

SUBMISSION:
Consultation on Phase 3
of Australia's Digital Identity legislation

AUSTRALIAN CHRISTIAN LOBBY

About Australian Christian Lobby

Australian Christian Lobby's vision is to see Christian principles and ethics influencing the way we are governed, do business, and relate to each other as a community. ACL seeks to see a compassionate, just and moral society through having the public contributions of the Christian faith reflected in the political life of the nation.

With ~~more than supporters~~ 200,000, ACL facilitates professional engagement and dialogue between the Christian constituency and government, allowing the voice of Christians to be heard in the public square. ACL is neither party-partisan nor denominationally aligned. ACL representatives bring a Christian perspective to policy makers in Federal, State and Territory Parliaments.

acl.org.au

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation**Digital Transformation Agency (DTA)**digitalidentity@dta.gov.au**27 October 2021**

Dear Sir/Madam,

On behalf of the Australian Christian Lobby (**ACL**), I welcome the opportunity to make a submission to the [Consultation on Phase 3 of Australia's Digital Identity legislation](#) (**Consultation**).

The *Trusted Digital Identity Bill 2021* (Cth) exposure draft (**Bill**) contains a multitude of provisions to establish a digital identity system. The ACL is broadly supportive of the Government expanding the current system through this Bill. However, it does not apparently address a key matter for pressing reform in this area – the establishment of a digital system for age verification on adult websites. We also note that there is considerable disquiet in some quarters regarding the Bill and its potential scope in future, including that it could be expanded to other attributes or become compulsory.

ACL's submission discusses that:

1. **Reform is vitally needed to establish age verification for adult websites, and the Government should prioritise linking this to the digital identity system:** A Parliamentary committee recently conducted an inquiry into age verification. It made it abundantly clear in its report that there is a pressing need for reform, given “serious impacts” on the welfare of minors exposed to adult content online. It also clearly recommended that DTA extend the digital identity system to include an age-verification exchange. The Government response indicated that, while it agreed in principle, this is not its initial priority and it will await the development of a ‘roadmap’. In our view, given the evidence of serious harms occurring to minors, the Government *must* prioritise reform. We are concerned that the roadmap may take 12 to 18 months to complete while such serious harms continue to occur. This is particularly so while the COVID-19 pandemic has increasingly required minors to spend more time online.
2. **The Government should otherwise ensure that the system is not expanded inappropriately to other attributes in future and remains genuinely voluntary:** It is vital that the Government retain community trust in the system. It should ensure it does not expand the scheme in future to cover other attributes than those appropriate to its current purposes or make it compulsory.

We make the following submissions to urge the Government to prioritise age verification reform, including suggesting practical ways in which this might occur. We have also detailed some other concerns of which we are aware regarding the potential future scope of the scheme.

We would be very willing to meet with DTA to discuss these submissions and confer regarding how age verification provisions might be drafted into the Bill's existing legal framework.

Yours Sincerely,

Wendy Francis

National Director of Politics

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation**EXECUTIVE SUMMARY**

There would likely be many benefits to society and business of having a central Trusted Digital Identity System (**TDIS**) run by government and supported by a network of accredited agencies under the Trusted Digital Identity Framework (**TDIF**).

The ACL is broadly supportive of the Government developing the digital identity system, including expanding the scheme under the [Trusted Digital Identity Bill 2021 \(Cth\) exposure draft \(Bill\)](#) to enable participation by state and territory governments and the private sector.

However, the scoping of this scheme is of critical importance. In our view, the Government should seriously consider two key matters in this regard, being:

1. Reform is vitally needed to establish age verification for adult websites, and the Government should prioritise linking this to the digital identity system

In 2019-2020, a Parliamentary committee specifically conducted an inquiry into age verification for online wagering and pornography. It made it abundantly clear in its report that there is a pressing need for a digital system for age verification, given “serious impacts” on the welfare of minors exposed to adult content online. It also clearly recommended that DTA extend the digital identity program to include an age-verification exchange. Since then, during the COVID-19 pandemic, Australian minors have also been increasingly active online. In our view, this has made the need for age verification on adult websites even more pressing now than ever.

The Government is clearly the appropriate entity to lead age verification reform, and has been inexorably linked to potential reform since at least the inquiry. The Government’s response to the inquiry report indicated that, while it agreed in principle to reform, this is *not* its initial priority and it will await an eSafety Commissioner ‘roadmap’. In our view, given evidence of serious harms to minors exposed to adult content, the Government *must* prioritise reform. We are concerned that the roadmap may take 12 to 18 months to complete while such serious harms continue to occur.

2. The Government should otherwise ensure that the system is not expanded inappropriately to other attributes in future and remains genuinely voluntary

We understand that there are many potential benefits to the expanded digital identity system and that the attributes to be captured are limited in an apparently appropriate way. However, it is vital that the Government retain community trust in the system. There is considerable disquiet in some quarters regarding the draft Bill and its potential scope in future, including regarding the attributes that it may be used to record or that it may become compulsory.

Recommendations:

1. The ACL urges the Government to prioritise linking age verification to the digital identity system. In particular, we suggest that DTA consider the draft Bill from the perspective of how age verification provisions might be incorporated, either now (if possible, to give minors a level of protection while it awaits a roadmap) or in future (with the aim of easily and quickly introducing them into the existing framework of the Bill after it receives the roadmap). We also suggest that the Government consider whether it may facilitate the roadmap to be developed more quickly.
2. The ACL recommends that the Government otherwise does not expand the program in future to cover other attributes than those appropriate to its current purposes or make it compulsory.

The ACL’s submissions are discussed in more detail below. Any **bold** emphasis in quotes is ours.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity Legislation

SUBMISSIONS

1. Reform is vitally needed to establish age verification for adult websites

Introduction

In our view, reform is vitally needed to establish age verification for adult websites.

The Government also appears to be aware of the need for reform. In 2019-2020, a House of Representatives committee specifically conducted an inquiry into age verification for online wagering and pornography. ACL's submission to the inquiry detailed our strong support for the inquiry and the need for age verification. DTA's submission also indicated that it considered the expansion of the digital identity system to age verification a "convenient" option, and that the system could, from a technological perspective, extend to age verification.

The Committee made it abundantly clear in its resulting report that there is a pressing need for age verification on adult websites. Among other evidence, it discussed widespread and genuine concern about the "serious impacts on the welfare of children and young people" associated with exposure to online adult content. It was "concerned to see this issue addressed as quickly as possible". It also clearly recommended that DTA extend the digital identity system to include an age-verification exchange.

Since then, during the COVID-19 pandemic, Australian minors have also been increasingly required to engage with online technologies and have spent more time online. As such, we consider the need for age verification on adult websites even more pressing than ever.

Inquiry into age verification for online wagering and pornography

As DTA is no doubt aware, the Australian Parliament has already been associated with an inquiry establishing the need for a digital system for age verification on adult websites. It seems clear that the Government is therefore aware of the need for reform.

In particular, following a referral,¹ the House of Representatives Standing Committee on Social Policy and Legal Affairs (**Committee**) resolved on 10 September 2019 to conduct an inquiry into age verification for online wagering and pornography (**Inquiry**).²

ACL's submission to the Inquiry³ detailed our strong support for the Inquiry and the need for age verification processes. Although we will not reiterate our submissions in detail, we discussed the context for pressing reform, including that:

- The ease of access to hardcore pornography and online gambling has been an issue on which the ACL has campaigned for many years. It is vitally important to protect children from online predators. Statistics show that 44% of Australian children aged between 9 and 16 report that they have encountered sexual images online.

¹ From the Minister for Families and Social Services, Senator the Hon Anne Ruston and the Minister for Communications, Cyber Safety and the Arts, the Hon Paul Fletcher MP: See website associated with the Committee and Inquiry on the Parliament of Australia website: <https://www.aph.gov.au/onlineageverification>.

² See website associated with the Committee and Inquiry on the Parliament of Australia website, including the Terms of Reference, details of hearings and submissions: <https://www.aph.gov.au/onlineageverification>.

³ Available for download on the Parliament of Australia website at https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Online_ageverification/Submissions.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation

- While many may argue that it is the responsibility of parents to ensure the safety of their children, advances in online technology have exceeded the rate at which parents can maintain effective safeguards. Most children now have access to personal computers and laptops which are often mandated by the schools they attend. Many children are also more technologically competent than their parents. Further, children and young people are able to access the internet from many public locations which may or may not have filters. Alcohol and gambling advertisements are also part of the sporting culture and as such there is a constant inducement for viewers of online sport to participate in such activities.
- Children are adversely affected by online adult material. Among other things, pornography can lead to addiction, contributes to children being victims and perpetrators of sexual violence and is a factor in increasing reports of children sexually assaulting other children. Even the majority of young people themselves apparently support restrictions on pornography.
- Research shows that viewing pornography can traumatize children and young people, and negatively influence their attitudes to sex, sexuality and relationships. Pornography also eroticises violence towards women and girls and is linked to the early sexualisation of children. The average age of first exposure to pornography is 11, often happening accidentally. One in 10 children under the age of 10 have seen pornography which can include violent porn, bestiality and child pornography. Research by entities such as Australian Psychological Society and Australian Institute of Family Studies expressly discuss the need to protect children and seek to measure the rise in sexual related violence.
- It is the obligation of government to assist parents in protecting their children from this type of harm, both in the interest of those children and to promote a society which fosters respect.

DTA's own submission to the Inquiry ([here](#)) also indicated that it was aware of the possibility of expanding digital identity technology to age verification and considered this a "convenient" option:

*"The DTA believes that **the Digital Identity program could be used to reduce technological barriers in achieving stronger age verification requirements by providing a convenient alternative for users to verify their age.**"*

As such, even before the Committee released its Inquiry report, DTA apparently considered that reform in this area may be beneficial.

DTA's submission also indicated that its digital identity system could, from a technological perspective, extend to age verification, including because its governance would extend to online sites seeking to verify age:

*"... Furthermore, identity providers in the Digital Identity system must meet the strict privacy and security requirements. These requirements are set out in the **DTA's Trusted Digital Identity Framework (TDIF) and other governance**. This governance **would extend to any online wagering and online pornography sites which seek to verify age through the Digital Identity system.***

...

The current Digital Identity system only provides access to selected federal government services. While the system is expected to allow access to private sector and state/territory government services, this is some way down the track and will require

ACL Submission to Consultation on Phase 3 of Australia’s Digital Identity legislation

both legislative and technological change. The use of Digital Identity to achieve age verification for all global online wagering and online pornography sites would require the expansion of the Australian Digital Identity system to international private entities.

...

Digital Identity could be used to verify identity attributes, including age, for online wagering and online pornography. Such sites would only receive the information required to confirm the user meets the age requirements of the service ...”

This indicates that DTA expressly acknowledged, even before the Inquiry report was released, that age verification could practically be linked to digital identity technology.

The Inquiry Committee’s ‘Protecting the age of innocence’ Report

The Committee’s report regarding the Inquiry was published with the title ‘Protecting the age of innocence’ (PTAOI Report) ([here](#)) by the Australian Parliament.⁴

It was dated February 2020, but we understand that it was not released until 5 March 2020, according to the subsequent Government response (discussed further below):⁵

The Australian Government received the report by the House of Representatives Standing Committee on Social Policy and Legal Affairs (the Committee) into age verification for online wagering and online pornography released on 5 March 2020.

The PTAOI Report also made it abundantly clear that there is a pressing need for online age verification. For example, the Committee wrote about “serious impacts” on the welfare of children and young people associated with online exposure to adult content (particularly pornography):

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

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

...

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

It also commented⁶ that evidence showed “very clearly” that there is a genuine concern and noted its “strong view that age verification should be pursued”. It also acknowledged its “strong view” that

⁴ Parliament of Australia (2020). *Protecting the age of innocence*. https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Online_ageverification/Report.

⁵ See page 1 of Government Response, discussed further below.

⁶ See the broader context around the extracts of comments reproduced here at paragraphs 3.174 to 3.183.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation

although age verification might operate imperfectly, “we should not let the perfect be the enemy of the good”:

Committee comment

- 3.174 The Committee recognises that there is increasingly clear evidence that children and young people are being exposed to online pornography, and that this exposure is associated with a range of risks and harms.
- 3.175 Evidence given to the inquiry showed very clearly that there is widespread and genuine concern among the community about the negative impact of online pornography on the welfare of children and young people.
- 3.176 Based on the evidence to the inquiry, it is the Committee's strong view that age verification should be pursued as a measure to limit children and young people's exposure to online pornography.
- 3.177 The Committee acknowledges that age verification is not a silver bullet—some websites containing pornographic material may not be captured, and some determined young people may find ways to circumvent the system. However, when it comes to protecting children from the very real harms associated with exposure to online pornography, the Committee's strong view is that we should not let the perfect be the enemy of the good.

These robust comments indicate to us that the Committee was of the view that there was a pressing need for age verification reform, even if it was not the only (or perfect) solution.

Section 3 of the PTAOI Report also contained many statistics relating to the need for age verification, including regarding specific effects and social impacts on minors exposed to pornography. We have not recited these statistics here but they plainly support the Committee's assertion that exposure to adult online content has serious impacts on minors.

The Committee also recommended clear action to address these harms. In particular, it recommended that age verification be implemented in Australia. It also clearly recommended that DTA do so by extending the existing digital identity system to include an age-verification exchange.

Extracts of its Recommendations include:⁷

Recommendation 1

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

...

Recommendation 2

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

It stated that it was “important” for the work of developing technical standards “to begin now”.⁸

The Committee also discussed DTA's acknowledgement that digital identity technology could be used for age verification (though not in the original program scope).⁹ Extracts include:

⁷ Note – there were 6 recommendations in total, and the 3 recommendations we have noted are extracts only.

⁸ PTAOI Report, paragraph 2.138.

⁹ See paragraphs 2.70-2.78 for the full context of these comments in the PTAOI Report.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation

- 2.76 The DTA submitted that Digital Identity could be used to verify identity attributes, including age, for the purpose of accessing age-restricted sites:
- Such sites would only receive the information required to confirm the user meets the age requirements of the service. Other information could potentially be provided, but this would be consent based to ensure the [user's] privacy is protected.⁶⁵
- 2.77 However, Mr Alexander told the Committee that while there would be some benefits to using the Digital Identity program for online age verification, the DTA would need legislative authority for the program to connect directly to services in the private sector, and further investment would be required as age verification was not in the original scope of the program.⁶⁶

Overall, the Committee seems to have expressly accepted that DTA is an appropriate entity to implement age verification in Australia. DTA also appears to have accepted that it is technically possible and likely beneficial to extend its digital identity program to age verification.

Notably, the Committee also recommended that the eSafety Commissioner be resourced to develop a roadmap for the implementation of a mandatory age verification regime for online pornography:

Recommendation 3

- 3.184 The Committee recommends that the Australian Government direct and adequately resource the eSafety Commissioner to expeditiously develop and publish a roadmap for the implementation of a regime of mandatory age verification for online pornographic material, setting out:
- a. a suitable legislative and regulatory framework;
 - b. a program of consultation with community, industry, and government stakeholders;
 - c. activities for awareness raising and education for the public; and
 - d. recommendations for complementary measures to ensure that age verification is part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.

The Committee clearly stated that it was “concerned to see this issue addressed as quickly as possible”, and recommended that the roadmap be presented to government within 12 months:

- 3.189 Lastly, the Committee is concerned to see this issue addressed as quickly as possible. As such, the Committee recommends that this work be completed and presented to government for decision within 12 months of the presentation of this report.
- 3.190 The Committee encourages the Australian Government to provide additional resources to the Office of the eSafety Commissioner as is required to complete this work without compromising the important existing work carried out by the office.

We have discussed such timeframes further below.

In any case, by propounding such clear recommendations, the Committee seemed to accept that reform is vitally needed and should occur as quickly as possible.

The Government's response to the PTAOI Report is discussed below.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation**The impact of the COVID-19 pandemic response on the online activity of minors**

Notably, following the Inquiry and PTAOI Report, the COVID-19 pandemic caused a marked shift in how our society uses online technologies. This includes Australian minors, who have been required through the pandemic response and lockdowns to increasingly engage with remote learning and have apparently spent more time online.

For example, according to research by Roy Morgan,¹⁰ during COVID-impacted 2020 young Australians aged 6 to 13 years old spent an average of almost 16 hours a week online, including 11 hours a week on the internet at home, a figure which was up 0.9hrs from 2018. Australian Institute of Family Studies also discusses research which found that during COVID-19 lockdowns, families reported that children were spending 35 minutes more time on screens a day on weekends.¹¹ A report by Australian Childhood Foundation in 2020¹² also found that, from 375 parents surveyed:

- 46% reported that their children spent more time by themselves in their room.
- 71% reported that their children had more screen time than usual during COVID-19 lockdown.
- 35% were worried about regulating what their child was exposed to on the internet and 33% about ensuring that their children were not abused or exploited when they used the internet.

Other broad estimates also indicate a general increase in online activity across age categories. For example, a report in early 2021¹³ stated that the amount of time Australian users aged 16 to 64 reported spending online in 2020 had jumped by 10% (or 32 more minutes). Such effects have apparently also been seen internationally – research studies report that screen time increased globally for both children and adults during the pandemic.¹⁴

A Ministerial media release¹⁵ also discussed online safety for this “time when children are spending more time online” because of COVID-19. It stated that “higher use of the internet during the COVID-19 crisis has been accompanied by a 40 per cent spike in reports to eSafety across its reporting areas”.

Regardless of which source is used to quantify the increase, the trend seems clear – Australian minors have generally spent more time online through the COVID-19 pandemic. As such, we consider the need for age verification reform even more pressing than ever.

¹⁰ Roy Morgan (2021, 3 May). *During 2020 Young Australians spent more time online and less time watching TV and playing with friends*. <http://www.roymorgan.com/findings/8697-young-australians-time-spent-activities-may-2021-202105030417>.

¹¹ Australian Institute of Family Studies (2021, 5 August). *Too much time on screens? Screen time effects and guidelines for children and young people*. <https://aifs.gov.au/cfca/2021/08/05/too-much-time-screens-screen-time-effects-and-guidelines-children-and-young-people>.

¹² Tucci, J., Mitchell, J. and Thomas, L. for Australian Childhood Foundation (2020, August). *A Lasting Legacy – The impact of COVID-19 on children and parents*. https://www.childhood.org.au/app/uploads/2020/08/A_Lasting_Legacy_-_The_Impact_of_COVID19_on_Children_and_Parents_Final.pdf. See particularly page 14.

¹³ We Are Social (2021, 8 February). *Digital 2021: Australia: We spend 110% more time online*. <https://wearesocial.com/au/blog/2021/02/digital-2021-australia-we-spend-10-percent-more-time-online/>.

¹⁴ See, for example, Pandya, A. and Lodha, P. (2021) *Social Connectedness, Excessive Screen Time During COVID-19 and Mental Health: A Review of Current Evidence*. *Front. Hum. Dyn* 3:684137. DOI: 10.3389/fhumd.2021.684137. See <https://www.frontiersin.org/articles/10.3389/fhumd.2021.684137/full#B9>.

¹⁵ By the Minister for Communications, Urban Infrastructure, Cities and the Arts The Hon Paul Fletcher MP (2020, 7 April). *Keeping our kids safe online during COVID-19*. <https://minister.infrastructure.gov.au/fletcher/media-release/keeping-our-kids-safe-online-during-covid-19>.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation**2. The Government should prioritise linking age verification to the digital identity system****Introduction**

The Government is clearly the appropriate entity to lead age verification reform. It has been inexorably linked to potential reform since at least the Inquiry.

The Government's response to the PTAOI Report indicated that, while it agreed in principle to reform, this is not its initial priority and it will await a 'roadmap' currently being developed by the Office of the eSafety Commissioner (**eSafety**).

In our view, given widespread concern and evidence of serious harms occurring in respect of minors from exposure to adult content online, the Government *must* prioritise reform. We find it concerning that eSafety may take 12 to 18 months to provide a roadmap while such serious harms continue to occur, and particularly while the COVID-19 pandemic has minors spending more time online.

We have made several suggestions below regarding how the Government and particularly DTA might seek to practically prioritise reform.

The Government's response to the 'Protecting the age of innocence' report

The official Government response to the PTAOI Report was published on 1 June 2021 ([here](#)) (**Response**),¹⁶ apparently over a whole year after the report was first released.

Commendably, the Response acknowledged online safety concerns as a key issue:¹⁷

"The Government recognises that children's access to age-inappropriate or potentially harmful online services and content is a key online safety concern for the Australian community."

It also cited research regarding online pornography and gambling and safety concerns¹⁸ and clearly acknowledged that age verification may limit harmful online exposures to children:¹⁹

"While there are no simple solutions to any online safety issue, technologies, such as age verification, age assurance and age prediction, are developing at pace. If used in conjunction with filtering and other proactive user safety settings, they can play a role in limiting exposure to harmful content for children."

Notably, in response to Recommendation 2 regarding DTA extending the digital identity system to age verification, the Government supported the recommendation *in principle only*, as this is *not its initial priority*.²⁰ It agreed that DTA was well placed to explore extending the system, but indicated that its initial priority is the completion of work discussed in its response to Recommendation 1:

¹⁶ Parliament of Australia (2020). *Government Response*.

https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Online_ageverification/Government_Response.

¹⁷ See page 1 of the Government Response.

¹⁸ See page 1 of the Government Response.

¹⁹ See page 2 of the Government Response.

²⁰ See page 4 of the Government Response.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation**Recommendation 2:**

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

The Government **supports** this recommendation **in principle**.

Initially, the Government's priority will be to complete work underway that explores the potential for changes to the policy and accreditation framework, as discussed in the response to Recommendation 1. Depending upon the findings of this work, further technical interventions may be required. If so, the Government agrees that the Digital Transformation Agency is well placed to explore extending the Digital Identity program.

The Government's response to Recommendation 1 refers to matters including a roadmap being developed by eSafety for the implementation of a mandatory age verification regime for online pornography:

Recommendation 1:

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

- a. These standards should specify minimum requirements for privacy, safety, security, data handling, usability, accessibility, and auditing of age-verification providers.
- b. Consideration should be given to the existing technical standards in Australia and overseas, including but not limited to the UK Age Verification Certificate, the PAS 1296 Age Checking code of practice, the Trusted Digital Identity Framework, and the European Union General Data Protection Regulation.
- c. Opportunities should also be provided for consultation with industry, including private age-verification providers, and members of the public.

The Government **supports** this recommendation **in principle**.

The Government is committed to protecting young people while safeguarding the privacy and security of people of all ages in an increasingly digital environment.

The Government has several work streams underway that examine the efficacy of existing measures and identify further measures required to meet this commitment:

- the Office of the eSafety Commissioner is leading the development of a roadmap for the implementation of a mandatory age verification regime for online pornographic material, as discussed in the response to Recommendation 3.
- the Department of Social Services is completing a review of customer verification requirements for online wagering services as discussed in the response to Recommendation 4.

Subject to the findings of the work outlined above, further technical standards-based work may be required which could include requirements for privacy, safety, security, data handling, usability, accessibility, and auditing of age-verification providers. If so, the Government agrees that:

- the Digital Transformation Agency (DTA) is well-placed to develop any necessary technical standards; and
- the Australian Cyber Security Centre (ACSC) is well-placed to provide any necessary advice and support relating to the cybersecurity of IT systems.

As such, the Government seems to have clearly indicated that while it agrees *in principle* to age verification reform, this is *not* its initial priority and it will await completion of the eSafety roadmap (and other matters) first.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity Legislation

In this vein, the Government clearly supported Recommendation 3 that the eSafety Commissioner develop and publish such a roadmap, and be adequately resourced to “expeditiously” do so:

Recommendation 3:

3.184 The Committee recommends that the Australian Government direct and adequately resource the eSafety Commissioner to expeditiously develop and publish a roadmap for the implementation of a regime of mandatory age verification for online pornographic material, setting out:

- a. a suitable legislative and regulatory framework;
- b. a program of consultation with community, industry, and government stakeholders;
- c. activities for awareness raising and education for the public; and
- d. recommendations for complementary measures to ensure that age verification is part of a broader, holistic approach to address risks and harms associated with the exposure of children and young people to online pornography.

The Government **supports** this recommendation.

With children accessing or being exposed to sexually explicit material on a diverse range of online platforms, the Government recognises that there is no straightforward solution. The development of a comprehensive roadmap that adequately explores the complexities of regulating online pornography will require considerable amounts of research and stakeholder consultation over a 12 to 18 month period.

The Office of the eSafety Commissioner (eSafety) is leading the development of this roadmap, in collaboration with community, industry, state and territory governments, and Commonwealth agencies including the Department of Infrastructure, Transport, Regional Development, and Communications (DITRDC); Department of Social Services; Department of Home Affairs; Digital Transformation Agency; and the Australian Cyber Security Centre. The roadmap will be based on detailed research as to if and how a mandatory age verification mechanism or similar could practically be achieved in Australia. The roadmap, including a recommended way forward, will be provided to Government for consideration.

The Government is committed to keeping Australians safe online and maintaining Australia's position as a world leader on this issue. On 11 December 2019, the Government released the online safety legislation reform discussion paper which outlined key elements of a proposed new Online Safety Act. DITRDC considered the feedback received during consultation. The challenge of children's access to age inappropriate content, including pornography, is being considered through these reforms.

The Government is also considering the risks and harms posed by the exposure of children and young people to online pornography through its work on developing a National Strategy to Prevent Child Sexual Abuse (National Strategy). The National Strategy is a key recommendation of the Royal Commission into Institutional Responses to Child Sexual Abuse. The National Strategy will be a long term policy framework that establishes a coordinated, nationally aligned approach to preventing child sexual abuse in all settings. As such, it will incorporate the important work being progressed by eSafety to keep children safe online.

However, we note that the Government estimated that the roadmap would require “considerable amounts of research and stakeholder consultation over a 12 to 18 month period”.

In our view, the Government *must* prioritise age verification reforms and should consider whether it is possible to expedite the reform process. We have discussed this further below.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity Legislation**The eSafety Commissioner's roadmap for a mandatory age verification regime for online pornography**

The eSafety website ([here](#)) confirms that on 1 June 2021, the Australian Government requested the eSafety Commissioner to “develop an implementation roadmap for a mandatory age verification regime relating to online pornography” as part of its Response.

eSafety welcomed the Government's Response and confirms that it is also of the view that children must be protected from “harmful online content”:²¹

“eSafety welcomes the Government's response and commitment to protecting children from harmful online content. For young children, accidental encounters with pornography can be distressing and even harmful. For older children who stumble upon or seek out pornographic material, there is a risk that it will give them unrealistic and damaging ideas about what intimate relationships should look like – especially as the material becomes increasingly violent and extreme.”

eSafety subsequently issued a call for evidence on 16 August 2021, seeking “insights into effective age verification techniques, as well as the impact of online pornography on children and proven methods of educating young people about both respectful and harmful sexual behaviours”.²²

The call for evidence has now closed and eSafety is using the submissions to inform the next phase of its review. In particular, it is embarking on “targeted consultations with stakeholders” to identify appropriate mechanisms for an Australian age verification regime that restricts access by minors to online pornography. Once its review is complete, eSafety will present minimum requirements and elements to the Government for consideration.²³

In terms of timeframes:²⁴

- In June 2021, eSafety was called to lead the development of the implementation roadmap.
- In July 2021, internal research and policy development began.
- In August 2021, it put out the call for evidence.
- In September 2021, it began the engagement process for key stakeholders.
- In April 2022, it intends to hold working groups with key stakeholders to establish principles and minimum standards for an age verification regime and recommended wraparound initiatives.
- In December 2022, it intends to present the roadmap to Government.

As such, we understand that eSafety may take a total of 12 to 18 months to develop the roadmap and present it to Government. This seems to reflect the timeframe anticipated by the Government in its Response (see above).

We have discussed our concerns regarding this timeframe below.

²¹ eSafety Commissioner (2021). *Age verification*. <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>.

²² eSafety Commissioner (2021). *Age verification*. <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>.

²³ eSafety Commissioner (2021). *Age verification*. <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>.

²⁴ eSafety Commissioner (2021). *Age verification*. <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation**The need to prioritise age verification reform**

The Australian Government is clearly the appropriate entity to lead age verification reform through legislative change. It has also been inexorably linked with potential reform right back to at least 2019 when the Committee was referred the Inquiry.

We commend the Committee for conducting the Inquiry. We also commend the Government for considering the PTAOI Report, publishing a response which recognises that minors accessing harmful content online is a key issue and agreeing in principle to reform. We also specifically commend DTA for acknowledging that the digital identity system may potentially expand to age verification, and eSafety for leading consultation. Each of these steps has been critical in starting the reform process.

However, in light of the pressing need for reform discussed above, we find it concerning that age verification reforms are not an initial priority of the Government. In our view, given the widespread concern and evidence of serious harms occurring from minors being exposed to adult content online, the Government *must* prioritise reform.

We acknowledge that the PTAOI Report did recommend that the Government direct and adequately resource eSafety to expeditiously develop and publish a roadmap (see above). We also note that the Government supported this approach and directed eSafety to do so. It has also confirmed that further consideration is in fact needed regarding whether age verification is “appropriate for certain industry sectors”, and that technology is only part of the solution.²⁵ For these reasons, we understand that the development of the roadmap is a recommended and likely valuable process in shaping reform. As such, we are not suggesting that the Government implement reform prior to receiving it.

We also note that DTA intends to introduce the Bill into Parliament in late 2021,²⁶ well before the eSafety timeline for presenting the roadmap to Government. As such, we are also not suggesting that the Government delay the introduction of the Bill to Parliament while it awaits the eSafety roadmap.

However, we note that the roadmap was recommended by the Committee to be expeditiously provided. We find it concerning that it may take up to 18 months to complete while such serious harms continue to occur to minors, particularly while the COVID-19 pandemic has caused them to spend more time online. We understand that the Government Response anticipated that 12 to 18 months would be required for extensive consultation regarding the roadmap (and that the Committee also indicated a 12 month timeframe), but query whether it could be completed any more quickly in light of the telling PTAOI Report and the delay in the roadmap process beginning (discussed further below).

Essentially, it would seem that any age verification reform is unlikely to practically occur until the beginning of 2023 *at the very earliest*. Other sources which comment on this also expect that action will not be taken until “at least 2023”.²⁷ We note that if the roadmap takes longer or other factors complicate the delivery of reform, the timeframe may also possibly extend even further.

While acknowledging the complex context for change, we urge the Government to prioritise reform by whatever appropriate means possible. The Government was made aware of the pressing need for age verification reforms some time ago now, at very least upon the release of the PTAOI Report (over a year and a half ago). Our key concern is not criticising the Government for the time that it may take

²⁵ See page 2 of Government Response.

²⁶ DTA (2021). *Digital Identity Legislation Position Paper*. <https://www.digitalidentity.gov.au/have-your-say/phase-2-digital-identity-legislation/digital-identity-legislation-position-paper>.

²⁷ See, for example, InnovationAus (2021, 2 June). *Digital ID for age verification gets the nod*. <https://www.innovationaus.com/digital-id-for-age-verification-gets-the-nod/>.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation

to introduce reform, as it is appropriate that such reform be appropriately scoped and effective when introduced, but in preventing serious online harms for minors as soon as reasonably possible .

If reform is not undertaken until at least early 2023, around three years will have passed since the PTAOI Report confirmed the gravity of the dangers for Australian minors online. This is three years during which Australian minors are able to suffer the harms discussed above (and perhaps more likely actually will as they spend more time online). While age verification reforms may be complex to scope and introduce, this is a sobering reality for Australian minors, their parents and the community at large.

As noted above, the Committee also stated that it was “concerned to see this issue addressed as quickly as possible”, and clearly recommended that the roadmap be presented to government *within 12 months* of presentation of the PTAOI Report:

3.189 Lastly, the Committee is concerned to see this issue addressed as quickly as possible. As such, the Committee recommends that this work be completed and presented to government for decision within 12 months of the presentation of this report.

3.190 The Committee encourages the Australian Government to provide additional resources to the Office of the eSafety Commissioner as is required to complete this work without compromising the important existing work carried out by the office.

As mentioned above, we understand that the PTAOI Report, though dated February 2020, was released on 5 March 2020 (according to the Government Response).²⁸ If so, we understand that the Committee was recommending that the eSafety roadmap be presented to government by March 2021.

However, according to the eSafety website, the Government only requested eSafety to develop a roadmap on 1 June 2021²⁹ (the Government itself did not even publish its Response to the PTAOI Report until that month). This was apparently well after the roadmap was recommended to have already been completed and presented to Government. It seems that eSafety may also take slightly longer than the 12 months recommended by the Committee (up to 18 months) (see above) to develop and present the roadmap to Government.

We assume that perhaps the COVID-19 pandemic response has impacted the relevant timeframes. However, it is nonetheless concerning that the Committee recommended this issue be addressed “as quickly as possible” if the roadmap may be presented to Government in *December 2022* rather than *March 2021* (over a year and a half later). We note that the main source of delay appears to be the Government taking over a full year to issue its official Response, and thereby only directing eSafety to develop the roadmap after the date by which the Committee had recommended it already be done.

In any case, the position now remains that this reform should be implemented as soon as possible.

In terms of possible practical steps to prioritise reform, we suggest consideration of the following:

1. **Age verification provisions:** We suggest that DTA consider the draft Bill from the perspective of how age verification provisions might be incorporated.

Ideally, this might occur with the aim of inserting provisions into the draft Bill now, if possible, to give minors some level of protection while the Government awaits the eSafety roadmap.

²⁸ See page 1 of Government Response.

²⁹ eSafety Commissioner (2021). *Age verification*. <https://www.esafety.gov.au/about-us/consultation-cooperation/age-verification>.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation

However, this seems impractical given that it remains to be seen what actual mechanisms the roadmap will specify as appropriate for the age verification regime. The Government seems to not yet be in a position to appropriately scope and draft such provisions.

In any case, we still suggest that DTA consider the draft Bill now from the perspective of readily including age verification provisions in future. It could consider an outline for such provisions with the aim of easily and quickly introducing them into the existing framework of the Bill after it receives the eSafety roadmap. It would be beneficial for the Bill to be considered from this perspective now, before it is actually passed, to ensure that such provisions could fit into its overall structure and save detailed changes later on.

We note that even if the eSafety roadmap is yet to specify the specific minimum requirements and elements for an Australian age verification regime, it seems that DTA is likely to be at least one entity to deliver it through expanding digital identity technology. This seems apparent from the PTAOI recommendations as well as DTA's submissions to the Inquiry indicating that this is technologically possible and likely a "convenient" option (see above). As such, it seems likely that, even if the specifics are yet unknown, DTA will be responsible for implementing age verification reforms in future and should consider the Bill from this perspective now.

2. **eSafety resourcing:** We also suggest that the Government consider whether the eSafety roadmap might possibly be facilitated to occur more quickly. For example, we query whether any additional Government resources could be dedicated to further expedite the review, or at least shorten its anticipated timeframe to the recommended 12 months rather than 18 months.

We acknowledge that the Government has other priorities to balance in addition to age verification reforms, as well as its own initial priorities in terms of digital identity technology specifically. We also understand that the Government is now well aware of the possible link between digital identity technology and an age verification exchange, has accepted reform in principle and will apparently move towards changes once it receives the eSafety roadmap.

However, we still urge the Government to consider the abundant evidence of harms currently occurring to minors in Australia from exposure to adult content online and thereby also determine to make age verification reform a concurrent priority and seek to expedite it if possible.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity Legislation**3. The Government should otherwise ensure that the system is not expanded inappropriately to other attributes in future and remains genuinely voluntary****Introduction**

We understand that there are many potential benefits to an expanded digital identity system and that the attributes to be recorded under the system are already limited in an apparently appropriate way.

However, it is vital that the Government retain community trust in the system. We note that there is considerable disquiet in some quarters regarding the draft Bill and its potential scope in future, including with respect to the attributes it may potentially record or that it may become compulsory.

In our view, the Government should ensure that it does not expand the scheme in future to cover other attributes than those appropriate to its current purposes and that it remains genuinely voluntary.

The structure of the expanded system and its purposes

According to DTA's website, digital identity technology is currently just used for identity verification in respect of government services.³⁰

A DTA fact sheet indicates that Australians currently use the digital system to access a total of 80 government services.³¹ DTA's Acting Chief Executive Officer (CEO) also stated in an official guide that over 4 million people and 1.2 million business use digital identity technology.³²

According to DTA, the purposes of the draft Bill are to:³³

1. enable the expansion of the digital identity system to facilitate participation by state and territory governments and the private sector;
2. enshrine in law various privacy and consumer protections, so that Australians can have confidence in the System and know that their personal information is safe and secure; and
3. establish permanent governance arrangements and a strong regulatory regime.

The [Minister's foreword](#) to the official guide propounds the likely economic benefits of expanding the scheme in these ways, and indicates that "safety" is a key focus.³⁴ DTA also notes a range of benefits which stakeholders across Australia may realise once the Bill is passed, including better consumer access to services, certainty for businesses, fraud protection and improved security.³⁵ The [Digital Identity Legislation Background Paper](#) calls this scheme steps towards a "whole-of-economy solution".

³⁰ DTA (2021). *About Digital Identity*. <https://www.digitalidentity.gov.au/about-digital-identity>.

³¹ DTA (2021). *Digital Identity Legislation: What is it?* <https://www.digitalidentity.gov.au/sites/default/files/2021-09/Digital%20Identity%20Legislation%20-%20what%20is%20it%20-%20factsheet.pdf>.

³² DTA (2021). *CEO statement*. <https://www.digitalidentity.gov.au/have-your-say/phase-3/ceo-statement>. See also DTA (2021). *Your guide to the Digital Identity Legislation*. <https://www.digitalidentity.gov.au/sites/default/files/2021-10/Your%20guide%20to%20the%20Digital%20Identity%20legislation.pdf>, page 4.

³³ DTA (2021). *Have your say on Australia's Digital Identity Legislation*. <https://www.digitalidentity.gov.au/have-your-say/phase-3>.

³⁴ DTA (2021). *Your guide to the Digital Identity Legislation*. <https://www.digitalidentity.gov.au/sites/default/files/2021-10/Your%20guide%20to%20the%20Digital%20Identity%20legislation.pdf>, page 3.

³⁵ See DTA (2021). *Digital Identity Legislation: What is it?* <https://www.digitalidentity.gov.au/sites/default/files/2021-09/Digital%20Identity%20Legislation%20-%20what%20is%20it%20-%20factsheet.pdf>.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity Legislation

We also expect that there will be many benefits to both society and business of expanding the digital identity system and having a central TDIS run by government and supported by a network of accredited agencies under the TDIF. These could include benefits from various perspectives including economy, security, privacy and convenience. ACL is therefore broadly supportive of the Government developing the digital identity system, including expanding the scheme under the Bill to enable participation by state and territory governments and the private sector.

We note that DTA has already conducted two rounds of extensive public consultation regarding the proposed changes, so it has already considered public expectations for the legislation generally.³⁶ We also note that the Government has been developing the digital identity system since 2015.³⁷ However, we think it is vital that the Government retain community trust in the system and wish to assist DTA in this regard. We understand that DTA also considers this vital, given that DTA's CEO called trust in digital systems "critical" and noted that DTA has used community feedback so far to ensure that the draft legislation will enhance trust in the digital system (among other things).³⁸

In that vein, we note that there is considerable disquiet in some quarters regarding the draft Bill and its potential scope in future, including for example with respect to:

1. the attributes that it may potentially be used to record; and
2. that it may become a compulsory scheme (or otherwise less than genuinely voluntary).

To assist DTA in further considering public expectations for the digital identity system, we have discussed these concerns below.

Concerns regarding the potential expansion of the system to other attributes

DTA states that the system is focussed on "limiting" the collection, use and disclosure of personal information to a narrow purpose and minimising information retention (among a few other focuses).³⁹

We note that section 10 of the Bill defines the meaning of an attribute of an individual as follows:

10 Meaning of attribute of an individual

- (1) An **attribute** of an individual means information that is associated with the individual, and includes information that is derived from another attribute.
- (2) Without limiting subsection (1), an **attribute** of an individual includes the following:
 - (a) the individual's current or former name;
 - (b) the individual's current or former address;
 - (c) the individual's date of birth;
 - (d) information about whether the individual is alive or dead;
 - (e) the individual's mobile phone number;
 - (f) the individual's email address;
 - (g) if the individual has a digital identity—the time and date the digital identity was created.

³⁶ DTA (2021). *Have your say on Australia's Digital Identity Legislation*. <https://www.digitalidentity.gov.au/have-your-say/phase-3>.

³⁷ DTA (2021). *Digital Identity Legislation: What is it?* <https://www.digitalidentity.gov.au/sites/default/files/2021-09/Digital%20Identity%20Legislation%20-%20what%20is%20it%20-%20factsheet.pdf>.

³⁸ DTA (2021). *CEO statement*. <https://www.digitalidentity.gov.au/have-your-say/phase-3/ceo-statement>.

³⁹ DTA (2021). *Digital Identity Legislation Background Paper*. <https://www.digitalidentity.gov.au/have-your-say/phase-1-digital-identity-legislation/digital-identity-legislation-background-paper>.

ACL Submission to Consultation on Phase 3 of Australia's Digital Identity legislation

- (3) However, the following is not an attribute of an individual:
- (a) biometric information of the individual;
 - (b) a restricted attribute of the individual;
 - (c) information or an opinion about the individual's:
 - (i) racial or ethnic origin; or
 - (ii) political opinions; or
 - (iii) membership of a political association; or
 - (iv) religious beliefs or affiliations; or
 - (v) philosophical beliefs; or
 - (vi) membership of a professional or trade association; or
 - (vii) membership of a trade union; or
 - (viii) sexual orientation or practices; or
 - (ix) criminal record;
 - (d) information that is prescribed by the TDI rules and relates to the individual.
- (4) Subsection (3) does not prevent information described in any of the paragraphs in subsection (2) from being an attribute of an individual if the information is not primarily of any of the kinds described in subsection (3), even if information of any of those kinds can reasonably be inferred from the information.

Example: Even if an individual's racial or ethnic origin can reasonably be inferred from the individual's name or place of birth, this does not prevent the individual's name or place of birth from being an attribute of the individual.

As such, we understand that the attributes to be recorded under the expanded system are currently limited by section 10. We also consider that the way an attribute is currently defined by section 10 is apparently appropriate. For example, we support the inclusion of section 10(3) in particular which carves out certain information from being an attribute.

However, we are aware that there still exists concern among some quarters that the scheme could potentially be linked to other attributes in future. For example, we understand that some members of the community are particularly concerned that personal health information, such as vaccination status, could potentially be recorded by digital identity systems in future.

We understand that DTA does not currently intend for digital identities to be linked to health matters (either generally, or specifically with respect to vaccination). For example, we note that:

- DTA's website clearly states that there is "no link between digital identity and vaccination certificates". Digital identity is also not used to track vaccination status.⁴⁰
- Section 11 of the Bill defines a "restricted attribute" (which is specifically carved out from the definition of an attribute in section 10) as including "health information" about the individual (among other things). It also refers to individuals' Medicare numbers and healthcare identifiers. On this basis, we understand that health information about individuals, including their Medicare numbers and healthcare identifiers, are generally restricted from being considered relevant attributes under the digital identity system.

In our view, personal health information (including vaccination status) should in no way be linked to digital identities now or in future. This is highly personal information and should remain a matter between individuals and medical professionals. This also seems critical in respect of what DTA describes as a system "designed with privacy in mind" and in respect of a Bill intended to provide

⁴⁰ DTA (2021). *About Digital Identity*. <https://www.digitalidentity.gov.au/about-digital-identity>.

ACL Submission to Consultation on Phase 3 of Australia’s Digital Identity Legislation

“assurance to consumers that their privacy and security is protected”.⁴¹ If the Government took such an approach, we expect a notable portion of the community would lose trust in the system.

The need for Digital Identity technology to remain voluntary

DTA’s website confirms on multiple subpages that digital identity technology is already “entirely voluntary” and controlled by users of the system – they choose when to use it and their information is not shared with any service unless they consent. People who can’t or don’t want to use it do not need to.⁴² Both creating and using a digital identity is a choice, not compulsory.⁴³

We understand that the Bill does not intend to change this. For example:

- The legislation background paper lists “choice” and “consent” as two core principles.⁴⁴
- The Objects in section 3 of the Bill clearly state that they are to be achieved by “establishing a trusted digital identity system that is ... voluntary” (among other things).
- Section 30 of the Bill establishes that generating and using a digital identity is voluntary, such that “a participating relying party must not, as a condition of providing a service or access to a service, require an individual to generate or use a digital identity” (except in limited circumstances).
- The official digital identity guide notes that both the TDIF accreditation scheme and the actual TDIS are both “distinct, voluntary schemes which entities can choose to join”.⁴⁵ It also lists as a “protection” in the TDIS that “creating/using a digital identity is voluntary”.⁴⁶
- Under section 61 of the Bill, digital identities must be deactivated on request by individuals.

As such, it seems clear that the digital identity scheme is intended to be genuinely voluntary both now and in future. However, we are aware that there still exists concern among some quarters that the scheme could potentially become compulsory (or otherwise less than genuinely voluntary, if changes are made to effectively or practically require individuals to use the system).

In our view, it is vital that the system remains *genuinely* voluntary, including because it records very personal information about individuals. If the Government ever does make participation compulsory, or otherwise changes any aspect of the system so that it is no longer genuinely voluntary, we expect that this would also cause a notable portion of the community to lose trust in the system.

⁴¹ See, for example, discussion in DTA (2021). *Digital Identity Legislation: What is it?*

<https://www.digitalidentity.gov.au/sites/default/files/2021-09/Digital%20Identity%20Legislation%20-%20what%20is%20it%20-%20factsheet.pdf>.

⁴² DTA (2021). *About Digital Identity*. <https://www.digitalidentity.gov.au/about-digital-identity>.

⁴³ DTA (2021). *Digital Identity system*. <https://www.digitalidentity.gov.au/about/digital-identity-system>.

⁴⁴ DTA (2021). *Digital Identity Legislation Background Paper*. <https://www.digitalidentity.gov.au/have-your-say/phase-1-digital-identity-legislation/digital-identity-legislation-background-paper>.

⁴⁵ DTA (2021). *Your guide to the Digital Identity Legislation*. <https://www.digitalidentity.gov.au/sites/default/files/2021-10/Your%20guide%20to%20the%20Digital%20Identity%20legislation.pdf>, page 13.

⁴⁶ DTA (2021). *Your guide to the Digital Identity Legislation*. <https://www.digitalidentity.gov.au/sites/default/files/2021-10/Your%20guide%20to%20the%20Digital%20Identity%20legislation.pdf>, page 28.