

# Talking points

Meeting:	Deep Dive: Digital Identity and Age Verification
Time/date:	3.30pm, Tuesday 3 August 2021 Microsoft Teams: <a href="#">Click here to join the meeting</a>
Attendees:	<p>The Hon Stuart Robert MP, Minister for Employment, Workforce, Skills, Small and Family Business</p> <ul style="list-style-type: none"><li>- [REDACTED], Chief of Staff</li><li>- [REDACTED] Senior Adviser</li><li>- [REDACTED], Adviser</li></ul> <p>Peter Alexander, A/g CEO DTA</p> <ul style="list-style-type: none"><li>- [REDACTED], Head of Digital Identity and myGov Division</li><li>- [REDACTED], Head of Digital Identity and myGov Strategy Branch</li><li>- [REDACTED], Head of Digital Identity and myGov Capability Branch</li></ul>

## AV implementation roadmap

- The AV implementation roadmap for online pornography focuses on identifying effective tech tools, public awareness and educational measures that protect children from any harms associated with exposure to pornography.
- Technological capabilities for age verification and assurance are still emerging and continue to advance.
- Technical interventions will never be able to eliminate the risk of children being exposed to online pornography and certainly won't prepare children to interpret and understand online pornography once they reach adulthood. There is no such thing as an *'out of the box technology solution'*

- We believe there is a multilayered approach to harm minimisation that needs to be taken - which includes a combination of technological solutions, education and awareness raising.
- That's why we'll also be consulting with tech companies, academics and not-for-profits to better understand what other measures exist to restrict access and how to better educate children on distinguishing healthy intimate relationships from extreme or violent sexual behaviours.
- The process for designing the implementation roadmap will also include interdepartmental meetings, so that the roadmap is informed by any other efforts that government agencies are making on age verification and mitigating children's access to age inappropriate content or activity.
- A call for evidence will be published on eSafety's website w/c 9<sup>th</sup> August, and will act as an information and evidence gathering exercise. Targeted questions will be posed to different sectors to help inform and direct our second phase on consultations which will commence in Q2 2021.
- Through our call for evidence and consultations, we hope to gain an understanding of the safest, more secure and privacy-protecting methods of restricting children's access to pornography. This will ensure that any recommended AV systems present appropriate and effective measures which receive general support from both industry and the general public.

## **AV survey**

- In May, we undertook a small-scale community survey (1,200 adults) to better understand the awareness of AV technology amongst the Australian adult community, their perceptions and experiences of AV and their views on government implementing such a system.
- Our key findings centred around the following themes:
  - General community confidence to use online technologies was greater than their confidence to remain safe while using these same systems (70% vs 61%).

- Much work still needs to be done in educating the general community and raising awareness of 'age verification' as a concept and its application in ensuring access to online pornography reflects a minimum legal age.
- The general community was very unfamiliar with 'age verification' conceptually and in practice.
  - There was approx. 70% awareness of 'identity verification' as a concept versus 51% for age verification and only 5% awareness of terms such as 'age gating'.
- There was broad support for using AV for online pornography, but this was coupled with some scepticism. The benefits of age verification were well recognised, particularly in terms of providing safeguards for children. However, almost half of respondents were ambivalent or sceptical that the government could successfully implement an AV system.
- Government systems were considered best placed to process personal information (41%), but respondents also felt people would not feel comfortable providing their personal data to any organisation for age verification purposes.
- Knowledge on the security of the system that conducting age checks and having evidence that the system actually worked were the most important factors for people supporting implementation.
- Date of birth (73%) and driving licence (62%) were nominated most frequently as appropriate personal information to provide for age verification as part of accessing online pornography.

### **eSafety's interest in DTA's pilot**

- The DTA's digital ID framework is one method of age verification that we will be exploring as a potential technological solution in our roadmap.

- We are very interested in looking at the ways that DTA's Trusted Digital Identity Framework (TDIF) could support age verification, particularly in relation to establishing minimum technical standards.
- There is alignment in our objective to provide a certified standard which tool providers should have to meet, to ensure public trust and accountability.
- We are also interested in the pilot's findings on the public's enthusiasm and uptake of the digital ID for private online activity - which we will consider from the perspective of the AV roadmap.

### General queries/questions

- I would like to know more about how the pilot will work in practice. How will the additional complexity of delivery be managed in relation to online alcohol sales?
- How will this pilot effectively indicate or measure its ability to prevent children from accessing gambling platforms or purchasing alcohol online? It's very important to be able to demonstrate how many children were prevented from using these services, compared with how many people (child or adult) did not use the service due to the AV requirement.
- What communication strategy is being planned to build public awareness and trust of the digital ID?
- What incentives are being offered to businesses to participate in the pilot (noting it may impact their online sales)?
- How do this pilot's objectives differentiate from the those of the eftpos/YOTI trial in NSW?
- The pilot is not considering online service providers but many online gambling services are based overseas. If the pilot is successful, how what consideration is being given to how digital ID can be used in that context? *(If that is where most underage access occurs)*

