – both in terms of the ecosystem that has been built for this specific project, but also to ascertain the effectiveness of solutions that exist (from a data protection, privacy, safety and security perspective), as well as from a public acceptability viewpoint.

Age verification in the United Kingdom

A variety of positions and actions are being undertaken in different jurisdictions: from blocking all access to pornographic content for all citizens; enforcing real-name identification and age verification to access platforms and services; and mandating that age verification provisions are in place on all commercial pornographic sites.

An overview of steps taken in different jurisdictions in relation to age verification for the purposes of protecting access for minors is provided in appendix A to this report.

Given the recent decision by the UK government for age verification to be subsumed within their wider online harms regulatory framework, it will be important to fully understand the rationale and reasons for this alternative approach. eSafety is aware that there is an age verification taskforce that has been established by the UK government, and as such, collaborating with both the UK and other jurisdictions that are taking a similar

approach will be essential moving forward so that we can learn from each other. Given the global nature of the digital environment, interoperability and consistency across jurisdictions is also a key consideration when considering age verification solutions.

Digital Economy Act 2017

On 27th April 2017, the *Digital Economy Act 2017* (UK) (the DEA) received Royal Assent, putting in place provisions to prevent under 18s accessing online pornography[29]. Under the DEA, all online commercial[30] pornography services, accessible from the UK, would be required to have in place age-verification provisions to prevent children from accessing content that is not appropriate for them. In addition, the DEA also provided powers to ensure that extreme pornographic content[31] is not made available to people in the UK.

The UK government appointed the British Board of Film Classification ('BBFC') as the Age-verification Regulator, who under the DEA were provided with a range of powers to ensure compliance. These include requesting ancillary service providers[32] to withdraw services such as advertising, asking payment service providers to withdraw services, and requiring internet service providers and mobile network operators to block access to the non-compliant service.

In addition, the DEA requires that the online age regulator publish 'guidance about the types of arrangements for making pornographic material available that the regulator will treat as complying with section 14(1).' As such, the BBFC have developed a set of criteria[33] that they would use to assess whether the requirements of the DEA had been met by age verification solutions, including information about adherence to data protection legislation. The guidance makes clear that a principle-based approach would be undertaken when assessing age-verification arrangements and given the evolving and fast changing technology in the space – that the guidance and criteria would be updated accordingly.

The BBFC, alongside the Information Commissioners Office, have also produced a voluntary, non-statutory certification scheme for age verification solutions. This scheme incorporates a third-party assessment of the data security standards within solutions. To date, only one provider has received certification, though eSafety have been informed that a number of solutions are being assessed. The guidance also outlines a non-exhaustive list of issues that the ICO consider as raising data protection concerns[34], as well as cryptographic policies, penetration testing methodologies, domain and control requirements, access controls, operational security procedures, software lifecycle guidelines, vulnerability and incident management policies and third-party data processing policies.

Additionally, in accordance with the Secretary of State's Guidance to the Regulator, a memorandum of understanding has been developed between the BBFC and the Information Commissioner's Office, to allow any concerns arising over non-compliance with data protection legislation to be referred and investigated as appropriate. It is important to note, that under the General Data Protection Regulations (GDPR), age-verification solutions and online pornography providers processing personal data, have a general obligation to follow the ICO's guidance on data protection and specifically data minimisation, security and data protection by design and default. More details on the provisions under the GDPR are outlined in a separate section below.

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. We note however that, social media and search engines were captured, but only as 'ancillary service providers' in the DEA. By being ancillary services, the BBFC could make requests to these services that they withdraw services, such as advertising, from non-compliant commercial pornographic services.

However, it is understood that this potential gap in the legislation could have been addressed via the legislated requirement for a report on the impact and effectiveness of the regulatory framework to be made to the Secretary of State following 18 months of implementation. The BBFC had therefore established a robust research programme to determine the impact that the DEA had on access to pornography for young people, where young people were still able to access online pornography, what (if any) evasion strategies were being utilised.

On 16th October 2019, the Secretary of State announced that it would not be commencing Part 3 of the DEA concerning age verification for online pornography. Instead, the age verification objectives would be delivered through the proposed online harms regulatory regime. According to the official statement made by the UK government, this was to ensure that a coherent approach to online harms was achieved. Addressing age verification in the online harms regulatory regime would also allow the government to revisit the definitions of pornographic material and services covered in future legislation, as both of these areas were raised as concerns during the tabling of the DEA.

In relation to concerns over the definitions used in the DEA, the use of 'extreme pornography' as defined under section 63 of the *Criminal Justice and Immigration Act 2008* (UK) was raised during debates, given that simulated (animated and computer generated) forms of child sexual abuse is not captured under this definition. As such, certain simulations of child sexual abuse that feature on online pornographic sites would fall out of scope of the new Regulator, creating an imbalance between how pornographic content is classified and restricted in the online context versus the offline. This type of material would therefore still be accessible to both adults and children online, on age-verified sites as well as smaller and unregulated platforms. At the time, the UK Government did make a commitment to debate the definitions used in the DEA, and made assurances that a consultation would take place in the future.

The other major concern in relation to the DEA centred on concerns relating to privacy and specifically data sharing safeguards. 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.

The UK government has made clear that they expect age-verification tools to continue to play a key role in protecting children online, alongside other developments in online safety technologies.

The UK government estimates that approximately 2.2m GBP (roughly $4.15m) have been spent to date on the proposal to introduce Part 3 of the DEA. This figure is substantially less than the anticipated costs for implementation, which the Regulatory Policy Committee estimated at 4.45m GBP (approx. $8.38m). In

addition, the UK government requested that the HM Treasury to provide indemnity of up to 10m GBP (approx. $18.84m) to the BBFC, to protect it against legal challenges in its first year of operation.

The Data Protection Act 2018 (UK)

Under the *Data Protection Act 2018* (UK), the Information Commissioner (ICO) was directed to prepare a code of practice and appropriate guidance on standards of age-appropriate design of relevant information society services which are likely to be assessed by children. Of note, section 123 of the DPA stipulates that the code would not only apply to services aimed specifically at children but also to services that aren't specifically aimed or targeted at children, but are nonetheless likely to be used by under-18s.

The ICO published its draft Code for consultation in May 2019, and the consultation process closed in May 2019. The finalised Code is expected to be laid before Parliament for approval by 23 November 2019. In the draft code, the ICO made clear that services should apply the standards as set out in the code to all users, unless robust age-verification mechanisms or age-checks were in place to distinguish children from adults.

The code states that asking users to self-declare their age or age-range does not in itself amount to a robust age-verification mechanism, and that users should be given a choice over the use of age verification where possible. The code states that services need to comply with data protection obligations in relation to the retention and collection of data, including data minimisation, purpose limitation, storage limitation and security obligations. Consideration for the use of third-party age-verification services are also highlighted.

The Commissioner makes clear that she will support work to establish clear industry standards and certification schemes for age verification mechanisms in order to assist the public to identify robust systems that comply with data protection standards.

The benefits of age appropriate design by default is stated as recognising that 'some children do not have access to identity documents and may have limited parental support, making it difficult for them to access age-verified services at all, even if they are age-appropriate.'

European Legislation

The UK, as current members of the European Union, are obligated to pay heed to EU legislation.

General Data Protection Regulation

Under the General Data Protection Regulations (GDPR) age-verification solutions and online pornography providers have a general obligation to comply with the following key and important requirements when processing personal data:

- age-verification systems must be designed with data protection in mind – ensuring users' privacy is protected by default
- individuals must be told why, when, where and how their personal data is being processed, and by which organisations. Where an organisation processing personal data is based outside the EU, an EU-based representative must be appointed and notified to the individual
- the need to 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. There must be an appropriate lawful basis for the processing of any personal data in line with the requirements of data protection legislation
- the need to process personal data securely in light of the associated risks presented by the processing
- the need to facilitate individuals' rights (including the rights of access, erasure and rectification)
- the need to ensure that personal data is not retained for longer than is necessary to achieve the purposes for which it was originally collected

Audiovisual Media Services Directive

Under the Audiovisual Media Services Directive (AVMSD), new legal responsibilities were created in relation to:

- the protection of minors from harmful content[35] (which may impair the physical, mental or moral development); access to which would have to be restricted, and
- the protection of the general public from incitement to violence or hatred and content constituting criminal offences (public provocation to commit terrorist offences, child pornography and racism or xenophobia).

The measures listed in the AVMSD include flagging and reporting mechanisms, age verification tools, systems to rate the content by the uploaders or users, or parental control systems, as well as clarification in the terms and conditions of the platform of a prohibition for users to share the content citizens should be protected from. In relation to online pornography, this content would be subject to the strictest measures that provide a high degree of control (such as encryption and effective parental controls).

Of note, Article 28b of the AVMSD specifically states that the personal data of minors collected or otherwise generated by video-sharing platforms in relation to operating age verification systems and parental controls systems should not be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

Of note, the country of origin principle has also been strengthened in order to protect media service providers established in one Member State from restrictions imposed by other EU Member States receiving their services. Audiovisual providers do not need to comply with rules of 28 different Member States, only with those of the country where they are established.

Finally, the Directive includes a requirement for Member States to have independent regulatory authorities for audiovisual media services that are legally distinct and functionally independent from respective governments, should exercise its powers impartially and transparently, should have its competencies and powers clearly defined in law, and have adequate resources and enforcement powers to carry out their functions effectively. These bodies are required to establish the necessary mechanisms to assess the appropriateness of the measures (including age verification tools) taken by these services.

Lessons to be learned for Australia

The opinions on age verification for access to online pornography was polarised in the UK, which the government acknowledged in the government's response to the initial consultation exercised in July 2019. 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.

Given the research and evidence provided to the UK government, and corroborated by research here in Australia[36], that young people are frequently exposed to sexual content and online pornography on social media, the fact that the UK legislation focused solely on commercial pornography providers was a grave concern for many. The fact that the UK has since incorporated its age verification into its wider online harms regulatory regime, highlights the importance of taking a broad harm-minimisation approach to addressing online safety concerns.

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.– Further agencies such as the Office of the Australian Information Commissioner and Cyber Security Centre amongst others, will likely need to play a pivotal role in the formation of any expectations or requirements in relation to age verification.

For the last few years however, the BBFC has been developing the infrastructure and ecosystem required to implement effective and robust age verification regulation for online commercial pornography services and ancillary services. In addition, the British Standards Institute and the Digital Policy Alliance have developed a code of practice for online age verification services (PAS 1296:2018), which is intended to assist providers of age restricted products and services online with a means to adopt and demonstrate best practice. Both of these standards and certification schemes should be referred to and assessed in the Australian context to determine suitability and viability.

The UK experience and the challenges faced (despite the strong investment financially by the UK government) strongly suggests the need for further research and the need to take a balanced and measured approach.

In Summary:

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 that would include the following:

- **Identifying and developing the components of a digital ecosystem to support an age verification trial.**
- **Ascertaining the current capabilities and gaps in age verification technologies in Australia and what digital verification ecosystems could be leveraged for the purposes of age verification.**
- **Developing a proportionate and harms minimisation approach to age verification to ascertain what age verification and age assurance technologies or techniques are required to ensure children and**

young people are adequately protected. Consideration should be given to the development of a risk matrix that points to potential technological solutions that balances individuals' fundamental human rights in digital environments.

- **Liaising with other jurisdictions, particularly the UK and USA, who are embarking on wider age verification debates, to ensure consistency, harmonisation and amplification of efforts.**
- **Developing measures for accountability and transparency over the security, safety and privacy of existing and any proposed systems.**

Alternative Technologies to AV

Technological interventions are an important component of a comprehensive response to protecting children and young people from online pornography. These are not limited solely to age verification technologies, and a broader multifaceted approach that provides citizens with options, tools and control is required. Risks and harms will more likely be minimised through a combination and layering of technological solutions.

Filtering

The Family Friendly Filter Scheme (FFFS) was introduced in 2005 through Internet Industry Codes of Practice for Internet and Mobile Content under Schedules 5 and 7 to the BSA. Under the FFFS, Internet Service Providers (ISPs) are required to make one or more accredited family friendly filters available to end users to install. Filters need to be tested by Enex Testlab in order to be accredited as 'family friendly'.

There are currently three certified filters available and offered to Australian families to assist them with controlling access to harmful, unwanted content. A number of ISPs are advertising the FFFS to their customers, and where major service providers are not explicitly referring to the scheme, they do provide safety information and, in some instances, provide alternative filtering tools.[37] The Communications Alliance has updated its website to promote and reflect the FFFS.

eSafety provides data about adult and explicit overseas-hosted web content to vendors of the FFFS, improving their software in the process. Australian families can inexpensively implement these filters on their home networks and devices to ensure that unwanted and inappropriate content is controlled.

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, although they need to be considered as part of a broad suite of tools. Filtering tools exist at both a network level, at a device level and within operating systems themselves.

Consumers need greater confidence in, and choice among, the tools available to promote their own and their families' online safety. While not a silver bullet, achieving high uptake of accredited device-level filters, and greater awareness of the tools and systems provided by many industry players—accompanied by eSafety's awareness-raising resources and industry's implementation of more proactive safety measures—could significantly reduce the risk of harm to children associated with inappropriate online content.

ISP blocking

There are different forms of blocking that are used by ISPs; Internet Protocol (IP) address blocking, domain name system blocking, URL blocking, and Server Name Identification (SNI) filtering.

In all of these systems, a blacklist is created of web, IP, DNS, or URL addresses (dependent on the blocking system being used) so that ISPs or internet infrastructure operators can implement blocks on their systems. Over- and under-blocking are common risks with many of these systems, and costs relating to the maintenance of blacklists and implementation costs for these systems can be prohibitive. In fact, there is a great deal of internet traffic that cannot be captured on blacklists and lists are only ever as good as the list itself.

Further filtering at the router or network level will not capture activity on mobile technologies. The steady growth of the mobile market in Australia, and the high degree of mobile usage by children and young people, highlights the importance of device-level filtering.

There is very little publicly available information on the effectiveness and accuracy of content-blocking systems. In addition, ISP blocking has a number of limitations, including but not limited to: issues of over- and under-blocking, can easily be circumvented and can suffer from problems of redundancy. The creation and maintenance of lists of sites or services (blacklists) that ISP blocking rely upon, also have severe maintenance and administrative costs for both those administering and overseeing the lists, and not all internet traffic can be captured on a blacklist.

Protective measures within operating systems

There are a number of proactive and preventative steps that online services and platforms can take to ensure that known and anticipated harms have been adequately evaluated and addressed in the design and development of their product or service. Indeed, innovations in user safety features and measures are growing at pace – particularly in relation to muting, blocking, hiding, delisting, deleting and filtering content, conduct or contact that is unwanted by end-users.

Safe search or safe mode filters are not uncommon on many platforms, with many beginning to switch these on by default. Some sites are encouraging users to tag or flag content as ‘sensitive’ or ‘explicit’ on upload, so that filters can catch user-generated content that is inappropriate for general audiences. Others are using machine learning and AI to surface and filter images and content at upload, detecting nudity or potentially sexually explicit content, and either removing these images directly, prompting users to reconsider their post, or prompting them about the rules and conditions of the site. Age-gating and interstitial warnings on adult and other forms of harmful content are also common. Finally, some platforms are also redirecting users to support services or alternative content when harmful or risky search terms are used.

The last few years has also seen an upsurge in parental control features offered by operating systems. Many of these offer parents and carers tools to control their child’s time spent on specific sites, apps or the device itself, as well as offering a wide range of content blocking and filtering options.

Safer WiFi

Organisations making Wi-Fi freely available have a responsibility to balance the safety and security of their networks, ensuring that appropriate controls are in place to protect users from accessing harmful material in unsupervised spaces. The development of best practice guidance and minimum safety standards for each of the above services could go some way to reduce potential exposure to illegal or harmful content through wi-fi offerings. This guidance could cover necessary terms and conditions for use of the service, measures that can be implemented for harm minimisation purposes, training and support for staff to handle instances of misuse, and steps to strengthen the safety of the network.

There are currently five major publicly available Wi-Fi network types in Australia[38]: Large scale networks; municipal spaces, public transport, enterprise hotspots and closed networks. eSafety has engaged with a range of these major Wi-Fi providers and have found that the majority understand the importance of risk mitigation to general audience users and employ filtering technologies.

Device Level Filtering

Device level filtering can provide some of the strongest levels of controls currently available for content filtering. In an evaluation of the efficacy of a range of control tools and technologies that was carried out in 2017[39], device level filtering solutions were found to be amongst the most effective on the market at the time. However, none of the solutions were regarded as complete content protection for families or children.

Since that time, more granular parental controls have come on the market which can be layered and interoperate with other technological solutions. eSafety believes that there would be robust demand for the offering of "Family Friendly Phones" that had smart phone capabilities and robust filtering technologies to be made more available for young people.

In Summary:

Age verification is one possible solution to address and minimise children and young people's access to online pornography. However, to effectively address the issue will require a combination and layering of technological solutions.

Educational and Other Initiatives

It is imperative that we help guide, educate and support children and young people as they navigate their digital environments. 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. Unfortunately, given the dearth of age appropriate material on such topics – and the preponderance of adult content –it is unsurprising that young people are at risk of exposure to sexually explicit content and online pornography.

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.

eSafety's functions include supporting, conducting and evaluating educational programs and research about online safety. In 2018, we published a cross-jurisdictional report in collaboration with Netsafe New Zealand and the UK Safer Internet Centre on parenting and pornography. The report found that the risk of children's

exposure was a strong concern for parents, but that only a minority of parents in Australia and New Zealand thought that their children had been exposed to pornography. Parents were relatively confident in their ability to seek out relevant information to deal with their children's potential exposure to pornography.

eSafety's research also shows this education needs to start early, with 94% of parents with pre-schoolers reporting that their child was already using the internet by the age of 4.[40] Educational resources 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 no matter when or how it is accessed, given the wide variety of circumstances in which online pornography is viewed.[41] This approach requires multi-level awareness raising and capacity building for parents and carers, educators and young people themselves.

We ensure a strong evidence base underpins our education outputs. As a result, we know that successful education interventions tend to include:

- multiple exposures to online safety, using varied platforms, such as videos, games, posters, class discussions and parent and carer engagement
- a focus on specific skills, along with opportunities to practice those skills
- early education prior to the onset of targeted behaviour, as guided by well-trained educators, and
- monitored implementation and improvement of programs through evaluation.

Globally, there is a growing awareness that comprehensive sex education is vital to improve outcomes for all students, and a number of countries have taken steps to incorporate and embed sexuality and respectful relationship education in national school curriculum, with some containing units on online pornography for older students. There is currently limited evidence of the efficacy of any one particular approach and most countries are at the early stages of implementation.

In Australia, while there are opportunities to teach young people about sex and sexuality education through the Health and Physical Education (HPE) learning area, and opportunities to discuss concepts such as consent and respect through the general capabilities, eSafety's is of the view that opportunities to teach young people about online pornography should be explicitly addressed in the curriculum.

Furthermore, where there are opportunities for learning, most are located within the elaborations of learning areas or through the general capabilities, which are not compulsory and are generally not assessed. Their teaching is therefore discretionary; it is up to teachers to incorporate the general capabilities into learning experiences where relevant. It should also be noted that the Australian Curriculum focuses on content rather than application or pedagogy, which means there are no specifications for delivery methods, timing, frequency, or intensity of pornography education. Nor does there appear to be robust training for teachers to deliver pornography education with confidence and rigour. It is the responsibility of state and territory government and non-government education authorities to determine how the curriculum is implemented, with these decisions often made at the school level. With competing curriculum priorities and a perceived lack of teacher confidence in this area, it is highly likely that online pornography education is omitted, partially covered, or

addressed only when a perceived need arises. Educators need to be appropriately supported to develop knowledge, skills, capacity and confidence to cover this content.

eSafety would like to see we need comprehensive and nationally coordinated respectful relationships and online safety education embedded in the Australian Curriculum and consistently delivered throughout a child's educational journey, that includes age appropriate education on dealing with online pornography. As a suggestion this could be based on the 'Four Rs of Online Safety' - respect, resilience, responsibility and reasoning.

In addition to materials for educators, eSafety also provides a wealth of information for parents and carers. The eSafety Parents and Carers site has a range of resources to support parents to have age-appropriate conversations with young people about pornography. It includes topics such as setting family rules, using parent controls to prevent children from accessing pornography at home, and what to do if they discover it at school or a friend's house. The resources also cover dealing with a situation in which a parent has discovered their child has found pornography online, for example, listening with an open mind, providing reassurance and how and when to seek professional help.

We also provide parents with recommendations for starting the hard to have conversations about sex and pornography with young people. The advice includes targeted suggestions for children, pre-teens and teenagers. To assist parents to open these conversations up in a non-threatening setting our resources include video content designed to open discussions of equality, safety and consent in relationships.

Details of all our programs can be found on our website.

Finally, it is important to note that a small proportion of young people are engaging in technology facilitated harmful sexual behaviours, including developmentally inappropriate use of pornography. Research in this space is somewhat limited, but attention should be paid to the support needed for young people who have developed unhealthy relationships with pornography, as well as for young people who have concerns over the impact that sexually explicit content has had on them. Educative campaigns[42] that empower and support young people to engage in positive, healthy and respectful interpersonal relationships and information awareness campaigns around pornography and its impacts, that are targeted and co-created with young people are also important steps to helping young people access advice, support and guidance.

In Summary:

Consideration on how comprehensive and nationally coordinated respectful relationships and online safety education could be embedded and delivered in the Australian Curriculum should be undertaken. eSafety believes that this should address harmful online content, including children's exposure to pornography, and be based on the 'Four Rs of Online Safety' - respect, resilience, responsibility and reasoning. In addition, further research into what constitutes effective education on the topic of online pornography, including content, pedagogy, professional learning and support for vulnerable cohorts is required. This should also include capacity building and support for educators to develop knowledge, skills, capacity and confidence to cover this content.

Safety by Design

As eSafety's research shows, children's exposure to pornography is not parents' only concern about online safety. In fact, it is ranked as the fourth highest parental concern, after exposure to inappropriate content other than pornography (such as violent content), contact with strangers and cyberbullying.[43] Children themselves tell us that their negative experiences online include unwanted contact and content, but also extend to social exclusion, threats and abuse and damage to reputation.[44] It is therefore important to consider online safety in a holistic manner, across all of the potential risks and harms, rather than addressing issues in an ad hoc manner through stove-piped requirements for industry.

eSafety recognises the need to drive-up standards of user safety within the technology community, and to encourage and secure greater consistency and standardisation of user safety considerations. To reduce risks and counter threats online, a proactive approach is critical. We recognise the importance of proactively and consciously considering user safety as a standard risk mitigation and development process, rather than retrofitting safety considerations after online harms have occurred.

In June 2018, eSafety laid out our intention to develop a Safety by Design Framework and set of Safety by Design Principles. At its core, Safety by Design (SbD) is about embedding the rights of users and user safety into the design, development and deployment of online and digital products and services. Consideration and care was taken to ensure that the SbD Principles and Framework balance an individual's right to provision, participation and protection. In addition, the clear expectations on businesses to meet human rights responsibilities to children in the online world have been reflected in the SbD Principles.

SbD places user safety considerations at the centre of product development. 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. While personal information privacy and cyber security fall outside of eSafety's remit, SbD looks to the well-established processes surrounding privacy and security, and endeavours to elevate safety as the third design pillar in the developmental process.

Following an eight-month consultation process with industry, parents and carers and children, eSafety developed a set of 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. Three overarching principles were developed:

1) **Service Provider responsibilities**: This is premised on the fact that the burden of safety should never fall solely upon the end user. Preventative steps can be taken to help ensure that known and anticipated harms have been fully evaluated in the design and provisions of an online service, and steps taken to make services less likely to facilitate, inflame or encourage illegal and inappropriate behaviours.
2) **User empowerment and autonomy**: The dignity of users is of central importance, with users' best interests a primary consideration. Human agency and autonomy can be supported, amplified and strengthened when designing services – allowing users greater control, governance and regulation

of their own experiences, particularly at times when their safety is being, or is at risk of being, compromised.

3) **Transparency and accountability**: These are hallmarks of a robust approach to safety, that provide assurances that services are operating according to their published safety objectives, as well as educating and empowering the public about steps that can be taken to address safety concerns.

In essence, the SbD Principles provide the overarching infrastructure and framework by which industry can embed safety into their services, allowing them to be better able to address and implement measures that are targeted towards specific harms, such as online pornography and sexually explicit material. It is important that the foundations for safety are built first - rather than trying to address online harms in a piecemeal, fragmented and siloed manner. eSafety has received overwhelmingly positive feedback from all stakeholders on our SbD framework, particularly in relation to the collaborative approach undertaken in their formation, but also in relation to the principled-based approach of the initiative.

Advancements in technology, machine-learning and artificial intelligence have the potential to radically transform user experiences and safety online. Innovations are occurring at pace, and eSafety believes that its SbD initiative will act as a catalyst for further innovation, whilst also embedding user empowerment and autonomy as a core business objective for those developing products, platforms or services online.

Our consultation process highlighted that the general public wants greater control over, and more transparency from, the platforms and services that they use – particularly children and young people. A powerful vision statement which lays out what children want and expect from online industries to help users navigate the online world freely and safely is provided in full in appendix A of this submission. This was generated during our consultations with young people, and clearly articulates the desire for tools and features that provide users with controls and choices in relation to what they see, and how they interact online.

Of particular relevance to this inquiry is that young people want industry to use technology to Identify and minimise exposure to threats, risks, problems or content that Is triggering, harmful or appropriate. Importantly, this is not just filtering and blocking – but also prompts or alerts that provide users with advice, support and guidance at point of need; muting or diluting features to limit the visibility of content that the user does not want to see; warnings over potential breaches or violations of community standards so that users can rectify their actions before posting or uploading content; and reward systems, commendation systems and endorsements to motivate and change behaviour directly. Also of note, is that user safety was perceived as a shared responsibility by all stakeholders who eSafety consulted, indicating that measures to address user safety can also be distributed and shared. Steps can be taken to encourage users to flag and tag content as sensitive or explicit at point of upload, so that this content can be appropriately filtered. This means that services are not solely reliant on reports or complaints in managing the content on their sites.

eSafety is currently embarking on phase 2 of the SbD initiative, creating a Framework of guidance and resources to facilitate the adoption of the Principles. Attention will specifically be paid to developing guidance for SMEs and the start-up community, as well as generating collaboration and the sharing of safety-enhancing

tools, best practices and technologies. Safety by Design can act as a catalyst for further innovation and global leadership.

In Summary:

There is a need to drive-up standards of user safety within the technology community, and to encourage and secure greater consistency and standardisation of user safety considerations by all players in the digital environment. If we truly want to reduce, and counter, the risks and threats that citizens face online, then Safety by Design should be a core business objective and whose principles are addressed and adhered to by all online services and providers.

Conclusion

Children and young people's exposure to online pornography is a concern shared by many. The negative impact that online pornography can have on a young person's mental health and wellbeing; their knowledge, attitudes, beliefs and expectations about sex and gender; and their involvement in risky or harmful sexual practices or behaviours is well documented.

Technological solutions that limit children and young people's access to online pornography is an important facet in the arsenal of solutions that can be used to better protect children and young people. Age verification is one such approach.

Whilst it still remains challenging to prove that a "child is a child" sitting behind a particular screen, there has been increased investment in the development of online age verification systems and products over the last few years. 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.

Equally, we need to leverage other technological solutions - so that we are addressing online and harms in a holistic, and multi-faceted way. So that issues and harms don't slip through any cracks, gaps or loopholes. We need to drive up standards of user safety in the technology community at large, encouraging and assisting industry to embed Safety by Design into the design, development and deployment of online services and platforms. We should encourage industry to utilise and innovate on a suite of technological measures and solutions that best address issues on their services. We should expect that all players in the digital ecosystem address children and young people's access to illegal and age-restricted products and services as part of their safety impact and risk assessments. Age checking, assurance or verification are certainly tools that can be used by industry, alongside a suite of other measures, to better protect and empower users.

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.

Appendix A

eSafety scanned the global landscape to understand the approaches other nations were taking to limit children's exposure to online pornography, and especially the consideration of age verification technologies. A summary is provided below, in alphabetical order.

Canada

A recent inquiry by the House of Commons Standing Committee on Health recently published a report on the Public Health effects of the ease of access and viewing of online violent and degrading sexually explicit material on children, women and men (June 2017).

On age verification, the report noted that the Committee had heard evidence that "child access to online violent and degrading sexually explicit images could be addressed through various technological measures". The need for meaningful age verification tools was cited, but no specific solutions or technologies were recommended or indeed, what an age verification solution could look like or how it could be implemented. The UK model was cited in some of the submissions.

Of note, the Government response did not address age verification technologies or blocking/restricting access for explicit content which is not child abuse / exploitation material.

China

The production, dissemination and sale of sexual, pornographic and obscene material online is strictly forbidden in China.

Controls on media are strict and are strengthened by regulation to enforce real-name registration, legislation that holds platforms liable for online content, laws that require internet chat service providers to verify the identities of users, and apparent orders to telecommunication firms to bar the use of VPNs. The Ministry of Industry and Information Technology, the Cyberspace Administration of China and Ministry of Culture all play a role in regulating the digital infrastructure in China.

In relation to age verification, the most high-profile example of its use in China relates to the frameworks implemented by media giant and games publisher Tencent, in response to the government and community concerns around myopia and internet addiction in children and adolescents. Tencent made it mandatory for players of its games to verify their age to log in to their services. The identification process verifies the information provided by users against government records (namely the police database), as well as cross-referencing the information against public security databases.

More recently, Tencent is trialling facial recognition technology to verify identities through camera checks, whereby biometric data is matched using a smartphone camera (noting that Tencent's games are predominately mobile games). This was in order to address gaps in the system where children were using the information of an adult (often a grandparent, older sibling/friend or a stranger who sold their information online) to register an unrestricted adult account. This technology is intended to target accounts which have been confirmed as adult, but then display behavioural characteristics of minors.

From what can be gleaned from publicly available information, Tencent's self-reporting indicates that playtime has decreased from underage users. However, Tencent have reported that underage players have attempted to use photos of sleeping relatives, and impersonated grandparents in order to remove the age-based limit.

Germany

There is a complex network of regulations in Germany with regards to protection children and young people online. These include the German Interstate Treaty on the Protection of Minors in the Media (JMStV), the German Protection of Young Persons Act (JuSchG), the German Criminal Code (StGB) and Act on Regulatory Offences (OWiG).

In relation to age verification specifically, the JMStV mandates the use of age verification solutions.[45] This legal obligation can be fulfilled in a number of ways:

- using technical means to label the content with an age bracket (the users will not normally see such age labels, but the technical label will be recorded by providers in the root directory of its server)
    - Of note, providers have the option of labelling specific subpages and sections of a website, or an entire (sub-) domain to ensure maximum availability for their content.
- using other technical measures (e.g. requesting an ID card or other age verification systems)
    - in relation to age verification systems, the following components are necessary:
        - it is necessary for the user to be reliably identified, at which point it is determined whether or not the person in question is of legal age.
            - Of note, such a determination can only be made through personal contact ("face-to-face monitoring"). Age verification by purely technical means is also conceivable if it can achieve the same level of reliability as a personal age check[46].
    - authentication at each individual usage: it must always be ensured that the content is only being accessed by the person identified as being of legal age at the first step. The risk of access data being passed on to minors should also be reduced.
- scheduling restrictions (for live streaming of content or not making material available in a media library until a certain time)

Of note, the categorising of content is not designated in a binary child/adult format but is placed under age brackets to take into consideration degrees in intensity and impact of content. This allows greater nuance in the age rating and age labelling systems utilised. However, the only product available on the German market (JusProg) has recently been refused approval[47] as it only worked on Windows PCs and not other platforms[48].

Please also note, that the Commission for the Protection of Youth in the Media (KJM) has reviewed various age verification systems, all of which are listed on their website, and have assessed them as satisfactory.

India

Currently, there is no legislative or formal obligation to verify age to prevent minors from online harms in India, but publishing and transmitting obscene material or material containing sexually explicit acts in electronic form is prohibited under the Information Technology Act 2000.

Of interest, there is a draft Personal Data Protection Bill 2018 which is due to be tabled in the winter session of 2019. As part of a suite of data protection reforms, the bill states that 'data fiduciaries will be required to incorporated appropriate mechanisms for age verification and parental consent in order to process personal data of children.' The bill does not prescribe methods of verification, nor does it identify or create a regulatory or body to certify whether the appropriate methods have been employed. It also recognises that different types of data processing require different levels of verification – hence 'appropriate'.

New Zealand

In 2018, the Office of Film and Literature Classification surveyed more than 2,000 New Zealand teenagers (aged 14-17) to better understand how and why they were viewing pornography. Of particular relevance to this submission, were questions surrounding young people's perceptions on restricting access to pornography. 71% of young people surveyed felt that access to pornography should be restricted in some way.

New Zealand have been keeping an active watching brief on developments in the UK on age verification, and have indicated that they view age verification as one option that should be considered. They have stressed the importance of keeping pace with international developments in this area and have recently indicated that they are actively considering introducing restrictions for citizens under the age of 18. Regulation was seen as providing some options for limiting access to young people who may be vulnerable, and that solutions should be developing in a collaborative way with the young people being affected.

Singapore

Singapore is introducing a National Digital Identity, based on 'mobile crypto-based identity'. This will build on the tradition of earlier of National ID systems, the National Registration Identity Card, a compulsory ID document in Singapore, has been in use since 1965. In addition, Singapore's Personal Access, a digital ID providing access to government services, has been in place since 2003.

Online or 'remote' gambling is prohibited in Singapore, except for certain operators, under the Remote Gambling Act 2014. Singapore Pools (one of two exempt operators) allows users to verify their age in person or online using the National Registration Identity Card and a video call with a Customer Service representative.[49]

South Korea

In February 2019, the Korean Communications Commission announced that the Korean Communications Standards Commission (KCSC) would enforce existing legislation relating to harmful content in the online context. This would be carried out by blocking access to gambling sites and certain pornography sites. Essentially, the KCSC creates a set of backlisted web addresses that host illegal content and compels internet infrastructure operators to block those sites by monitoring the Server Name Identification field (which is an extension of the transport layer security protocol). This is one of the first observed cases of SNI-based filtering for national level content filtering.

Given the legality and availability of VPNs and Tor browsers, this system is not completely effective. However, the Internet Engineering Task Force is moving to encrypt the SNI field, which would make this system inviable.

However, SNI-based filtering is more precise – in that it identifies specific web addresses, rather than relying on blocking an IP address or block of IP addresses, as is done with traditional DNS filtering.

South Africa

The South African Law Reform Commission (SALRC) published a discussion paper on sexual offences (pornography and children) and an accompanying draft bill in April 2019. Of particular relevance to this inquiry are areas covered in the paper concerned with improving "the regulation of pornography, including on the Internet".

One of the biggest proposed changes within the documents, is the recommendation for a new 'default setting' on any and all devices for anyone wishing to access the internet in South Africa, which would automatically block adult content. Under these proposed changes any person, device manufacturer or internet provider who does one of the following, will be guilty of a criminal offence:

- Unlawfully and intentionally provides a child with or allows a child to engage with any form of technology or device including a mobile phone, that is capable of accessing the internet, social media or other digital content, without ensuring that the default setting blocks access to child sexual abuse material or pornography;
- Uninstalls the default setting;
- Uninstalls the default setting blocking access to pornography without valid identification proving that the requester is a user over the age of 18.

Concerns have been expressed that this provision is "not only technologically determinist and impractical from an implementation point of view, but wholly neglects children's rights to information, health, expression, and freedom of association. In trying to protect children, it risks restricting children's rights in a manner that would arguably fail to meet constitutional thresholds of legitimacy and proportionality."[50]

Of interest, and to note, the South African Department of Home Affairs and the South African Banking Risk Identification Centre (SABRIC) has launched an Online Fingerprint Verification System, which will verify an individual's identity using a biometric reader, which reads fingerprints against the Home Affairs database.[51]

United States

There is very little government regulation of internet content in the United States, the classification of which is generally performed on a voluntary basis by industry due to freedom of speech protections, as afforded by the First Amendment. However, as in most other jurisdictions, internet content is not exempt from laws.

The US does not require that pornography be classified, and labelling occurs on a voluntary basis by producers. In most states, laws prohibit the sale of pornography to under 18s (and under 17s in some states).

In relation to content that is harmful to minors, online services can be penalised for using misleading domain names to deceive individuals into viewing obscene content or other harmful content[52]; and the 2001 Children's Internet Protection Act made the implementation of content filters in schools and libraries a condition of certain federal government grants.

With regards to age verification more specifically, Given that the majority of social media services are domiciled in the United States, these companies are bound by the federal Children's Online Privacy Protection Act (COPPA), which currently stipulates that services cannot collect personal information about users who are under the age of 13. Hence, the age rating of 13 for most social media platforms and services. Of note, the COPPA Rule does not require operators to ask the age of visitors, but indicates that should a service choose to screen age 'in a neutral fashion', that the service may rely on that information "even if the information is not accurate."

Given these loose requirements, many services simply require users to self-declare their age either manually, through the use of a drop-down menu, or via a check/tick box. This tends to occur at point of registration or access. In order to prevent circumnavigation, some sites use session cookies or other such tracking tools in order to prevent users from being able to immediately go back and change the date of birth to gain access. Of note, some pressure has been placed on the Federal Trade Commission to re-examine the issue of age-screening techniques and to update its guidance on this matter. The FTC has recently requested public comment on COPPA and the COPPA Rule, which includes questions on age screening.

[1] 'Regulated interactive gambling service' is defined in section 8E of the *Interactive Gambling Act 2001* (Cth). Essentially, it includes those services that are excluded from the definition of a prohibited interactive gambling service, and includes telephone betting services and online wagering services (other than those offering in-play betting).
[2] Such as the Office of the Australian Information Commissioner, the Australian Cyber Security Centre and the Australian Signals Directorate
[3] eSafety, Netsafe and Safer Internet Centre, Parenting and pornography (2018), available at: https://www.esafety.gov.au/about-us/research/digital-parenting/pornography.
[4] New Zealand Classification Office, NZ Youth and Porn (2018), available at: https://www.classificationoffice.govt.nz/news/latest-news/nzyouthandporn/.
[5] Hovarth et al, 2013; Paolucci et al, 2000; Guy, 2012; Vega and Malamuth, 2007; Kinder et al, 2010.
[6] Haggstrom-Nordin et al, 2006; Ybarra & Mitchell, 2005, Mesch, 2009
[7] Haggstrom-Nordin et al, 2010
[8] Hovarth et al, 2013; Lofgren-Martenson & Mansson, 2010
[9] http://www.classification.gov.au/About/Pages/National-Classification-Scheme.aspx
[10] Broadcasting Services Act 1992 s 3(1)(l)-(m).
[11] Broadcasting Services Act 1992 Schedule 7, cl 20-21.
[12] The minimum requirements for restricted access systems are set out in the *Restricted Access Systems Declaration 2014*. These requirements include the provision of content warnings, safety information and age gating through a declaration of the user's age.
[13] Broadcasting Services Act 1992 (Cth), Schedule 7, cl 47.
[14] ACMA eSafety Annual Report 2015-16 page 126
[15] Schedule 5 of the BSA establishes the processes for complaints about internet content hosted outside Australia.
[16] Broadcasting Services Act 1992 (Cth) Schedule 5, cl 40.
[17] Enhancing Online Safety Act 2015 Part 5A.
[18] Criminal Code Act 1995 Division 474 subdivision H.
[19] Please note that this label is only recognised by a list of 25 filtering products and services, which can be found at http://www.rtalabel.org/index.php?content=partners
[20] KPN, a Dutch telecommunications company and audiovisual distributor, has a compulsory PIN code protection for all content rated 16+ content. The PIN is provided to the subscriber by letter, and KPN can carry out age verification checks on subscribers as part of the agreement.
[21] In Australia, these databases include: Real estate agents; Utility Providers; Insurers, Loss assessors, Loss adjustors and investigators; Law courts; Credit Providers and Access Seekers; Australian Securities and Investments Commission; Australian Financial Security Authority; Telstra and other telecommunication providers; Australia Post; Australian Electoral Commission; Australian Communications and Media Authority; Market research organisations; Direct marketing companies; Government agencies (such as the Office of the Australian Information Commissioner and the Federal Department of Human Services); External Dispute Resolution schemes.
[22] Please see Yoti, who is currently the only provider to have received an Age-Verification Certificate from the BBF
[23] Berkman Center for Internet and Society, Enhancing Child Safety & Online Technologies (2008), available at: https://cyber.harvard.edu/pubrelease/isttf/.
[24] https://www.equifax.com.au/privacy as at 23 October 2019
[25] https://www.illion.com.au/privacy-policy/
[26] https://www.vixverify.com/news-resources-2/privacy_policy/#whatpersonal1 at 10 October 2019
[27] Multiple providers will provide the general public a choice of who to verify their identities with

[28] Government digital services will use the system to confirm a person's identity
[29] Part 3 of the Digital Economy Act 2017
[30] The definition of 'commercial' is defined within the Online Pornography (Commercial Basis) Regulations.
[31] Extreme pornography as defined under section 63 of the Criminal Justice and Immigration Act 2008
[32] Ancillary service providers are defined as
[33] See pages 9 to 10 of the BBFC Guidance on age verification arrangements, as published in October 2018.
[34] See pages 13-14 of the BBFC Guidance on age verification arrangements, as published in October 2018.
[35] Article 28b outlines that video-sharing platforms need to take appropriate measures to protect minors from programmes, user-generated videos and audiovisual commercial communications that may impair their physical , mental or moral development in accordance with Article 6a(1).
[36] Lewis et al study, 2018 'I see it everywhere': young Australians unintended exposure to sexual content online
[37] As these products have not been certified under the FFFS, it is unknown as to whether these filtering solutions are equivalent to those that have been through the certification process
[38] As identified by research carried out by ACMA in 2014: https://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Research-snapshots/Strong-signals-growing-use-of-public-Wi-Fi-hotspots
[39] This was a confidential internal evaluation whose results are not publicly available. Given the changes in the market, a further evaluation would be necessary to ascertain levels of effectiveness within the current market.
[40] eSafety, Digital Parenting (2018), available at: https://www.esafety.gov.au/about-us/research/digital-parenting/supervising-preschoolers-online.
[41] eSafety Parenting and pornography (2018); BBFC 2018 study published in November; Lewis et al study, 2018 'I see it everywhere': young Australians unintended exposure to sexual content online; NZ study 2018
[42] Our Watch are developing a campaign *Change the Story* that is seeking to encourage and support young people to recognise when and how pornography portrays sexism, gender discrimination, gender inequality and other norms, attitudes and behaviours that drive violence against women.
[43] eSafety, Netsafe and Safer Internet Centre, Parenting and pornography (2018), available at: https://www.esafety.gov.au/about-us/research/digital-parenting/pornography.
[44] eSafety, State of Play—Youth, Kids and Digital Dangers (2018), available at: https://www.esafety.gov.au/about-us/research/youth-digital-dangers.
[45] Under Article 4 Para. 2 Sentence 2 of the German Interstate Treaty on the Protection of Minors in the Media (JMStV), content illegal for minors (e.g. pornography) is admissible in telemedia if the provider ensures that such content is accessible only to adults
[46] Please see: German Federal Supreme Court I ZR 102/05, Kommunikation und Recht, 2008, pp. 361, 365
[47] Approval was refused by the Commission on Youth Protection in the Media (KJM) in May 2019. The KJM was delegated the responsibility for approving age labelling software by the state media authorities.
[48] https://www.die-medienanstalten.de/service/pressemitteilungen/meldung/news/kjm-stellt-fest-beurteilung-der-fsm-zur-eignung-von-jusprog-als-jugendschutzprogramm-ist-unwirksa/
[49] http://www.singaporepools.com.sg/en/faq/Pages/account-registration.html
[50] The Association for Progressive Communications Submission to South African Law Reform Commission Discussion Paper 149 on Sexual Offences: Pornography and Children https://www.apc.org/sites/default/files/SALC_30July2019_APCRIA.pdf p13 and summary submission website https://www.apc.org/en/pubs/submission-south-african-law-reform-commission-discussion-paper-149-sexual-offences-pornography as at 22 October 2019
[51] South African Government ' Banks now verify your identity online' https://www.gov.za/services/verify-identity-online as at 22 October 2019

[52] Please see U.S. Code 2252B Misleading domain names on the Internet