To: Andrew Walter
First Assistant Secretary, Integrity & Security Division
Attorney General's Department
By email: Andrew.Walter@ag.gov.au; OnlinePrivacyBill@ag.gov.au

cc. Sarah Croxall
Principal Director, Regulation and Strategy Branch
Office of the Australian Information Commissioner
By email: sarah.croxall@oaic.gov.au

Friday December 10, 2021

Dear Mr. Walter,

The Digital Industry Group Inc. (DIGI) thanks you for the extended opportunity to provide our views on the exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the Bill).

By way of background, DIGI is a non-profit industry association that advocates for the interests of the digital industry in Australia. DIGI's founding members are Apple, eBay, Google, Linktree, Meta, Twitter, Snap and Yahoo, and its associate members are Change.org, Gofundme, ProductReview.com.au and Redbubble. DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected.

DIGI fully supports the intention of the Bill to protect the privacy of minors online and to safeguard them from harm. We agree that specific privacy protections for minors should be expanded upon within the Privacy Act.

DIGI's members both endorse and enable consumers to be informed about the use of their data, privacy choices including the right to data erasure, cross-functional systems of internal privacy governance and strong cyber security protections. They also provide privacy safeguards for minors, such as parental controls, age restrictions and a number of proactive measures in place to enforce those restrictions, and a range of policies and other measures to ensure that the experience of minors online is age-appropriate.

DIGI's commitment to the protection of minors online is exemplified through our work to standardise system-wide protections in this area through our co-leadership of industry code development the Online *Safety Act 2021* (OSA Codes) that also address the exposure of minors to age-inappropriate material. DIGI is developing these codes together with the Communications Alliance, a steering group of industry associations and in partnership with the Office of the eSafety Commissioner.

DIGI therefore supports the intention of the Bill, and the wider review of the Privacy Act, to encourage widespread adoption of such safeguards across a diverse span of companies. To that end, we raise questions in this submission as to whether the Bill's scope reflects its goal, and we encourage a cohesive approach with the wider Privacy Act Review (the Review).

While we are supportive of additional privacy protections for minors and widespread standardisation of those protections, **DIGI's primary concern with the Bill relates to its proposals for universal age verification on services enabling interaction**, and this is the main focus of our submission.

We note that the age verification requirements were a new addition to the Bill when it was released on October 25, 2021 and had not previously been foreshadowed when the Bill was first announced on March 24, 2019 nor in the ensuing 2.5 year period. Given the unprecedented implications of age verification of Australians on a wide range of digital services, in light of the extremely broad definition of "social media services", wider consultation must take place in relation to this specific proposal.

We suggest that the Office of the eSafety Commissioner's existing roadmap on age verification (AV Roadmap) – that was a result from Government's parliamentary inquiry into age verification for online wagering and online pornography – provides an appropriate avenue for further exploration of age verficaton. DIGI has engaged in consultations for the AV roadmap, and we understand that the AV roadmap will be presented to the Government in 2022[1]. Further exploration of age verification within the context of the AV roadmap would signal a whole-of-Government approach that is prudent with taxpayer funds, as opposed to legislating for widespread age verification in the absence of necessary consultation, and in advance of an existing Government work program on the same issue.

Our secondary area of focus in this submission relates to code development. Should the solution to the Bill's goals be advanced by way of a code under the Bill (OP Code), and not as part of the wider Privacy Act Review as we strongly recommend, **DIGI also advances several recommendations to ensure the code development process is set up for success**, including how code developers should work closely with the Office of the Australian Information Commissioner (OAIC). In making these recommendations, we draw upon DIGI's experience leading the development of *The Australian Code of Practice on Disinformation and Misinformation* and the aforementioned OSA codes, for which we are leading the drafting of the sections pertaining to social media services, search engines and app distribution services.

DIGI supports measures, whether proposed through this Bill or the wider Privacy Act Review, to strengthen clarity and compliance with the Australian Privacy Principles (APPs). **We also support interoperability between Australia's updated privacy regulation with the European Union's General Data Protection Regulation (GDPR)**; for example, the Bill's proposals in relation to ceasing to use or disclose personal information upon request should be amended for consistency with the GDPR.

We thank you for your consideration of the matters raised in this submission, and we look forward to further engaging in this review process. Should you have any questions, please do not hesitate to contact me with any questions.

Best regards,

Sunita Bose
Managing Director, DIGI
sunita@digi.org.au

[1]Office of the eSafety Commissioner, (16/8/21), *Consultations begin on age verification roadmap*, available at:
https://www.esafety.gov.au/newsroom/media-releases/consultations-begin-on-age-verification-roadmap

Table of contents

Section 1: Scope of services covered under Bill

1. The Bill's proposals must converge with the Privacy Act Review for efficiency and effectiveness

1.1. The Bill and the Privacy Act Review Discussion Paper were launched together on October 25, 2021. This timing implies that the Government sees the two reforms as connected. We understand from roundtable discussions with the Attorney General's Department that the Bill will be introduced to Parliament in early 2022. We also understand, from those discussions, that the next step for the Privacy Act review will be in the form of a report to Government next year, presumably after which the legislation will be developed.

1.2. We understand that the Bill is a result of a pre-election commitment that the Government made on March 24, 2019[2], and there is a desire to pass the Bill ahead of the 2022 election, set to take place before May 2022. However, two and a half years transpired between the announcement of the Bill and the release of the exposure draft on October 25, 2021; this long delay makes it hard to argue for the sudden urgency of the Bill. The fact that the Bill was released on the same day as the proposals for wider Privacy Act Review Discussion Paper, there is an obvious opportunity to converge these two processes for greater effectiveness and efficiency. If the Bill's passage is accelerated ahead of the Review, the ultimate convergence of the two reforms will occur at taxpayer expense; this is not an efficient use of Government resources.

1.3. Furthermore, we do not believe that the Bill's OP Code can constructively be progressed in advance of the broader reform of the Act being settled. The OP Code is required to operationalise certain Australian Privacy Principles (APPs), however there is a high likelihood that the APPs may change while the OP Code is being drafted. Particularly with the short timeframes for code development, it will be unclear to code developers the status of the many areas of overlapping content including notice, consent, and treatment of minors' data. Given the interaction between this Bill and the Privacy Act Review, we strongly urge that these two pieces of fundamentally interlinked reform be converged.

2. The Bill's scope of services does not address its aims

2.1. The Bill proposes the OP Code be binding on three sectors: 1) "social media platforms", "large online platforms" 2) "data brokerage services". While we believe that "social media services" and "large online platforms" have been broadly defined, we question the rationale for the inclusion of these three service types, when there are many other categories of services across the Australian economy that collect minors' data.

2.2. For example, the categories do not explicitly identify education technology, health technology, or the banking sector. Such services routinely collect minors' information, and often market to them. For example, up until 2021, the Commonwealth Bank operated its

[2] Attorney-General & Minister for Communications Minister for the Arts, joint media release (24/03/2019). *Tougher penalties to keep Australians safe online*. Available at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F6577790%22;src1=sm1

"Dollarmites" program which signed up primary school aged children to their bank accounts, in a program that consumer organisation CHOICE has described as "decades of relentless promoting of their financial products to young and impressionable minds"[3]. While that program stopped this year, the Bill does not explicitly cover the development of similar products in the future.

2.3. We acknowledge the possibility that a subset of those services may be classified as "social media services" depending on the level of user interaction enabled, or "large online platforms" depending on the number of end-users. However, the ambiguity around who is covered by the Bill, and who is not, may work against its intention. The goal of Australian privacy reform should be to make systemic improvements that are industry agnostic with a view to restricting certain practices, in an increasingly digitising economy.

2.4. The Bill's approach to in-scope services seems to classify certain services as having a higher risk profile, regardless of whether those entities have implemented data minimisation or anonymisation, or pseudonymisation measures. This approach runs contrary to the affordances given by a regulator to companies that implement reasonable technical and organisational measures to render high risk into low risk processing.

2.5. We therefore see an opportunity to make these improvements in the wider Privacy Act Review that is occurring simultaneously. For example, the Privacy Act Review Discussion Paper puts forward an proposal that DIGI supports whereby:

> *APP entities that engage in the following restricted practices must take reasonable steps to identify privacy risks and implement measures to mitigate those risks:*
>
> - *Direct marketing, including online targeted advertising on a large scale**
> - *The collection, use or disclosure of sensitive information on a large scale*
> - *The collection, use or disclosure of children's personal information on a large scale*
> - *The collection, use or disclosure of location data on a large scale*
> - *The collection, use or disclosure of biometric or genetic data, including the use of facial recognition software*
> - *The sale of personal information on a large scale*
> - *The collection, use or disclosure of personal information for the purposes of influencing individuals' behaviour or decisions on a large scale*
> - *The collection use or disclosure of personal information for the purposes of automated decision making with legal or significant effects, or*
> - *Any collection, use or disclosure that is likely to result in a high privacy risk or risk of harm to an individual.*
>
> **'Large scale' test sourced from GDPR Article 35. Commissioner-issued guidance could provide further clarification on what is likely to constitute a 'large scale' for each type of personal information handling.*[4]

[3] CHOICE. (25/102021). *Commonwealth Bank drops Dollarmites program*, available at: https://www.choice.com.au/money/banking/everyday-banking/articles/commonwealth-bank-drops-dollarmites

[4] Attorney General's Department (25/10/21), *Privacy Act Review Discussion Paper*, available at: https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review---discussion-paper.pdf, p.97

2.6. In contrast to this list in the Privacy Act Review Discussion Paper, the Bill's choice of in-scope services makes a hypothesis about the perceived risk of three service types using different metrics to the list of restricted practices above. That hypothesis is premised around categorisations of service type or end user numbers, rather than the risk of certain practices. This is a limiting approach when we consider that the uptake of the restricted practices above is not limited to the services in scope in the Bill. For example, "large online platforms" does not equate to "large scale data processing"; A small online platform can be a large scale data processor, and vice versa.

2.7. In this context, we question why customer loyalty schemes have been excluded. These operate with a high level of consumer opacity. Customers generally opt-in to such schemes with the expectation that they will be provided with discounts from the service; they do not expect the transaction of their data for other purposes such as third-party advertising. Such schemes are often initiated through the provision of a physical card in a retail environment, and as such there are arguably less points of continuous interaction with the consumer through which privacy information can be communicated, as opposed to "digital first" services. This raises the question: why should a loyalty card scheme initiated in an online shop environment that meets the threshold of a "large online platform" be included, but a loyalty card scheme in a physical store (such as a supermarket or department store) be excluded? If loyalty card schemes are excluded then, by extension, one could argue that subscription-based services otherwise complying with the Bill's requirements should be excluded as a matter of policy.

2.8. The ACCC has recommended in its report into customer loyalty schemes that these schemes improve how they communicate with their members, and that data practices must be improved[5]. While we understand from the consultation roundtables with the Attorney General's Department that the ACCC has a separate process to examine customer loyalty schemes, which has informed the decision to exclude them from the Bill, there are many separate ACCC processes relating to other services in scope in the Bill, such as its inquiry into online marketplaces[6], and digital advertising services[7]. Therefore, this does not provide an acceptable reason to exempt a sector that is engaging in "restricted practices" under the Privacy Act Review. Relatedly, it is also worth emphasising that the ACCC is obviously not the privacy regulator in Australia.

2.9. **In conclusion, it is unclear why *any organisation* that collects minors' personal information should not need to take the highest level of privacy measures under Australian law.** These questions need to be addressed in the wider Privacy Act Review, as opposed to a Bill that focuses on an unclear subset of organisations that is not comprehensive in capturing the practices that the Department is seeking to restrict.

---

[5] ACCC (3/12/2019), *Customer loyalty schemes Final Report*, available at: https://www.accc.gov.au/system/files/Customer%20Loyalty%20Schemes%20-%20Final%20Report%20-%20December%202019.PDF, p. ix

[6] ACCC (22/072021), Media release, *Competition, consumer issues in general online marketplaces to be examined*, available at: https://www.accc.gov.au/media-release/competition-consumer-issues-in-general-online-marketplaces-to-be-examined

[7] ACCC. (2020). *Digital advertising services inquiry*, available at: https://www.accc.gov.au/focus-areas/inquiries-finalised/digital-advertising-services-inquiry

3. If the Bill retains in-scope services, adjustments need to be made to its definitions

Social media services

3.1. It is worth emphasising that the definition of "social media services" in the Bill centres around interaction between two or more end users. This definition is by no means limited to large, mainstream social media services as it encompasses a wide range of services, such as local and small business community forums, educational forums, business forums, health support forums, and any blogs with comments enabled. For example, the mental health organisation Beyond Blue operates a number of online community forums on topics relating to anxiety and depression where Australians can share their experiences and connect[8]. We therefore believe the estimation of 150 companies falling into this category, as put forward by the Regulatory Impact Statement (RIS) is low. Relatedly, the RIS must look beyond the code implementation costs, and also take into account the long-term barriers that the age verification requirement might result in for these wide range of forums; for example, people may not want to provide personally-identifying age verification information when seeking support on a mental health forum, and this may actually negatively impact the uptake and viability of these and other important services over time.

3.2. DIGI is also concerned that there are inconsistencies in definitions across many areas of online safety and privacy reform that create confusion for industry participants. The Bill and its explanatory material advances a different definition of social media services to the definition under the Online Safety Act. The Bill defines "social media services" as:

> *(i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end users, including online interaction that enables end users to share material for social purposes;*
> *(ii) the service allows end users to link to, or interact with, some or all of the other end users;*
> *(iii) the service allows end users to post material on the service;*
> *(iv) such other conditions (if any) as are specified in a legislative instrument made under subsection (7); and*
> *(b) is not specified in, or does not belong to a class of organisations specified in, a legislative instrument made under subsection (7)*[9].

3.3. The Online Privacy Bill Explanatory Paper (The Explanatory Paper) elaborates on this definition indicating that social media services includes:

> *Social networking platforms such as Facebook*
> *Dating applications such as Bumble*
> *Online content services such as Only Fans*
> *Online blogging or forum sites such as Reddit*
> *Gaming platforms that operate in a model which enables end-users to interact with other end-users, such as multiplayer online games with chat functionalities*
> *Online messaging and videoconferencing platforms such as WhatsApp and Zoom*

[8] Beyond Blue, *Online forums*, available at: https://www.beyondblue.org.au/get-support/online-forums
[9] The Bill, p. 6

This definition is not intended to capture organisations that enable online communication/interactions/content sharing as an additional feature – for example, business interactions with customers such as online feedback facilities[10].

3.4. The Online Safety Act defines social media services as:

(1) For the purposes of this Act, social media service means:
(a) an electronic service that satisfies the following conditions:
(i) the sole or primary purpose of the service is to enable online social interaction between 2 or more end-users;
(ii) the service allows end-users to link to, or interact with, some or all of the other end-users;
(iii) the service allows end-users to post material on the service;
(iv) such other conditions (if any) as are set out in the legislative rules; or
(b) an electronic service specified in the legislative rules; but does not include an exempt service (as defined by 19 subsection (4) or (5))[11]

3.5. While this appears similar to the definition in the Bill, it is important to note that the Online Safety Act has a separate category called "relevant electronic services", which encapsulates some messaging services, gaming services and dating services that the Online Privacy Bill defines as social media services. "Relevant electronic services" under the Online Safety Act is defined as follows:

relevant electronic service means any of the following electronic services:

(a) a service that enables end-users to communicate, by means of email, with other end-users;
(b) an instant messaging service that enables end-users to communicate with other end-users;
(c) an SMS service that enables end-users to communicate with other end-users;
(d) an MMS service that enables end-users to communicate with other end-users;
(e) a chat service that enables end-users to communicate with other end-users;
(f) a service that enables end-users to play online games with other end-users;
(g) an electronic service specified in the legislative rules.[12]

3.6. To add further confusion for the industry, the eSafety Commissioner's recent position paper, released September 29, 2021[13], elaborates on the definitions in the Online Safety Act as they relate to the development of the OSA Codes and provides the following exemplification of the two definitions:

---

[10] Attorney General's Department, *Online Privacy Bill Explanatory Paper*, (25/10/2021), available at: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf, p. 7
[11] Online Safety Act, Section 13, available at https://www.legislation.gov.au/Details/C2021A00076
[12] Online Safety Act, Section 13A
[13] Office of the eSafety Commissioner, *Development of industry codes under the Online Safety Act: Position Paper*, available at https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper, p. 33

	Section of the online industry	***Scope***
Social media services	*Providers of social media services, so far as those services are provided to end-users in Australia*	*All providers of social media services that can be accessed by end-users in Australia, including:* *- social networks* *- media sharing networks* *- discussion forums* *- consumer review networks*
Relevant electronic services	*Providers of relevant electronic services, so far as those services are provided to end-users in Australia*	*All providers of relevant electronic services that can be accessed by end users in Australia, including:* *- email services* *- instant messaging services* *- SMS and MMS services* *- chat services* *- online games where end-users can play against each other* *- online dating services.*

3.7. It is therefore unclear whether online dating services, gaming and messaging services are considered to be "social media services" or "relevant electronic services". The industry needs consistency in definitions, across digital industry regulations which will assist in the implementation of the legislation, as privacy regulation informs companies' privacy management plans. The Online Safety Act will come into force on January 23, 2022, and work is currently being led by industry associations including DIGI to register the first set of OSA codes in July 2022. Given that timeframe preceded the timeframe for the Bill, we suggest that the Bill and any ensuing guidance for the OP Code released by the OAIC be amended for consistency with the definitions under the Online Safety Act.

3.8. We also encourage a definition of "end users", to support the definition of "social media services", for reasons we explain below.

Large online platforms

3.9. With regard to both "social media services" and "large online platforms", further thought needs to be given to the definition of "end user". The Explanatory Paper says that "an end-user is any individual who uses the electronic service". This is far too broad, such that it captures end users who might simply visit a website, perhaps after discovering it

from a search engine, without the provision of any of their personal information. For example, an end user may search for a particular piece of information, locate the information on a platform, and then navigate away; currently the Explanatory Paper's definition would capture such a user, and we believe such users should not be included in determining an appropriate threshold for large platforms. We would recommend a focus on *registered users* from whom personal information is collected, such as an email address.

3.10. Per the previous section, we encourage more holistic cohesion to standardise privacy protections economy-wide. However, should the Bill capture large online services, further thought should be given to commonly used user metrics used within the technology sector such as "Monthly Active Users" (MAU). For example, the ACCC's Digital Platforms Inquiry final report used 1 million MAU in its recommended threshold for companies it hoped might adopt the voluntary disinformation code[14]. Often total, unregistered user numbers are considered a "vanity metric" in the technology sector, and are not indicative of the depth of user interaction and therefore possible information collection.

3.11. Our expectation is that, without a refinement of the definition of "end-users", the estimation put forward in the RIS that the category "large online platforms" may cover more than the 500 organisations is underestimated. This definition also impacts the calculation of "social media services" which, as mentioned, we also believe has been underestimated.

Summary of recommendations in Section 1

A. The Bill's proposals must converge with the Privacy Act Review for efficiency and effectiveness.

B. Should the Bill proceed independently of the Privacy Act Review, it should focus on "restricted practices" under the Privacy Act Review Discussion Paper, rather than the current scope of services. This will ensure that any organisation that collects minors' personal information takes the highest level of privacy measures under Australian law.

C. If the scope of services under the Bill is retained, we recommend resolution of the inconsistencies between the definitions under the Bill, the Online Safety Act, and the guidance material for the OSA Codes. We urge that the Bill and any ensuing guidance for the OP code released by the OAIC be amended for consistency with the definitions under the Online Safety Act.

D. If the scope of services under the Bill is retained, we recommend defining large online platforms and social media services in relation to *registered users* from whom personal information is collected, rather than end users.

[14] ACCC (2019), *Digital platforms inquiry - final report*, available at: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report, p. 34

Section 2: Age verification

4. Age verification requirements will see Australians sacrifice privacy in efforts to protect it

4.1. The Bill's age verification requirements run counter to the universally accepted privacy practice of data minimisation. Data minimisation requires goods or service providers to not seek to collect data beyond what is reasonably needed to provide the good or service. The final Bill must safeguard the cyber security and personal information of Australian Internet users. If the focus on *age verification* is retained, as opposed to *age assurance*, it will encourage the widespread collection of identity verification documentation such as drivers' licences, and documents that prove guardianship, such as Medicare cards and birth certificates. This runs counter to the universally accepted privacy best practice of data minimisation that forms part of the existing APPs under the Privacy Act 1988 (cth)[15]. Data minimisation is also a key principle of the Consumer Data Right[16].

4.2. It is also unclear whether Australians have the propensity to provide this information, and whether it will serve as a barrier to their uptake of a broad range of digital services. Further research must be undertaken to understand Australian consumer views on their willingness to participate in an age verification process as a precursor to the use of digital services, before the Bill is progressed in its current form.

Requirement to "take all reasonable steps to verify the age of individuals"

4.3. It is concerning that the Bill has adopted the language of "age verification" rather than "age assurance". *Age verification* is the most privacy-intrusive form of *age assurance*. If the requirement to "take all reasonable steps to verify the age of individuals" equates to identity verification, through the provision of drivers' licences, passports or other Government issued identification documents, the privacy intrusion of the Bill will be immense.

4.4. In April 2021, the United Nations Children's Fund (UNICEF) released a discussion paper, titled "Digital Age Assurance, Age Verification Tools, and Children's Rights Online across the Globe: A Discussion Paper"[17], which examines age assurance tools and provides a useful account of the available methods. This discussion paper identifies the main potential data sources and methods for age assurance tools, which are: State or government-provided, user-provided data such as official documents, automatically generated data, biometric data, blockchain and self-sovereign identities, behavioural and self declaration.

---

[15] OAIC, *Australian Privacy Principles*, available at: https://www.oaic.gov.au/privacy/australian-privacy-principles, aee APP 3 and APP 11.
[16] https://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/chapter-3-privacy-safeguard-3-seeking-to-collect-cdr-data-from-cdr-participants/
[17] UNICEF, (2021), *Digital Age Assurance, Age Verification Tools, and Children's Rights Online across the Globe: A Discussion Paper*, available at https://c-fam.org/wp-content/uploads/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-across-the-Globe.pdf

4.5. Interestingly, the paper notes that "age verification tools that use centralized data sources often connect to large data aggregators and credit rating agencies such as Experian and Equifax"[18]. Given the Bill intends to cover data brokerage services such as Experian and Equifax in scope, there is a circularity should these be the verification methods ultimately contemplated.

4.6. In relation to state or government methods of age verification, we seek clarity as to whether the Government's "Digital Identity"[19]solution is being contemplated as a solution for industry. DIGI understands from our attendance at a webinar on the Trusted Digital Identity Bill, held on October 15 2021 and hosted by The Digital Transformation Agency, that the Government's intention is for this program to be rolled out to the private sector[20].

4.7. In its assessment of each of these age assurance methods, there are still privacy concerns about the additional collection of personal information associated with all. The UNICEF report examines each age assurance approach against the United Nations Convention of the Rights of the Child (CRC). Article 16 of the CRC focuses on the right to privacy states:

Most age assurance tools with a high degree of accuracy rely on official data that can easily identify a child. It is important that children's right to privacy is respected as they continue to engage in online spaces, and that they are only identified where strictly necessary to prevent serious harm, and with their consent or the consent of their parents or caregivers[21].

4.8. The paper raises the need for age assurance processes to respect the data minimisation principle, and this is one of the fundamental challenges related to this proposal where we need a balanced approach. DIGI notes that self-declaration is the most common age assurance method used by the digital industry, which optimises for data minimisation and usability at the risk of accuracy.

4.9. It is also important to note questions of scope, raised earlier, in relation to this point. The Bill's definition of social media services is around services that enable "online social interaction between two or more end-users, and allows interactions between end-users, and allows end-users to post material on the service". This captures any website or community forum that enables comments; it is not restricted to large social media companies that will have more resources and internal expertise to ensure the cyber security of the additional data collection.

---

[18] UNICEF, p. 20

[19] Digital Transformation Agency (2021), *Digital Identity Australian Government*, available at: https://www.digitalidentity.gov.au/ .

[20] Digital Transformation Agency (2021), *Consultation on the exposure draft of the Trusted Digital Identity Bill and related legislative instruments*, available at https://www.digitalidentity.gov.au/have-your-say/phase-3?utm_source=Webinarf-up261021&utm_medium=Email&utm_campaign=Exposure+draft+%28phase+3%29&utm_id=Exposure+draft+%28phase+3%29&utm_source=Digital+identity+legislation+exposure+draft+stakeholder+list+27+Sept&utm_campaign=c7441697bb-EMAIL_CAMPAIGN_2020_11_11_04_05_COPY_01&utm_medium=email&utm_term=0_f63ad4c26c-c7441697bb-183943985

[21] UNICEF, p.11

4.10. In addition to the cyber security capacity of the broad number of services in scope, consideration also needs to be given to the volume of additional data collection on those websites which is likely to run counter to consumer expectations: do consumers want to routinely provide their personal information, age data, and potentially identity verification documents when they are perusing websites that include user interaction? On the basis that this represents a significant change in the ability to access digital services from within Australia, our hypothesis is that consumers will have legitimate and serious concerns with providing sensitive identification documents as a precursor to accessing digital services, and we recommend that this be explored with Australian-specific research before the Bill is advanced. We also consider there to be a real risk that Australians will increasingly use masking technologies such as VPNs in order to circumvent these identity requirements.

Requirement to "obtain parental or guardian express consent before collecting"

4.11. The privacy intrusion of the Bill is multiplied by the requirement to obtain parental or guardian express consent before collecting information. Not only could this require additional collection of personal information from additional end users, it may require the collection of secondary documents to verify parental status or guardianship. For example, there are many parents or guardians who do not have the same last name as their children. This may be because their children have the last name of their spouse, due to adoption, or for legal guardians who are not biological parents. Is the Government expecting parents to provide a birth certificate, Medicare card or other identification in order to demonstrate their guardianship of a particular minor? This would increase the amassing of personal identification documents at the platform level.

4.12. Neither the Bill, nor the Explanatory Paper, contemplate scenarios where a young adult may require access to digital services outside of the purview of their legal guardian, such as to access assistance or health information. This is particularly relevant in situations where the minor's relationship with their guardian may be constrained.

4.13. This is one of several concerns identified in the UNICEF Discussion Paper in relation to the CRC's Article 2 concerning non-discrimination, where it states:

It is important that age assurance processes do not inadvertently discriminate against children who do not have access to official documents, children with developmental delays, children whose ethnicity is not recognized by algorithms used to assess age, or children who do not have parents or caregivers who are able to engage with verification processes that require parental input.

4.14. The UNICEF discussion paper also discusses Article 5 of the CRC, which focuses on parental guidance and a child's evolving capabilities where it states: "It may be difficult to reconcile age-based restrictions with the concept of the evolving capacities of the child." Consideration needs to be given to the varying impact of the Bill on young adults, not just children.

4.15. One way to ensure parents can make decisions based on the evolving capabilities of minors in their care is through increasing the prevalence and uptake of parental controls that give parents visibility about children's online activity, and opportunities to intervene; DIGI members have extensive experience in developing and implementing such controls.

At the service provider level, Apple[22] and Google[23] provide applications to enable family sharing and limitations on minors' phones and tables, that include controlling their privacy settings, filtering access to content, screen time limits and other features designed to safeguard minors' privacy and experiences online. At the search engine level, Google's Safe Search filter[24] prevents search results containing or promoting nudity, sexually suggestive content, adult entertainment and other services from appearing within search results. At the app distribution level, restricted profiles can be established where more mature content can be filtered out of the app store. On browsers, such as Chrome, parents can create restricted profiles for minors that allow parents to block and approve sites viewed, and Safe Search is on by default in such accounts. At the platform level, there are similar "safe search" settings that hide sensitive content and remove blocked and muted accounts. There are also default privacy settings for minors; for example, Instagram defaults users between the ages of 13 and 17 into private accounts upon sign-up, and uses a number of safety measures for users in this category, including making it harder to adults to comment or interact with them, steps to inhibit inappropriate interactions with adults in private messaging, and preventing teens from seeing age-sensitive ads[25]. On Snapchat, default settings for *all users* prevent receiving a message from someone who is not your friend and location sharing is off by default, and there is no option for users to share location outside of their friend group.

4.16. We recommend that the parental consent and verification requirement be reconsidered in favour of other Government and industry measures to increase the prevalence and uptake of parental controls. The forthcoming OSA codes, to be registered by the Office of the eSafety Commissioner in 2022, are expected to cover in scope the tools available to parents to manage and oversee their children's experiences online. DIGI and the Communications Alliance, supported by a steering group of other industry associations, are developing the new mandatory codes of practice to regulate all online services and websites available in Australia, which will be registered by the Office of the eSafety Commissioner in 2022. In subject matter, the codes will relate to "Class 1" and "Class 2" materials under Australia's classification code. Class 1 materials include child sexual exploitation material, pro-terror content, content that depicts, promotes, incites or instructs in matters of crime, violence or drug misuse, and online pornography that depicts fetish practices or fantasies. Class 2 materials include other online pornography, X18+ and R18+ content, and material which includes high-impact sex, nudity, violence, drug use, language and themes; 'Themes' includes social Issues such as crime, suicide, drug and alcohol dependency, death, serious illness, family breakdown and racism. At a high level, the codes will contain commitments from industry to minimise the risk of harm to all Australian end-users due to the accessibility of Class 1 materials online. The OSA

[22] Apple Support, *Use parental controls on your child's iPhone, iPad, and iPod touch*, available at: https://support.apple.com/en-us/HT201304
[23] Google, *Google Family*, available at: https://families.google.com/familylink/
[24] Google Search Help, *Filter explicit results using SafeSearch - Android - Google Search Help*, available at https://support.google.com/websearch/answer/510?hl=en&co=GENIE.Platform%3DAndroid. NB. Safe search will soon be turned on by default for all under 18 year old users in Australia.
[25] See the following links for more information: Youtube, *YouTube - More choices for families*, available at https://www.youtube.com/myfamily/; Meta, *New Teen Safety Features and 'Take a Break' on Instagram*, available at https://about.fb.com/news/2021/12/new-teen-safety-tools-on-instagram/; Twitter, Understanding and obtaining parental consent to use Twitter, available at https://help.twitter.com/en/using-twitter/parental-consent

Codes will also contain commitments from industry to minimise the risk of harm to Australian minors due to the accessibility of Class 2 materials online.

4.17. The OSA codes will apply to eight sections of the industry, namely: providers of social media services (defined around online social interaction between 2 or more end-users), providers of relevant electronic services (includes any services with messaging, and gaming), providers of designated internet services (includes all websites), providers of internet search engine services, providers of app distribution services, providers of hosting services, providers of internet carriage services, and persons who manufacture, supply, maintain or install certain equipment (includes retailers). This is broader in scope than the Bill's requirements pertaining to age and guardian verification, which are limited to social media services. These therefore provide a "whole of system" approach to the issue.

4.18. Opportunities to explore appropriate avenues for age verification also exist under the Office of the eSafety Commissioner's Age Verification roadmap (AV Roadmap). We understand that the Office will undertake an engagement process with key stakeholders to analyse insights to inform the AV Roadmap. While details of this engagement process are yet to be released at time of writing, this arguably provides a more considered and consultative avenue to weigh the challenges and issues presented by age verification, than an attempt to hastily legislate the issue by way of this Bill in the two parliamentary sitting weeks that remain prior to the 2022 federal election. The consequences of this Bill for Australians at large, minors, guardians, as well as a broad scope of industry participants, must be fully considered. We request a coordinated whole of Government approach, where these issues are examined through a lead process, such as the Age Verification roadmap, which avoids duplicative Government process and unnecessary taxpayer expense.

5. The Bill's widespread use of age verification is globally unprecedented in democratic countries

5.1. Proposals around age assurance have primarily been explored in the EU, UK and China[26] The EU's Audio Visual Media Services Directive (AVMSD) contemplates age verification as a possible measure "for users of video-sharing platforms with respect to content which may impair the physical, mental or moral development of minors"[27]. It does not contemplate the universal application to broadly scoped "social media services" that enable user interaction.

5.2. Nor does the UK's Age Appropriate Design Code (AADC), which provides a useful model when considering the questions raised by the Bill, and the resulting code. This code came into force on September 2, 2020 with a 12 month transition period where organisations must confirm by September 2, 2021. The code sets out 15 standards, many of which overlap with the principles of the Bill, however it is noteworthy that the standards do not include age verification, but rather elevate the standard of data minimisation. On the topic of age assurance, the AADC guidance material states:

[26] UNICEF, p. 8.
[27] European Union (2018), *Audio Visual Media Services Directive*, available at https://eur-lex.europa.eu/eli/dir/2018/1808/oj

We recognise there is a tension between age assurance and compliance with GDPR, as the implementation of age assurance could increase the risk of intrusive data collection. We do not require organisations to create these counter risks. However, age assurance and GDPR are compatible if privacy by design solutions are used[28].

5.3. The only country, to our knowledge, that has legislation requiring the widespread collection of identity verification, to our knowledge, is China; Under a series of laws, passed in 2017, Internet users in China must provide national identity documents and real names on a wide range of digital services[29].

5.4. Research must be undertaken on age verification in other comparable countries, and an analysis should be published, ideally through the AV Roadmap process. This should include issues that arose with the implementation of the United Kingdom age verification scheme. It is worth exploring the UK Government's announcement in October 2019 that it would not proceed with Part 3 of the Digital Economy Act 2017 concerning age verification for online pornography after undertaking an extensive consultation process over several years. The scheme was criticised for being easily circumvented and raised considerable concerns around user privacy. The UK's Online Safety Bill, published earlier this year, appears to focus instead on access restrictions.

6. The Bill's approach to age limits is inconsistent with the US and EU

6.1. The first data protection law to set a digital age of consent for users was the Children's Online Privacy Protection Act (COPPA) in the US, which set the minimum age at 13.

6.2. In the EU, the GDPR introduced on May 25, 2018, set the digital age of consent at 16, giving member states the option to lower this to age 13. In practice, the majority of EU member states have settled on lower ages as the age of consent, with only a third opting to retain 16 as the appropriate age.

6.3. These two laws have been influential in relation to why most globally-accessible digital services have age restrictions between 13 and 16 in place.

6.4. The Bill's requirements for social media services centre around a child being 18 years of age, and require parental consent for those under 16 years of age. Especially given the broad scope of services under the Bill's definition of "social media services", there is a question as to whether the Bill results in the exclusion of young people from digital services offering interaction.

6.5. From an implementation perspective, digital services which are generally globally accessible, require consistency and interoperability with the relevant laws in major markets such as the US and EU.

---

[28]UK Information Commissioner's Office (2020), *Age appropriate design: a code of practice*, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf, p. 35

[29] Samm Sacks & Paul Triolo (25/9/2017), *Shrinking Anonymity in Chinese Cyberspace - Lawfare*, available at https://www.lawfareblog.com/shrinking-anonymity-chinese-cyberspace

6.6. We therefore recommend the Bill utilise the age requirement of 15 or 16 throughout, rather than 18, for consistency and interoperability with the GDPR. Setting the age limit at 15 would be consistent with current guidance from the OAIC in relation to children and young people. That guidance states: "If it's not practical for an organisation or agency to assess the capacity of individuals on a case-by-case basis, as a general rule, an organisation or agency may assume an individual over the age of 15 has capacity, unless they're unsure."[30]

7. The Bill's expansion to cover age verification was unforeseen and requires further consultation

7.1. The media release when the Bill was announced on March 24, 2019, did not make any mention of age verification. The media release also indicated that "legislation will be drafted for consultation in the second half of 2019", which has clearly been delayed by over two years[31].

7.2. Nor was the expansion of the Bill to cover age verification mentioned when the Attorney General's Department was asked about the Bill during, hearing during the Select Committee on Foriegn Interference through Social Media held on July 30, 2021, excerpted below:

Ms Julia Galluccio, Assistant Secretary, Information Law Branch, Attorney-General's Department: I'll also just note that in addition to the Privacy Act review, we are also separately working on exposure draft legislation that will specifically target social media companies and certain other online platforms, with similar themes in terms of ensuring that there's greater transparency about how personal information is being used and how consent is obtained, particularly from young people as well. So we're in the process of finalising that legislation at the moment, and that will also be released for public discussion as well[32].

7.3. As such, we do not believe that there has been due consultation on the propensity of Australians to undertake age verification as a pre-requirement to use digital services. Nor do we believe there is an understanding from Australians that this Bill will require such a fundamental change to how they use the Internet.

7.4. As a result of the seemingly late inclusion of age verification in the scope of the Bill, the Bill lacks, or has not presented, evidence based on the effectiveness of age verification and young people's use of digital services. Meaningful consultation must take place with

[30] OAIC, *Children and young people*, available at https://www.oaic.gov.au/privacy/your-privacy-rights/children-and-young-people

[31] Attorney-General & Minister for Communications Minister for the Arts, joint media release (24/03/2019), *Tougher penalties to keep Australians safe online*. Available at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F6577790%22;src1=sm1

[32] Select Committee on Foreign Interference through Social Media (30/07/2021), Transcript available at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22committees%2Fcommsen%2Fba9940d8-9927-4124-95fd-e22a48306943%2F0000%22

children and young adults, as well as the organisations that serve and research them, to ensure the final Bill is evidence-based.

7.5. With regard to the Bill's focus on "the best interests of the child", in some instances it may be best to restrict a minor from a service, however in other instances it might be in the best interests of the child to have access to a digital service. Parents or guardians can make judgements on what's in the best interests of the child, not platforms, because platforms rightly do not have that knowledge. Therefore, platforms may simply opt to remove young people from digital services, which may be to the detriment of certain young people.

7.6. As well as the impact on Australians and young people, the staggering cost of age verification this exercise requires pause and further evaluation. The RIS estimates the verification requirements of the Bill will have an implementation cost of $526,203,500, which is 99% of the total implementation cost of the Bill of $530,153,678.75. As we note elsewhere in this submission, we also have reason to estimate that some elements of the RIS have been underestimated.

7.7. We therefore recommend that the age verification requirements be removed from the Bill, and that this issue be further explored and consulted upon through the Office of the eSafety Commissioner's existing AV roadmap, which we understand is due to report back to Government in 2022.

7.8. If there is unwavering insistence by the Government that these be retained, DIGI encourages the consideration of age assurance mechanisms already in existence that are compatible with the principle of data minimisation. Specifically, we ask that the Bill's language of "age verification" be replaced with the terminology "age assurance".

8. The need for a whole-of-Government approach

PM&C Digital Economy Strategy

8.1. The Australian Government has set a goal that Australia will be a leading digital economy by 2030, in a Digital Economy Strategy led by the Department of the Prime Minister and Cabinet (PM&C). As we work towards that goal, we need to be acutely aware that Australia is starting this race from behind, with the second smallest technology sector in the OECD[33]. As noted, the age verification requirements in this Bill are globally unprecedented in democratic nations. By impeding the usability of digital services, through erecting age verification barriers that Australian may not be willing to undergo, This Bill will have a significant impact on Australia's ability to meet its goals under the Digital Economy Strategy[34].

[33] AlphaBeta (September 2019), *Australia's Digital Opportunity*, available at: https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf
[34] Department of the Prime Minister and Cabinet (PM&C), *Digital Economy Strategy,* available at https://digitaleconomy.pmc.gov.au/

8.2. For example, the Digital Economy Strategy aims for 95% of SMEs to use eCommerce tools, and has a goal relating to all new businesses being 'born' digital[35]. It is our expectation that many of the tools that SMEs might use to support and market their businesses fall in scope in the Bill and, for social media services, requirements for age verification will provide a barrier to entry.

8.3. There is a further compromise to the Digital Economy Strategy's goal that "All Australian businesses continue to improve cyber security practices", which we detail below.

Department of Home Affairs' Cyber Security Strategy

8.4. If the Bill proceeds as drafted, there is a reasonable assumption that these reform programs will likely require potential additional data collection on the part of in-scope services in Australia including age data, perhaps including drivers' licenses or other documentation. DIGI predicts that this potential increase in data collection for all websites will cause widespread cyber security risks to a whole range of websites in Australia.

8.5. As the eSafety Commissioner said in an interview with InnovationAus on age verification and cyber security: "If you don't balance the privacy, the security and the safety imperatives, it's not going to work… If you're creating a honeypot of really sensitive information, it's not going to work.[36]"

8.6. We encourage the Attorney General's Department to consult with the Department of Home Affairs to determine how the Bill aligns with their work program to strengthen Australia's cyber security regulations and incentives.[37]

8.7. Additionally, we encourage the Attorney General's Department to consult with the Australian Cyber Security Centre in the Australian Signals Directorate, the Department of Prime Minister & Cabinet and the Department of Communications on the age verification requirements of the Bill. We welcome acknowledgement that such consultation will occur in the RIS.

8.8. We urge a whole-of-Government approach to assess where reforms in different areas might undermine cyber security in Australia.

---

[35]Department of the Prime Minister and Cabinet, *Digital Economy Strategy on a page*, available at https://digitaleconomy.pmc.gov.au/sites/default/files/2021-05/digital-economy-strategy-on-a-page.pdf

[36] InnovationAus, (15/09/21), *The UK failed with age verification for porn. Now Australia's trying it*, available at https://www.innovationaus.com/the-uk-failed-with-age-verification-for-porn-now-australias-trying-it/

[37] Department of Home Affairs, (13/07/21), *Strengthening Australia's cyber security regulations and incentives*, available at https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-regulations-incentives

PM&C Deregulation Agenda

8.9. The Government has made a $120 million investment in its "Deregulation Agenda", overseen by PM&C[38]. As part of that agenda, it released a Regulator Performance Guide that came into effect from July 1, 2021. The guide states that "Best practice requires that regulators consider, and aim to improve on, the combined regulatory burden of governments on business and the community.[39]"

8.10. Consideration must be given to whether age verification requirements under the Bill help or hinder the Government's Deregulation Agenda, alongside the many other unintended consequences outlined in this submission. Per the RIS, the Department estimates that there will be a one-off code development and implementation cost of over half a billion dollars ($530,153,678.75) as well as ongoing regulatory costs of $7,943,457 per year, with 99% of the implementation cost owing to the age verification requirement.

Office of the eSafety Commissioner's Age Verification roadmap

8.11. As noted, we recommend that the Office of the eSafety Commissioner's existing roadmap on age verification (AV Roadmap) – that was a result from Government's parliamentary inquiry into age verification for online wagering and online pornography – provides an appropriate avenue for further exploration of age verfication. DIGI has engaged in consultations for the AV roadmap, and we understand that consultations are continuing and that the AV roadmap will be presented to the Government in 2022[40]. Further exploration of age verification within the context of the AV roadmap would signal a whole-of-Government approach that is prudent with taxpayer funds, as opposed to legislating for widespread age verification in the absence of due consultation on the issue, and in advance of an existing Government work program on the issue.

[38] Department of the Prime Minister and Cabinet (20/04/2021), *Deregulation agenda removing business red tape and lifting regulator performance*, available at https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22media%2Fpressrel%2F7917440%22;src1=sm1

[39] Department of the Prime Minister and Cabinet (01/07/2021), *Regulator Performance Guide and supporting material*, https://deregulation.pmc.gov.au/priorities/regulator-best-practice-and-performance/regulator-performance-guide

[40] Office of the eSafety Commissioner (16/8/21), *Consultations begin on age verification roadmap*, available at https://www.esafety.gov.au/newsroom/media-releases/consultations-begin-on-age-verification-roadmap

Summary of recommendations in Section 2

E. Further research must be undertaken to understand Australian adults, minors and parents' views on their inclination to provide age and identity information (beyond self-declaration) as a precursor to the use of digital services.

F. We recommend that the age verification requirements be removed from the Bill, and instead explored in a more consultative way through the AV roadmap, being led by the Office of the eSafety Commissioner.

G. If the age verification requirements cannot be removed from the Bill, DIGI asks that the language of "age verification" be replaced with the terminology "age assurance".

H. Research must be undertaken to implement schemes for age verification in other countries, and an analysis published of the experience of comparable democracies with age verification solutions, as part of the AV Roadmap or otherwise.

I. We recommend the Bill utilise the age requirement of 15 or 16 throughout, rather than 18, for consistency and interoperability with the GDPR.

J. We encourage the Attorney General's Department to adopt a whole-of-Government approach and to consult with the Department of Home Affairs, the Australian Cyber Security Centre in the Australian Signals Directorate, the Department of Prime Minister & Cabinet and the Department of Communications on the age verification requirements of the Bill.

Section 3: Code development process

9. The need for multiple codes to cover the diversity of industry participants

9.1. The Bill allows for the creation of one OP Code to cover three diverse industry sections. As noted in Section 1 of this submission, the three categories of organisations in scope in the Bill are expansive and diverse, and we recommend the best solution to standardise protections across these sectors and economy-wide is through the Privacy Act Review.

9.2. However, should the Government pursue the Bill in its current form, the Bill needs to be updated to allow for more than one OP Code.

9.3. Noting the inclusion of the data brokerage sector, DIGI is unaware of industry bodies that represent this sector in full. We expect that the data brokerage will have a different set of issues to the social media services sector, for example, which is arguably more "front of house" and B2C and has more opportunities for privacy notices with users. By contrast, the data brokerage sector is more "back of house" and B2B, and will have a different level of engagement and opportunities for privacy communication with the consumer. It is hard to imagine how the same industry code could apply to these two different sectors.

9.4. To our knowledge, there is no overlap in industry representation. DIGI's membership consists of social media services and large online platforms, as defined under the Bill; none of our members would identify as data brokerage firms.

9.5. Based on the Bill's thresholds, and evidenced by the diverse industries represented at the Bill's consultation roundtables (that included representatives from the news media and insurance industries, as two examples), there will be a diversity of sectors covered under the codes.

9.6. We note that the OSA codes enable the development of multiple codes. The Office of the eSafety Commissioner's Position Paper does not prescribe a number of codes, though encourages a few codes as possible as a criteria for her registration of the OSA codes[41].

9.7. We note that the Regulatory Impact Statement (RIS) estimates that the cost to OP code developers, being industry associations, will likely be $882,078.75. Industry associations like DIGI are usually non-profit organisations that are incredibly lean in size. There is no existing funding for this, so we must ensure both in questions of scope and process that we make this less costly for industry associations. In our experience with the OSA Codes – where DIGI has been undertaking broad consultation with a wide range of companies outside of our membership, and additionally coordinating through a steering group of six industry associations – the cost and workload for industry associations increases with the level of work. Increasing the number of acceptable codes will minimise the amount of coordination outside a clear industry section.

9.8. This will also serve to increase the specificity and applicability of the codes within an industry section. There is a risk that, in an effort to find common ground between highly diverse industry sections, that the OP Code becomes watered down to the lowest common denominator. The Bill and the OAIC's ensuing guidance should set the code development process up for success so that this does not occur.

10. The need for more time for code development, and appointment and implementation periods

10.1. We note that the RIS states that: "The OP code must be developed and registered within 12 months of the Online Privacy Bill passing and receiving Royal Assent." Based on our direct experience of comparable code development, we would request a minimum of 12 months after the date of which the OAIC provides the code developer with regulatory guidance.

10.2. In our direct experience with the OSA code timeline, we are finding the timeline extremely tight. The Online Safety Act passed parliament on June 23, 2021. The Office of the eSafety Commissioner released a position paper that offered guidance to the code developers on September 29, 2021, and is required to register the first of the codes by July 22, 2022. DIGI and the associations involved in this effort are working overtime to deliver high quality codes in a consultative and comprehensive manner. This is in addition to a full workload of engaging in Government consultations for which industry

[41] Office of the eSafety Commissioner, Development of industry codes under the Online Safety Act: Position Paper, p. 54

associations have no control over the volume nor the timing of those consultations. At time of writing, DIGI is engaging in at least ten open distinct Government consultations, in addition to our co-leadership of code development work under the OSA, and our oversight of the *Australian Code of Practice on Disinformation and Misinformation*.

10.3. Using our OSA Codes work as a guide, outlined below are the expected phases of code development and the *minimum* timeframe required:

Minimum timing	Action
13 weeks	Establish association steering group, ToRs, identify in-scope companies and associated outreach, formulate working groups.
13 weeks	Develop draft code(s), consolidation and consistency within working groups.
3 weeks	Regulator to consider a pre-public comment version of the code(s).
4 weeks	Refine draft code(s), incorporate regulator feedback. Develop public consultation plan and outreach lists.
5 weeks	Public consultation period.
6 weeks (assuming 1 public comment)	Consideration of and response to public comment input, and updating of code(s).
2 weeks	Association approvals.
9 weeks	Compilation of code(s) development methodology and consultation, registration document.
4 weeks	Regulator consideration of code(s) for registration.

10.4. Furthermore, we understand that the OAIC will undertake a code developer identification process to identify and appoint the industry associations undertaking the code. We ask that the time period for this process be outside of the 12 months; we would be amenable to clarity on the process being shared ahead of the passage of the Bill to enable this time.

10.5. This is particularly important given the broad scope of organisations expected to be covered under the code and, in our direct experience, it takes time for different industry associations to both determine whether they will be able to play a code developer role, and to develop a coordination mechanism with other associations. For the OSA codes, a steering group was formed which includes the Australian Mobile Telecommunications Association (AMTA), BSA | The Software Alliance, the Communications Alliance (CA), the Consumer Electronics Suppliers' Association (CESA), the Interactive Games & Entertainment Association (IGEA) and DIGI. The group assigned lead associations for the drafting of sections of the codes that best aligned with their membership, and coordinate around other functions associated with the project under an agreed Terms of Reference.

10.6. The more time that is afforded, the more consultative and evidence-based the code development process can be. As an indication of a timeline where the timeline was more flexible, and therefore consultative, we include a case study below of DIGI's timeline and process for the development of *The Australian Code of Practice for Disinformation and Misinformation*. We note that, as a voluntary code, this process did not require registration with the ACMA. This experience informs our recommendation that the code

developer be provided 12 months from the date from which the regulator is able to release their guidance

Case study: DIGI's process for the Australian Code of Practice for Disinformation and Misinformation[42]

Phase 1: Agreement, resourcing & partner engagement

- In March 2020, DIGI reached agreement within its membership that it would lead the development of this process.
- In April, DIGI contracted University of Technology Sydney's Centre for Media Transition (UTS CMT) and First Draft as key academic and civil society partners to support the development of the Code. UTS CMT is an interdisciplinary research centre that investigates key areas of media evolution and digital transition. First Draft is a global organisation that empowers societies with the knowledge, understanding and tools needed to outsmart false and misleading information.
- DIGI also convened a wider industry committee of potential signatories, outside of DIGI's current membership, to support the development of the code.

Phase 2: Issues mapping

- The Government tasked the ACMA with oversight of the code on December 11, 2019 and on June 26, 2020, the ACMA released a discussion paper outlining its expectations of the code.
- UTS and First Draft interviewed members of the industry committee, and conducted research into disinformation and misinformation in Australia. They also conducted a review of regulatory responses in different jurisdictions, and industry responses to the challenges.
- This research was released publicly as a discussion paper. This discussion paper and the ACMA's discussion paper were used to inform the development of the draft code.

Phase 3: Initial draft development

- A draft code of conduct was developed, and refined with input from the industry committee for comment over the course of August and September.

Phase 4: Public consultation

- On October 19, a six week public consultation was launched ending on November 24, 2020.
- The code was made publicly available on the DIGI website, and was open for submissions from the general public.
- During this consultation, DIGI, UTS and First Draft proactively identified interested civil society, consumer and academic stakeholders. They were emailed the draft code and invited to comment.

[42] DIGI has made much of the information in this case study publicly available in a report about the code's public consultation process. DIGI (22/02/2021), *Submission report: Australian Code of Practice on Disinformation and Misinformation*, available at https://digi.org.au/wp-content/uploads/2021/02/DIGI-Submission-report-ACPDM-Feb-22-2021-FINAL.pdf

- To provide an avenue for dialogue between academia and representatives of civil society, a smaller subset of this group was also invited to offer their views on the Code at a virtual roundtable meeting on 30 October 2020, facilitated by UTS and First Draft.

Phase 5: Revisions and final report

- All submissions were closely reviewed.
- Input from submissions was summarised into a report, later updated to indicate where the feedback had been reflected.
- Input was also sought from the ACMA.
- Over the course of December and January, the draft code was updated to reflect all stakeholder input.

Phase 6: Adoption

- In order to adopt a code, potential signatories must undertake an internal approval process, generally involving cross-functional institutional review, in order to determine whether they can become official signatories.

Phase 7: Launch

- Prior to launching the final Code, DIGI reconvened attendees of the October 30, 2020 roundtable with all submission authors for an additional roundtable meeting. This final roundtable meeting, held on 19 February 2021, aimed to report back to the people and organisations that contributed a submission, as well as other identified experts in academia and civil society.
- After the initial development of the code and launch of the code, a system for the ongoing administration of the code must be developed and maintained.

Phase 8: Governance of the code

- The final code is required before an appropriate governance model can be developed.
- After the code's launch, DIGI used that to research and develop an appropriate governance model, with the appointment of independent experts. This was launched on October 11, 2021.

Implementation period

10.7. We need to build in time for legislation for industry participants to implement compliance measures. As any company that has implemented the GDPR will attest, ensuring compliance is a significant cross-functional undertaking within a company and requires a minimum of six months to implement, taking into account the varying sizes, capacities and resources of in-scope services.

10.8. We note that the UK's AADC included a 12 month implementation period[43].

[43] UK Information Commissioner's Office (2020), *Age appropriate design: a code of practice*, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf

10.9. We recommend a minimum six month implementation period before any compliance measures are assessed by the OAIC.

Engagement with potential code developers prior to guidance release

10.10. DIGI would like to see clear guidance that is outcomes-based for code developers in order to enable the code to be flexibly and proportionately applied to diverse businesses.

10.11. In relation to the OSA Codes, DIGI provided input that was reflected in the Office of the eSafety Commissioner's position paper. We valued the opportunity to provide input to the Commissioner in the formative stages of their guidance on key substantive questions relating to the OSA codes, and suggest this process be replicated for the OP Code(s).

11. Areas requiring guidance from the OAIC

Comparative analysis between the Bill's requirements and the GDPR

11.1. All DIGI members have experience implementing the GDPR's requirements, which has evolved to become a global standard. DIGI urges the Bill and the Review to make recommendations that are consistent with the GDPR in order to ease implementation and ensure interoperability.

11.2. For example, the explanatory paper for the Bill says: "the OP code will require organisations to ensure that, when they seek consent from individuals, the consent is voluntary, informed, unambiguous, specific and current." DIGI notes that "current" is not included in the GDPR's definition of consent, and it is unclear what this entails for industry and whether this departure from the GDPR is specifically required in Australia.

11.3. If there must be departures from the GDPR in the final Bill and Review, we ask that the OAIC's guidance for any resulting codes include a justification, and a detailed comparative analysis to practically guide industry's implementation of the measures.

Ceasing to use or disclose personal information upon request

11.4. In relation to ceasing to use or disclose personal information upon request, we note that the Explanatory Paper says "This requirement is not intended to amount to a 'right to erasure' of the personal information". Guidance needs to be provided to entities that may not be able to provide an advertising-free version of their services for technical reasons.

11.5. As currently drafted, the right to object would extend beyond comparable requirements under the GDPR, where a right to object is only available for data processed on the grounds of legitimate interests or public interest. For example, it is not clear whether the Bill's proposal would apply to information collected from end-users through consent. Without further clarity, this is a possible interpretation of the Bill.

11.6. In the development of a right to object, it will be important to ensure it does not impede advertising-supported business models. Advertising may be an intrinsic part of an online service that enables it to be free and accessible to Australians more broadly. Personalisation of ads generates significant benefit for consumers, advertisers and small businesses by making advertising more efficient, relevant and helpful. Targeted

advertising has reduced the cost of advertising for Australian businesses and contributed to economic growth, especially in small businesses. A 2019 study of the advertising markets in four countries (Australia, the United States, France, and Germany) explains:

> *Better targeting leads to higher returns on investment, while the lower cost of entry opens the door to smaller firms. Small businesses can grow more quickly and easily through digital advertising. Consumers benefit by the increased choice and access to more business.*[44]

11.7. Assuming the definition of vulnerable groups is "other individuals who are physically or legally incapable of giving consent to the collection, use or disclosure of personal information; and" (as under the Bill), there is an inherent challenge here; in order to know that a group is "vulnerable", there is a level of privacy intrusion and potential sensitive data collection that needs to occur. There is no way of a platform knowing this organically.

Harmful tracking

11.8. A definition needs to be provided of "harmful tracking", supported by examples. Almost all websites use cookies, for example, and it is currently unclear as to whether this usage would meet the threshold of "harmful". We recommend an evidence based, outcomes-based focus on the outcomes that industry should be working to prevent in constituting the definition of harm.

Summary of recommendations in Section 3

K. As noted in Section 1 of this submission, we recommend the best solution to standardise protections across these sectors and economy-wide is through the Privacy Act Review. However, should the Bill proceed with its current scope, it should be amended to allow for more than one OP Code.

L. The timeline for code development should be 12 months from the date at which the OAIC is able to release its guidance for code developers.

M. A minimum six month implementation period should be established after the codes are registered, and before any compliance measures are assessed by the OAIC.

N. The Commissioner should be open to engagement and input with potential code developers before the release of her guidance, to help inform the guidance provided.

O. The Commissioner's guidance must be outcomes-based, flexible and proportionate, while also providing operational guidance on key concepts captured.

[44] Dr Michael Mandel (2019), *The Declining Cost of Advertising: Policy Implications*', available at https://www.progressivepolicy.org/issues/government-reform/the-declining-price-of-advertising-policy-implications-2/

P. DIGI urges the Bill and the Review to make recommendations that are consistent with the GDPR in order to ease implementation and ensure interoperability.

Q. Where there are departures from the GDPR in the final Bill and Review, we ask that the OAIC's guidance for any resulting codes include a justification, and a detailed comparative analysis to practically guide industry's implementation of the measures.

Conclusion

12. Overview of relevant member work

12.1. DIGI's members have made and continue to make extensive investments in the privacy and safety of their users. At a high level, that work extends far beyond the provision of privacy policies and notices. They have dedicated teams focused on privacy and cross-functional review processes for new products to ensure "privacy-by-design" before they are released. They provide privacy tools to provide people with transparency, choices and control about how their data is used. DIGI members all allow their users to destroy, de-identify, access and correct their personal information in accordance with the Australian Privacy Act 1988 and where relevant they apply the GDPR's requirements in this area.

12.2. In relation to age restrictions, relevant members set age restrictions on their user-generated content platforms and many other products to limit and discourage the use of services by underage users, ranging from under 13 to 18 as appropriate to the service. When a notice or express admission that a user is underage is received, it will be investigated and accounts will be suspended accordingly. Some services will also take steps to prevent users lying about their age to access an account after it has been denied, by placing a persistent cookie on the device to prevent the child from attempting to circumvent the age restriction or by using artificial intelligence to understand the true age of a user.

12.3. In addition to universal privacy protections, as previously noted in 4.15, relevant DIGI members have extensive programs in place to protect young people on their services. At the service provider level, they provide applications to enable family sharing and limitations on minors' devices, that include controlling their privacy settings, filtering, screen time limits and other features designed to safeguard minors' privacy and experiences online. At the search engine level, they filter ads containing or promoting nudity, sexually suggestive content, adult entertainment and other services from appearing within search results. At the app distribution level, restricted profiles can be established where more mature content can be filtered out of the app store. At the browser level, parents can create restricted profiles for minors that allow parents to block and approve sites viewed, and where "safe search" is on by default in such accounts. At the platform level, there are similar "safe search" settings that hide sensitive content and remove blocked and muted accounts. There are also default privacy settings for minors, and additional safety measures for users in this category, including restrictions aimed at inappropriate interactions and CSAM material, as well as advertising restrictions.

12.4. We recognise that “digital first” social media platforms and large online platforms are often in the spotlight when it comes to questions of data privacy, and are rightly held to a high level of public scrutiny. As a result of that and their depth of technical expertise with data governance, we would posit that the privacy and safety investments made in this sector may exceed those in some high risk sectors that equally use personal information, but do not have as much experience nor the same levels of public scrutiny. We believe that the “digital first” sector has learnings to share in the realm of privacy on what works, and what does not, and DIGI sees an important opportunity for system-wide improvements in our sector and economy-wide changes through the review of the Privacy Act.