To. Ms. Kate Reader & Ms. Morag Bond
Joint General Managers, Digital Platforms Branch
Australian Competition & Consumer Commission (ACCC)
By email: digitalmonitoring@accc.gov.au

Friday April 8, 2022

Dear Ms. Reader & Ms. Bond,

The Digital Industry Group Inc. (DIGI) thanks you for the extended opportunity to provide our views on the *Digital Platform Services Inquiry Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services* (the Discussion Paper).

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.

As this vision demonstrates, we share the goals of ensuring competition in Australia's digital economy, and strong consumer protection, and are pleased to have the opportunity to contribute to this inquiry.

DIGI and its members believe that the digital industry has a responsibility to address consumer detriment, and that the Australian Government has an important role to play in examining evidence of consumer harm, evaluating existing rules and providing proportionate and targeted interventions to protect consumers. DIGI sees itself as a key Government partner in this endeavour, through our code development, partnerships, and our ongoing engagement with proposed regulation where we advocate for approaches that are effective in their goals and can practically be implemented by industry.

Our submission is structured around the key lines of inquiry advanced in each chapter of the Discussion Paper. However, we wish to elevate the key themes which frame our comments, which are follows:

1. DIGI is concerned that the Discussion Paper extends the relationship between competition and consumer issues, such that it appears to reframe what is traditionally considered to be a *consumer protection issue*. Further definitional clarity is required on what is considered to be a *consumer protection issue* from *other issues arising on digital platform services*. In this submission, DIGI aims to advance thinking in this area.

2. We understand that, in Australia, competition and consumer issues at the federal level are dealt with by the ACCC under a single legislative regime: the Competition and Consumer Act 2010 (CCA). Nonetheless, consistent with emerging approaches in the UK and EU, Australia should better delineate the *competition regime* from *consumer protection regime* on digital platform services. Noting that DIGI's members include companies of ranging sizes and market status, our submission will largely focus on issues relating to consumer protection.

3. There is an extensive and evolving regime to address both *consumer protection issues* and *other digital platform service issues* in Australia that provide strong safety nets for consumers and

compliance requirements for digital platform services in Australia. While DIGI identifies some gaps within this regime, and specific areas that would benefit from increased consistency and coordination, we do not believe that a new framework for digital platform services is needed. A singular framework – particularly if it were to be owned by a single regulator – would lack the depth, breadth and clarity to be suitably comprehensive in addressing consumer privacy, safety, cyber security and fair trading issues on digital platform services.

4. The Discussion Paper explores new models of ex-ante rules for *consumer protection issues*. Ex-ante rules are typically reserved for market failures or egregious harms which cannot be addressed by traditional ex-post rules. DIGI believes the threshold for ex-ante rules to address consumer protection issues should remain high and well defined, and the next phase of this consultation should focus on identifying areas of the existing regime for targeted reform.

5. We believe that the best outcomes for consumers will arise from ensuring *capability* and *capacity* across the Australian Government and existing regulators to better address the digital manifestation of issues in various portfolio areas. Such an approach is effective because each issue arising on digital platform services is distinct and complex, and requires a high level of specialised knowledge across different regulators and regulatory instruments. We therefore believe that the best outcomes will occur when:
    a. Existing regulatory instruments are *modernised* for digital challenges, in close consultation with industry and other relevant stakeholders.
    b. Different regulators and Government departments are *resourced and skilled* to continue to specialise in their respective areas of expertise as they relate to digital platform services.
    c. There are strong *cooperation mechanisms* with other regulators and Departments, and transparency and consultation with the digital industry.
    d. *Consumers* and *industry* both have clear, comprehensive targeted and public communications about their rights and responsibilities respectively on digital platform services.

Noting that the ACCC is seeking to explore novel regulatory tools to address issues arising on digital platform services, DIGI highlights our experiences with code development, which we would be happy to discuss in detail to aid this exploration. Specifically:

- DIGI developed *The Australian Code of Practice on Disinformation and Misinformation* (ACPDM) to realise Australian Government policy in this area. Signed by eight major technology companies and open to any others, every code signatory commits to safeguards to protect against online mis- and disinformation, including publishing and implementing policies on their approach, and providing a way for their users to report content that may violate those policies. Signatories must release annual transparency reports about all of those efforts, the first set of which were released in May 2021, providing new insights on the scale of the online misinformation in Australia and its management.

- DIGI is also currently working with a wide range of companies, well beyond our membership, to develop industry-wide mandatory codes under the Online Safety Act 2021 (OSA Codes). We are working with the Office of the eSafety Commissioner to have the first set of these registered in the coming months, and they will be released for public consultation prior to then. DIGI is leading the drafting of the chapters of the codes relating to social media services, search engines, and app distribution services. Once in effect, these codes will standardise industry-wide protections for Australians in relation to Class 1 and Class 2 content under the classification code, which includes child sexual expoitation material, pro-terror content and pornography.

We thank you for your consideration of the matters raised in this submission, and for the opportunity to participate. We understand that the ACCC's Final Report is due to the Government in September 2022, we hope to have the opportunity to further discuss these issues with you in the coming months.

Best regards,

[redacted]

Sunita Bose
Managing Director, DIGI
[redacted]

Table of contents

Chapter 5: Harms to competition and consumers arising from digital platform services

DIscussion Paper consultation question: What competition and consumer harms, as well as key benefits, arise from digital platform services in Australia?

1. Key benefits

Economic impact of Australia's technology sector

1.1. In September 2019, a major report about Australia's technology sector called "Australia's Digital Opportunity" was released, produced by AlphaBeta (now Accenture) and commissioned by DIGI[1]. It quantifies the extraordinary contribution of Australia's technology sector to the national economy. It found that, at that point in time, the technology sector contributed $122 billion each year to the national economy, or 6.6% of GDP. A subsequent estimate by Accenture in 2021 found that the tech sector contributes $167bn, or 8.5%, of GDP, demonstrating the rapid growth of the sector[2].

1.2. The contribution and growth of the sector has an economy-wide impact. This $122 billion a year contribution comprises two components:

1.2.1. The direct impact of firms within ICT industries such as Internet publishing and broadcasting, search portals, data processing, computer system design, and telecommunications. The direct contribution from the tech sector is $69 billion, or 3.8% of GDP.

1.2.2. The indirect impact of technology on other sectors, which includes wages for technology professionals working in non-tech sectors, and profits enabled by digital activities, which is valued at an estimated $53 billion. This calculation does not directly estimate the productivity gains from the technology sector, for example through efficiencies gained through enterprise software.

1.3. The 2019 report also found that the sector employs 580 000 workers, and in 2021 this was estimated to be 860 000, with sizable proportions in regional Australia.

1.4. The technology sector is therefore truly unique -- it is a high performing industry in itself and also supports SMEs and regional Australia, and the productivity of almost all other industries. Gains in this sector can have a major ripple effect economy wide.

Australia is not realising its technology potential

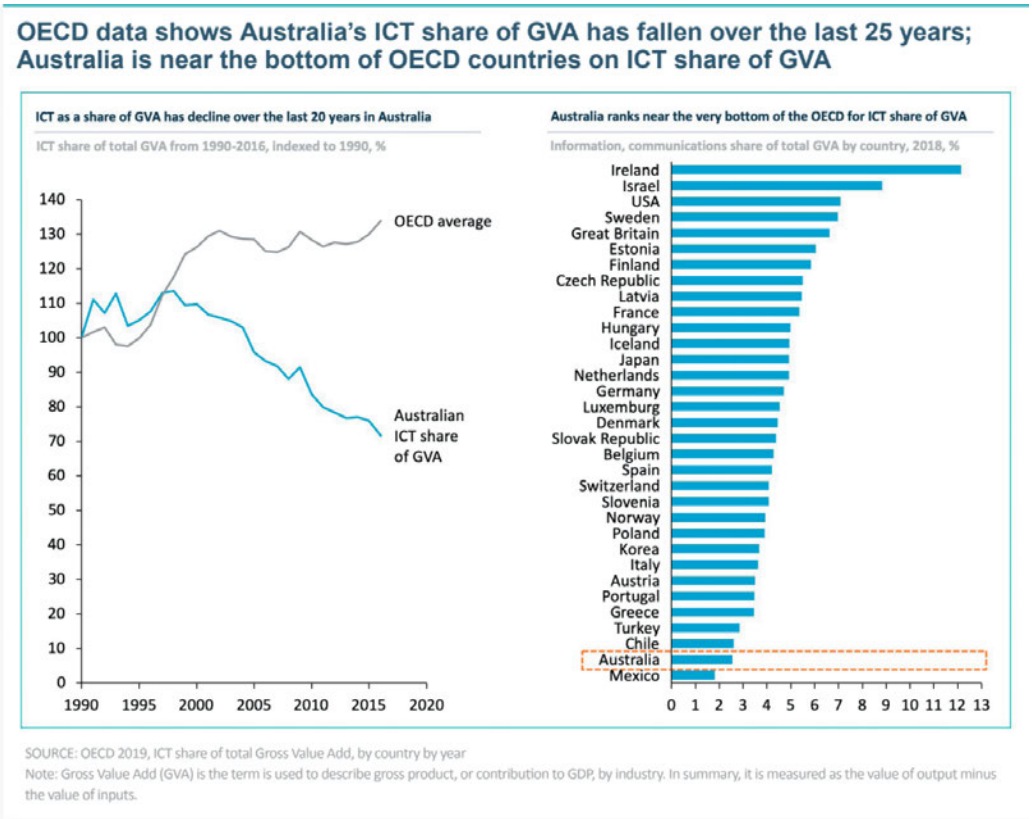
1.5. Yet the analysis also showed that Australia is not fully realising the economic potential of its technology sector. Per Figure 1, Australia ranks second last in the OECD for the size of its technology sector. In the past 25 years, Australia's ICT sector has contributed a declining proportion of net economic value.

---

[1] Unless otherwise noted, all statistics from this section are from AlphaBeta (2019), *Australia's Digital Opportunity*, accessed at: https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf

[2] Accenture (2021), *The economic contribution of Australia's tech sector*, accessed at https://techcouncil.com.au/wp-content/uploads/2021/08/TCA-Tech-sectors-economic-contribution-full-res.pdf

Figure 1: Declining ICT share of Gross Value Added



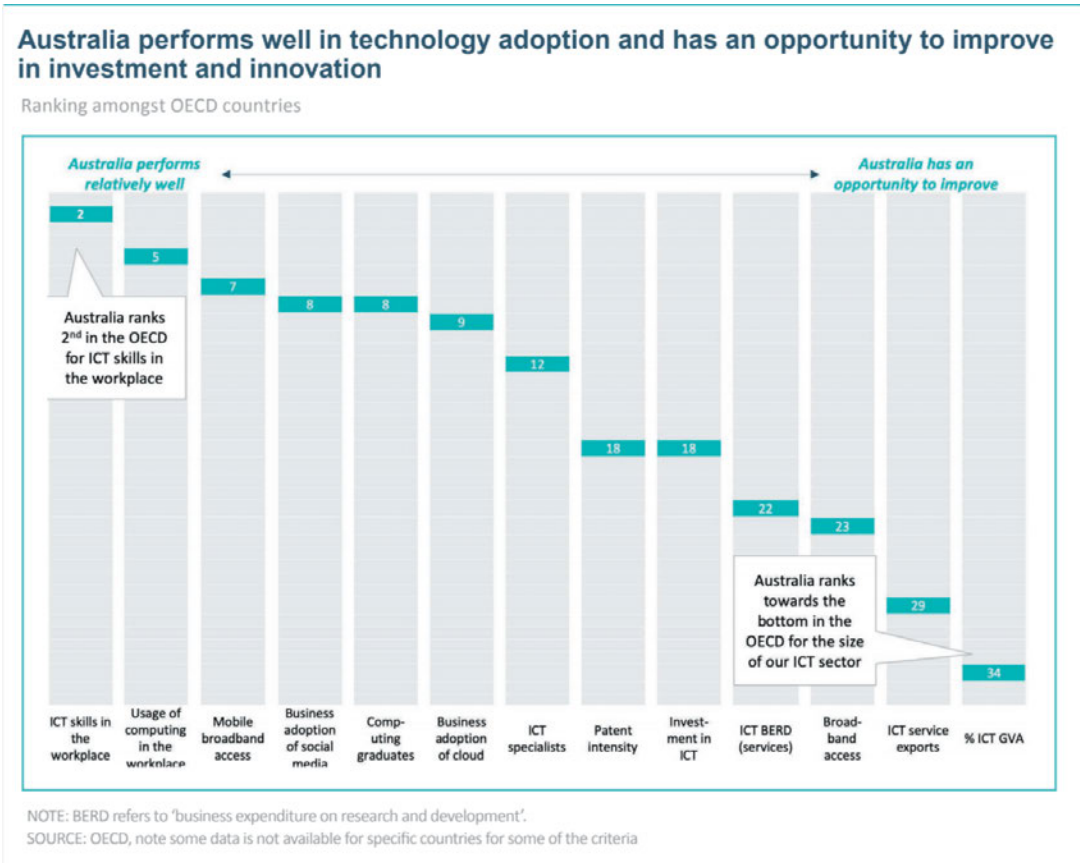
1.6. If Australia caught up with the growth rate of tech-leading countries in the OECD, that overall contribution could almost double to $207 billion per year to GDP by 2030, with the updated estimate in 2021 projecting this figure to be $241 billion.

1.7. A featured part of the Australian Government's Digital Economy Strategy, to become a leading digital economy by 2030, under the Morrison Government has been increasing rates of technology adoption. The Morrison Government has talked about how Australia has "just got to be the best at adopting" technology[3]. Adoption is crucially important, and has arguably been the bridge that has seen Australians maintain productivity and connection through the pandemic.

1.8. As Figure 2 shows, Australia performs well with technology adoption, which speaks to the uptake of digital platform services in Australia. By contrast, Australia is towards the bottom of the OECD ladder in relation to the size of the information communications technology (ICT) sector, and for technology exports.

[3] Sadler, Denham (2020) *Tech adoption not creation: the PM's digital plan*, InnovationAus, accessed at https://www.innovationaus.com/tech-adoption-not-creation-the-pms-digital-plan/

Figure 2: OECD rankings for technology performance areas

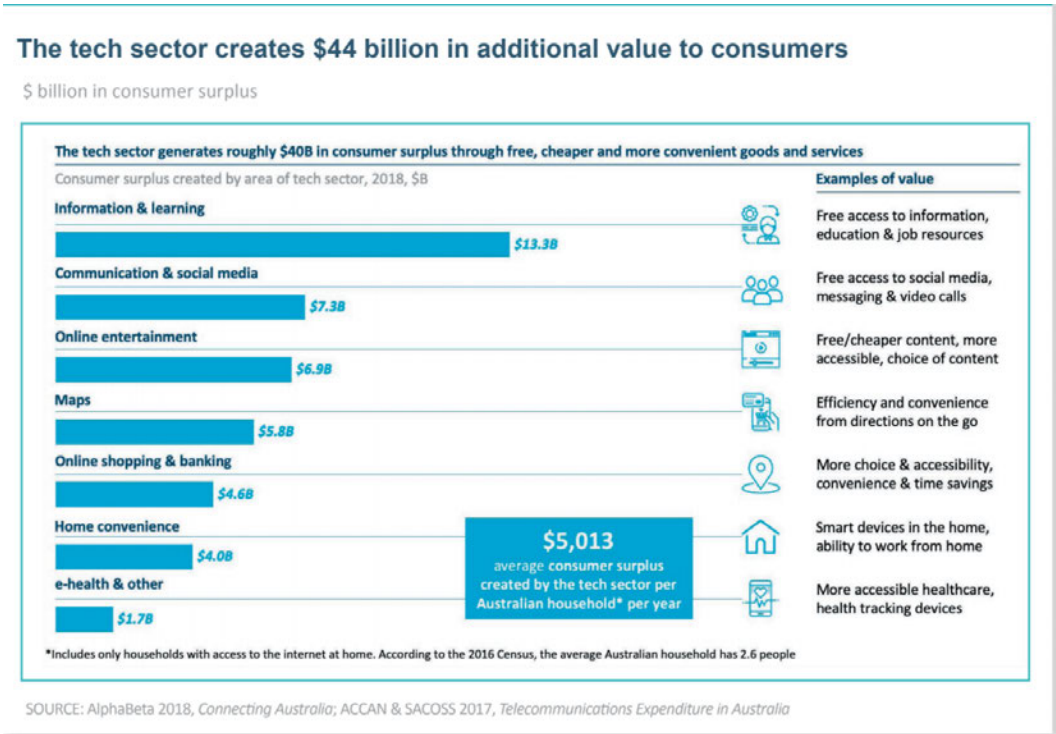


1.9. As Australia develops a roadmap to meet the Government's Digital Economy Strategy of becoming a leading digital economy by 2030, we need to be acutely aware that we are starting this race at the back of the pack with the second smallest technology sector in the OECD. While the incentives under the Government's Digital Economy Strategy are extremely important, the regulatory settings being proposed by the ACCC and other arms of the Australian Government play a crucially important role in the realisation of that strategy, and their impact on it need to be assessed.

The role of multinational enterprise in Australia's digital economy

1.10. Policy proposals need to take into account a more rounded view of the role of the benefits of multinational enterprises in Australia's digital economy. According to AlphaBeta, digital technologies like maps, web search, online banking and shopping generate considerable value for consumers that is not captured in traditional measures of GDP, and are therefore gains that may be measured as a 'consumer surplus'. Per Figure 3, AlphaBeta calculates that the consumer surplus created by the tech sector in Australia is estimated to be nearly $44 billion, or approximately $5,000 per Australian household per year on average.

Figure 3: Consumer surplus from digital platform services



1.11. In addition to the consumer surplus, the presence of multinational technology companies brings other benefits to the domestic market. In an analysis of the value that streaming services bring to local economies, Adam Behsudi argues that: "In economic terms, the internet has created economies of scale and scope, meaning there is more supply and demand for greater quantity and variety of creative content"[4]. Evidence of this exists in Australia, with a recent assessment of the economic, societal, and cultural Impact of YouTube conducted by Oxford Economics, estimating that the video sharing platform contributed A$608 million to the Australian economy in 2020 and supported 15,750 full time equivalent jobs[5].

1.12. The supply and demand benefits are complemented through the networks that multinational technology companies provide to local consumers that create an ease of trade both within and across economies. Companies are beginning to export very early,

[4] Behsudi, Adam (2021), "From stream to flood", June edn., *Finance & Development*, accessed at https://www.imf.org/external/pubs/ft/fandd/2021/06/streaming-video-services-flood-emerging-markets-behsudi.htm

[5] Oxford Economics (2021), *A Platform For Australian Opportunity: Assessing The Economic, Societal, And Cultural Impact Of Youtube In Australia*, accessed at https://kstatic.googleusercontent.com/files/c2f33cb4f0613a65db06d4d7d95951121a4c52fb45d369b163de619ed2e06597f60a4e4589821ea0500766b25ebbc9e23795952a03a1ce97c4274040eb6370d2

where 35% Australian globally active businesses are 'born-global' and earning international revenue within two years of establishment[6].

1.13. The growth of digital platform services creates opportunities for new homegrown companies. First, the networks provide both the basis and inspiration for new companies; The internationally successful Australian tech company Afterpay's founders' trajectory to founding a multi-billion dollar company began with a jewellery store on eBay, which they spun off into buy-now-pay-later online business which inspired the wider offering of that model to retailers[7].

1.14. There is also the phenomenon characterised by the story of the founders of PayPal, irreverently known as "the PayPal mafia", who have gone on to establish a number of other successful companies such as LinkedIn, Tesla, Yammer and Yelp and are also major investors in many more. This is already beginning to occur in Australia, where a former engineer from Google went on to be one of the original co-founders of Australian multi-billion dollar company Canva[8]. The challenges that Australian entrepreneurs have faced in attracting enough high skilled tech talent are well documented; having more global tech companies expand regionally in Australia over Singapore will serve to create a thriving ecosystem where the calibre of talent, the networking, mentorship, business opportunities all increase, and ultimately more technology products become available to Australians.

1.15. It is for these reasons that we need to give careful consideration to the regulatory environment in Australia, and whether it is conducive to encouraging small, medium and large technology companies offering digital platform services to stand and expand in Australia. We encourage a whole of Government approach, and close alignment with the ACCC's recommendations and the development of the Digital Economy Strategy Roadmap, being led by PM&C. As noted, Australia ranks second last in the OECD -- only to Mexico -- for the relative size of our technology sector. Given the downward trajectory of Australian ICT share of GVA for the last 20 years, and the need and immense potential to grow this industry, the unintended consequences of recommendations across this inquiry more broadly need to be carefully assessed.

2. Digital platform service issues, platform and regulatory responses

2.1. In this submission, DIGI seeks to advance the conversation about the types of issues that present themselves on digital platform services, the extensive and evolving regulatory landscape in these areas, and relevant industry responses.

---

[6] Agarwal, R., Bajada, C., Green, R., Rammal, H., Scerri, M. (2017), *Australia's International Business Survey 2017, University of Technology Sydney*, accessed at https://www.austrade.gov.au/news/economic-analysis/key-publications/australias-international-business-survey-2017

[7] Waters, Cara (2019), "Afterpay 'brain bubble' came from jeweller Ice Online", in *The Sydney Morning Herald*, accessed at https://www.smh.com.au/business/small-business/afterpay-brain-bubble-came-from-jeweller-ice-online-20191101-p536h6.html

[8] Two examples of Australian ventures being co-founded by former Google engineers are Canva and Neara. See Kim, J. (2018), "How he went from building a Google product to co-founding Canva" in *Tech in Asia,* accessed at https://www.techinasia.com/talk/cameron-adams-canva; See Redrup, Yolanda (2021), "Big-name VCs pile into digital twin company Neara" in *Australian Financial Review*, accessed at https://www.afr.com/technology/big-name-vcs-pile-into-digital-twin-company-neara-20210414-p57j96

2.2. To that end, we have developed Table 1 (included in the Appendix, on p. 31) that maps a high-level overview of these issues and the trends in industry responses to those. Table 1 also maps the current or forthcoming Australian Government regulation aimed at addressing specific issues, noting that these predominantly relate to services which host user generated material or allow user interaction. Table 1 demonstrates that there is an extensive and evolving Australian suite of regulations that provides strong safety nets for Australians and compliance requirements for digital platform services in Australia.

2.3. In addition, DIGI has developed Figure 4 (on p. 12) that maps the categories of digital platform services by broad category of issue type, identifies the arms of Government with primary regulatory expertise, and the primary regulatory tools at their disposal (noting that these are not exhaustive).

2.4. This analysis is used to demonstrate why DIGI does not believe that a new framework for digital platform services is needed; We consider that a new framework could indeed be counterproductive, as it would add further complexity to what has already been described as an overlapping regime for digital platform services. A singular framework would lack the depth, breadth and clarity to be suitably comprehensive in addressing consumer privacy, safety, cyber security and fair trading issues on digital platform services.

2.5. A similar view at an even more micro level is echoed in the March 2022 House of Representatives Select Committee on Social Media and Online Safety Committee report into Social Media and Online Safety[9], which states:

> *Given the broad suite of issues that fall under the rubric of online safety, further centralisation of responsibility for online safety policy or enforcement may be challenging, unsuitable and impractical.*

2.6. However, if the problem that the Discussion Papers proposal for a new framework is seeking to achieve is to improve consumer and industry clarity about their rights and responsibilities in relation to digital policy issues, as well as the ability of Government to oversee these, we believe there are more effective solutions – outlined below.

Consolidation in the online safety area

2.7. DIGI is supportive of further consolidation in the legislative framework for *online safety* in order to aid industry and user comprehension. For example:

2.7.1.1. In an effort to make logical consolidation and minimise overlap and inconsistency in regulation, DIGI recommends the The Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (AVM Act) be incorporated into a consolidated Online Safety Act.

2.7.1.2. Inconsistencies within the various online regulatory instruments under Online Safety Act need to be addressed. As one example of an inconsistency, the OSA's takedown schemes and the BOSE suggest that service providers should be required to remove all types of Class 1 material. However, the Commissioner's position as stated in their

[9] House of Representatives Select Committee on Social Media & Online Safety (2022), *Committee report*, accessed at https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Media_and_Online_Safety/SocialMediaandSafety/Report

position paper on the OSA Codes[10] is that an identified subclass of Class 1, termed "Class 1b (fetish practices)" can be treated as Class 2 materials, and therefore do not need to be removed. It is unclear whether this interpretation extends to other aspects of the OSA, which creates confusion for industry participants working in good faith to comply with the legislation.

Attention to existing frameworks and identified gaps

2.8. DIGI believes that improving the existing enforcement frameworks provide a more proportionate means of achieving desired outcomes.

2.9. However, there are gaps within these frameworks, and specific areas that would benefit from increased consistency and coordination; DIGI has highlighted perceived gaps in bold in Table 1. For example, DIGI encourages the Australian Government to develop a clearer legislative framework that defines hate speech. This will serve to help relevant stakeholders, including digital platforms, to better report, review and remove content that meets a defined Australian legal threshold.

Industry & consumer facing communication

2.10. Currently, there are no portals whereby new entrants to the Australian market or companies seeking to understand their compliance obligations can go to receive information about the various regulatory tools that may apply. Nor is there a comprehensive portal of information for consumers about the tools and avenues they may explore for recourse in relation to particular issues.

2.11. The ACCC should consider advancing recommendations that increase the clarity of rights and responsibilities for consumers and industry respectively through a consolidated website that provides links and information about their obligations and rights under the various regulatory frameworks aimed at addressing issues on digital platform services.

Ensure regulators are resourced to address digital policy issues

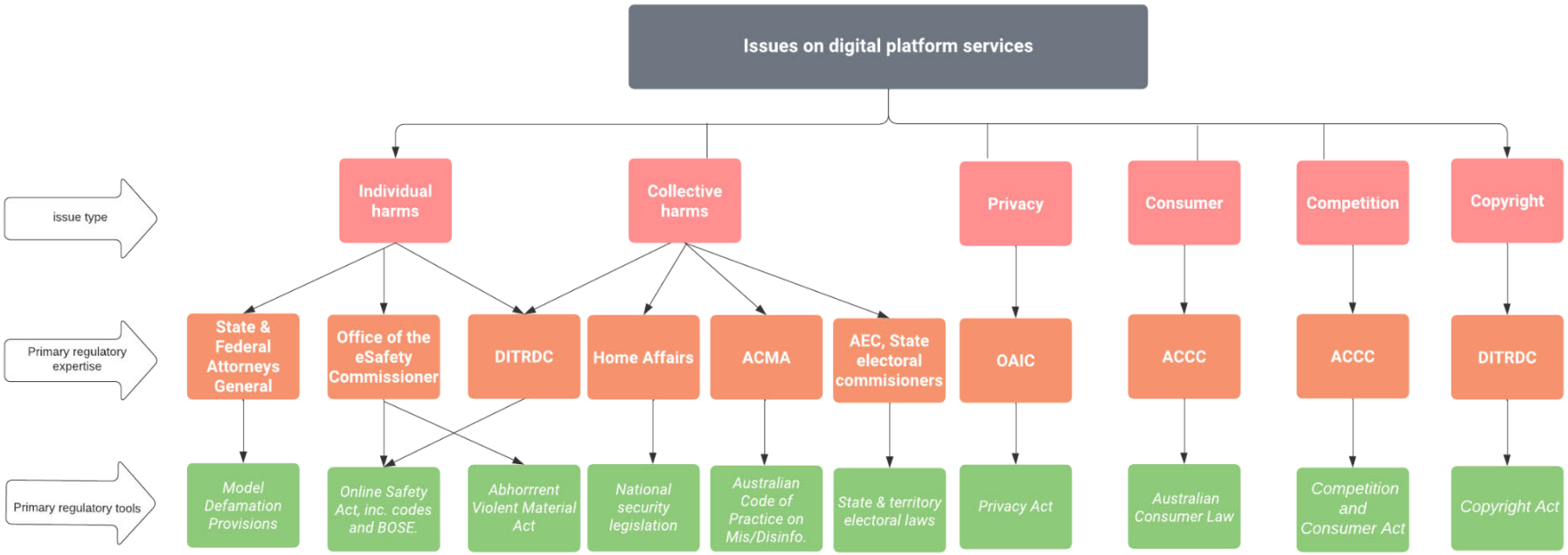
2.12. Each of these regulators and Departments identified in Figure 4 have developed extensive expertise in their issue area in their offline manifestation, as well as their online manifestation; this expertise may not be fully leveraged across the Australian Government associated with the various issues under a single framework.

2.13. Focus should be instead given to ensuring regulators and other departments with regulatory expertise are resourced and skilled to continue to specialise in their respective areas of expertise as they relate to digital platform services. For example, DIGI supports the recent announcement[11] by the Government that the ACMA will be empowered with a formal, long-term role in relation to misinformation and disinformation on digital platform services and hopes this is addressed in a timely fashion.

---

[10] Office of the eSafety Commissioner, *Development of industry codes under the Online Safety Act: Position Paper*, accessed at https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper.
[11] Minister Paul Fletcher, media release (21/03/22), *New disinformation laws*, accessed at https://minister.infrastructure.gov.au/fletcher/media-release/new-disinformation-laws

Figure 4: Digital platform service issues, regulatory expertise & tools



Summary of recommendations in relation to Chapter 5

A. There needs to be close alignment with the ACCC's recommendations and the development of the Digital Economy Strategy Roadmap, being led by PM&C through a whole-of-Government approach.

B. We encourage the Australian Government to consider the focus on gaps DIGI has identified within the regime in Table 1, included in the Appendix at p. 31.

C. We encourage further consolidation and consistency in regulation, specifically through the uniformity of definitions across the regulatory tools in the Online Safety Act, and the incorporation of The Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (AVM Act) into that Act.

D. The ACCC should consider advancing recommendations that increase the clarity of rights and responsibilities for consumers and industry respectively through a consolidated website that provides links and information about their obligations and rights under the various regulatory frameworks aimed at consumer protection on digital platform services.

E. Relevant regulators and Government departments must be resourced and skilled to continue to specialise in their respective areas of expertise as they relate to digital platform services.

→ Note that DIGI discusses the specific issues identified in Chapter 5 of the Discussion Paper (e.g. "dark patterns online") in the section of this submission on Chapter 8, in response to the discussion questions posed in relation to those issues.

Chapter 6: Competition and consumer protection law enforcement in Australia

DIscussion Paper consultation question: Do you consider that the CCA and ACL are sufficient to address competition and consumer harms arising from digital platform services in Australia, or do you consider regulatory reform is required?

3. Avoid conflation of consumer harms and competition issues

3.1. DIGI is concerned about the premise of the discussion question quoted above, and the way that it has been framed in the Discussion Paper. DIGI understands that the Competition and Consumer Act 2010 (CCA) is a national law that governs how businesses must deal with suppliers, competitors and customers, and covers aspects of business such as advertising and price setting, that applies to all businesses including digital platform services. The Australian Consumer Law (ACL), set out in Schedule 2 of the CCA, specifically relates to the treatment of consumers.

3.2. These laws were not intended to address the broad array of issues arising on digital platform services, and the framing of the question implies as such. As DIGI's Figure 4 and Table 1 demonstrate, there are wide range of enforceable laws intended to address issues arising on digital platform services, such as the Online Safety Act, the Privacy Act, the Model Defamation Provisions and Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (AVM Act) which have all either been recently created, reviewed or are currently under review.

3.3. We do not believe the ACL and the CCA are the appropriate vehicles to address many of the issues identified in the Discussion Paper, though we recognise the ACL and CCA play an important role with certain consumer protection issues (e.g. false and misleading statements). When we take into account the array of regulatory responses outlined in Table 1, it would not make sense for most of these to be folded into either the ACL or CCA and they should be addressed separately.

3.4. More broadly, DIGI is concerned with the conflation of competition regulation and ex-post consumer protection regulation in the Discussion Paper. Australia should offer more separation between the competition regime from consumer protection regime on digital platform services, consistent with emerging approaches in the UK and EU.

3.5. For example, the EU has separated the Digital Markets Act, which is a targeted ex-ante regime applying only to firms with market power, from the Digital Services Act, which a broader regulatory framework to address issues arising from the operation of digital platforms and intermediary services[12].

3.6. Similarly, in the UK, the introduction of the proposed ex-ante pro-competition regime is subject to a separate consultation from reform of the existing ex-post regime for competition and consumer protection[13].

3.7. In both cases, the competition regime and consumer protection and competition regimes are legally separate and overseen and enforced by different regulatory frameworks, and also different regulators. While both areas should be broadly coherent with each other, a level of separation promotes a more objective assessment of the need and design of both areas of reforms, and ensures appropriate targeting of interventions and legal clarity for market participants.

3.8. The Discussion Paper explores new models of ex-ante rules for consumer protection. In contrast with ex-post rules, ex-ante rules are typically reserved for market failures or egregious harms which cannot be addressed by traditional ex-post rules. We believe the bar should remain high for ex-ante rules, to focus on types of conduct that are recognised to be particularly harmful, rather than seeking to address theoretical or speculative harm.

[12] European Parliament (04/04/22), *EU Digital Markets Act and Digital Services Act explained*, accessed at https://www.europarl.europa.eu/news/en/headlines/society/20211209STO19124/eu-digital-markets-act-and-digital-services-act-explained

[13] See UK Government (2021), A new pro-competition regime for digital markets, accessed at https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets; UK Government (2021), Reforming competition and consumer policy - GOV.UK, accessed at https://www.gov.uk/government/consultations/reforming-competition-and-consumer-policy

4. Ensure greater coordination across the Australian Government on digital policy

4.1. DIGI believes that strong cooperation mechanisms between Australian regulators and Departments that have a role in relation to digital platform services is critical to advancing efforts to address consumer harms.

4.2. DIGI therefore welcomed the formation of Digital Platform Regulators Forum (DP-REG), announced on Friday March 11, 2022[14], which formalises cooperation between the ACCC, ACMA, OAIC and eSafety.

4.3. DIGI agrees that such a forum is needed in order to ensure effective coordination on the regulation of digital platforms in a multilateral fashion. We welcome the focus on streamlining overlapping regulation, reducing duplication and creating proportionate, cohesive, well-designed and efficiently implemented digital platform regulation outlined in the DP-REG's Terms of Reference[15]. DIGI strives for similar goals in its extensive engagement with Australian digital policy.

4.4. As the newly formed DP-REG's operations are considered, DIGI would encourage a proactive programme of engagement with the digital industry in order to ensure deliberations are well informed, transparent to market participants and responsive to advances in technology. We welcome the inclusion within the Terms of Reference of the DP-REG that relevant stakeholders may have the opportunity to observe meetings or present on issues relating to the regulation of digital platforms.

4.5. Digital platform reform proposals and strategies advanced by many other agencies and Departments across the Australian Government, particularly the Department of Infrastructure, Transport, Regional Development and Communications, the Department of Home Affairs, the Attorney General's Department and the Department of Prime Minister & Cabinet. We therefore encourage the DP-REG to consider how it might regularly engage with other arms of Government that are advancing digital platform policy.

Summary of recommendations in relation to Chapter 6

F. The ACL and CCA are one of several instruments that regulate harms on digital platform services and have a specific role. They need to be examined alongside other existing relevant regulatory instruments advanced in Table 1 aimed at addressing online harms, including the Online Safety Act, the Privacy Act and the Model Defamation Provisions.

G. While DIGI notes that, in Australia, competition and consumer issues at the federal level are currently dealt with by the ACCC under a single legislative regime the Competition and Consumer Act 2010 (CCA). Consistent with emerging approaches in the UK and EU, Australia

[14] ACMA media release (11/03/22), *DP-REG joint public statement*, accessed at https://www.acma.gov.au/dp-reg-joint-public-statement
[15] DP-REG (2022), *Digital Platform Regulators Forum Terms of Reference*, accessed at https://www.acma.gov.au/sites/default/files/2022-03/DP-REG%20Terms%20of%20Reference%20.pdf

should better delineate the competition regime from consumer protection regime on digital platform services.

H. Ex-ante regulation should be limited to addressing market failures or consumer harms which cannot be effectively addressed by the traditional ex-post regime. The bar for introducing ex-ante rules should be set high, consistent with other regulated markets.

I. We encourage the DP-REG to consider how it might regularly engage with other arms of Government that are advancing digital platform policy, and the digital industry.

Chapter 7: Regulatory tools to implement potential reform

5. A new framework would add complexity to compliance

Discussion Paper consultation question: Should law reform be staged to address specific harms sequentially as they are identified and assessed, or should a broader framework be adopted to address multiple potential harms across different digital platform services?

5.1. As argued in the previous sections of this submission, DIGI is concerned that the proposal for a broad new framework with regard to digital platform services would add complexity to an already complex compliance environment for those services, as illustrated through the mapping exercise provided in Table 1. As the Discussion Paper notes, "a new framework would need to provide sufficient legal certainty for market participants"; we are concerned that a supplemental framework, when added to the existing matrix of frameworks, will conversely create confusion for market participants, particularly new entrants and SMEs, and risks overlapping with existing areas of regulation.

5.2. We are, however, supportive in principle of a targeted approach to address specific new harms as they are identified. This is because issues on digital platform services are a reflection of those same harms in the "offline" world, with complexities arising from their digital manifestation. They require careful investigation, consultation and design in order to target the source of a concern where it occurs and deliver the desired outcome for Australians.

5.3. For example, DIGI is supportive of the thorough processes to date that have been undertaken as part of the Stage 2 Review of the Model Defamation Provisions and the Privacy Act Review; Both of these processes have provided in-depth investigation into the issues, and meaningful and iterative engagement with stakeholders. Both processes are fundamentally related to digital platform services, yet it is hard to imagine any commonalities in the exploration of two sets of issues that would benefit from a shared framework.

6. Regulatory tools

Discussion Paper consultation question: What are the benefits, risks, costs and other considerations (such as proportionality, flexibility, adaptability, certainty, procedural fairness, and potential impact on incentives for investment and innovation) relevant to the application of each of the following regulatory tools to competition and consumer harms from digital platform services in Australia?

Key considerations for regulatory tools

6.1. DIGI believes that there are key considerations for *all* regulatory tools aimed at digital platform services, which should:

6.1.1. Be in response to a well-defined policy problem and informed by *evidence of that problem, specifically its prevalence and where in the digital ecosystem it occurs*.

6.1.2. Avoid "*tech tunnel vision*"; harms that arise on digital platform services are a reflection and manifestation of harms that occur offline. Technology-focused regulatory tools should not be considered in isolation, rather they should be considered alongside solutions in other areas of policy related to the problem, in order to make meaningful improvements. For example, new manifestations of online fraud require a law enforcement and criminal justice solution as well as action by digital platforms and the financial services sector.

6.1.3. Have *extensive and iterative consultation* with technology practitioners, to ensure that appropriate solutions are considered and that they keep pace with fast-moving technology, and can be effectively implemented.

6.1.4. Be *proportionate* to both the scale and nature of the issue and to businesses of different sizes, because digital platform services encompass start-ups through to large multinational enterprises.

6.1.5. Be *outcomes-based* and flexible, to account for the extreme diversity of the sector. There can be a myriad of different approaches each tailored to specific types of service or supply chains but delivering the same consumer outcome; conversely digital platform services are often each working to solve very different problems, with their only commonality being their medium.

6.1.6. Be *cohesive*, applying a *whole-of-Government approach*. Specifically, their impact on Australia's Digital Economy Strategy should be assessed, taking into account Australia's relatively small technology sector in relation to comparable OECD markets.

6.1.7. Have *procedural fairness* to ensure there are documented and transparent pathways for recourse for both consumers and industry participants, and review mechanisms.

6.2. DIGI encourages the Australian Government to develop "a digital economy assessment framework" where foundational and emerging policies across a range of departments can be evaluated against agreed principles, such as those above, and as other

Governments have done, and for their impact on Australia's Digital Economy Strategy to be a leading digital economy by 2030.

6.3. In the context of this recommendation, we note that the UK has developed a Plan for Digital Regulation[16], published in July 2021. The plan:

6.3.1. Sets out an overall vision for governing digital technologies, including new principles which will guide how the Government will design and implement regulating digital technologies as well as some practical proposals for how it will avoid overlaps and conflicts between different frameworks.

6.3.2. Sets clear objectives for digital regulation including promoting innovation, competition and growth.

6.3.3. Commits the Government to assess the case for regulation and to consider non-regulatory approaches in the first instance including self-regulation and industry standards.

6.3.4. Is presented as a cross-government approach which is intended to be followed by all departments initiating digital policy.

6.3.5. Repeats the UK Secretary of State's desire that the new Information Commissioner play a role in realising the economic benefits of data use and remove unnecessary barriers.

6.4. Adoption of clear principles and assessment framework for developing new Australian digital policy and regulation could serve as a consistent and predictable framework for Government and its external stakeholders. It would also complement the coordination efforts around existing regulation occurring at the DP-REG forum.

Tools should be promoted and assessed before new regulatory tools are advanced

6.5. DIGI has observed that, in the Australian digital policy environment, new regulatory tools are often proposed before the effectiveness of existing tools has been tested in response to a digital issue. Therefore, DIGI strongly encourages the rigorous assessment of existing regulatory tools before advancing proposals to replace or update them.

6.6. For example, on September 3, 2020, the Australian Government released the voluntary *Code of Practice: Securing the Internet of Things for Consumers*, which contains thirteen principles that signal Government expectations to manufacturers about the security of smart products. This voluntary code was only in operation for several months when the Department of Home Affairs was preparing its discussion paper titled *Strengthening Australia's cyber security regulations and incentives*, which proposes options for how that code might be replaced. Should the uptake of the original code not meet the Government's expectations, particularly in any priority sectors of the market, it should

[16] UK Government (2021), *Digital Regulation: Driving growth and unlocking innovation*, accessed at https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation#full-publication-update-history

prioritise targeted outreach and awareness raising initiatives. Targeted promotion of regulatory tools to relevant industry participants should be a baseline requirement upon finalisation.

6.7. In addition to promotion, there should be a minimum period where a tool is in force (e.g. 18 months) and a review process that assesses both the *awareness* and *effectiveness* of the tool in solving the defined policy problem. Otherwise, we risk layering regulatory proposals upon proposals, without taking stock of those in force; this is not an effective use of public resources.

DIGI's experiences with code development

6.8. As noted, DIGI has significant experience in novel solutions to digital platform issues including codes mentioned in the Discussion Paper, which we would be happy to discuss in detail with ACCC to aid this exploration of codes as a regulatory tool. As previously mentioned, DIGI developed *The Australian Code of Practice on Disinformation and Misinformation* (ACPDM) to realise Australian Government policy in this area. DIGI is also co-leading the drafting of the Online Safety Act Codes, with the Communications Alliance, supported by a broader steering group of industry associations.

6.9. We see many advantages to the use of codes in digital platforms services, as it allows for the practitioners and developers of fast-moving technology to channel their expertise into code development, making the regulatory tool more fit for purpose and future-proof. It is an efficient use of public resources, as the code development cost to Government is minimal.

6.10. As the digital platforms services sector is arguably more diverse than other sectors – with each service working to solve different problems, with often their only commonality being their digital nature – outcomes-based codes are the most effective. They enable a flexible approach that incentivises platforms with diverse models to continue to develop solutions that deal with the issue in their particular context, assess the effectiveness of different solutions and to make improvements based on their experience of what works. For example, with the issue of disinformation, perpetrators are often specialist "disinfo-for-hire" marketing firms or state-based actors that are constantly evolving their approach, determined to evade the responses of technology companies. With the ACPDM not prescribing the specific measures and instead focusing on outcomes, companies have agility to beat perpetrators at their own game without handing them the playbook.

6.11. While we do see many advantages to the use of codes in the digital platform services sector, we also need to be mindful of creating a matrix of different codes that also create confusion for a wide range of industry participants, particularly SMEs and new entrants, about their compliance obligations. In addition to the five codes identified by the ACCC in the Discussion Paper (News Media and Digital Platforms Mandatory Bargaining Code, Online Safety Act Class 1 code & Class 2 code, Online Privacy code, ACPDM), DIGI also understands that additional codes are being contemplated as part of the Privacy Act Review. The Review's October 2021 Discussion Paper released proposes that the APEC Cross Border Privacy Rules system would be implemented through the development of an APP code to ensure that requirements are enforceable[17]. The Department of Home

[17] Attorney General's Department (2021), *Privacy Act Review – Discussion Paper*, accessed at https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/, Chapter 23.

Affairs *Strengthening Australia's cyber security regulations and incentives* discussion paper also contemplates codes and standards in relation to cyber security.

6.12. We welcome the ACCC's statement in the Discussion Paper that, should any new codes be proposed, "that they would be developed in a way that minimises the risk of duplication or inconsistency in application". We recommend that DP-REG might consider a role in relation to assisting the coordination of various code development processes to avoid duplication in content, and overlapping timelines.

6.13. Because of how labour intensive code development is for industry associations and industry participants, any further code developments needs to be staggered to avoid duplicating timelines and processes. For example, the Regulatory Impact Statement (RIS) for the Online Privacy Bill estimates that the cost to OP code developers, being industry associations, will likely be $882,078.75[18]. Industry associations like DIGI are usually non-profit organisations that are incredibly lean in size. Undertaking representative code development processes requires intensive engagement with non-members of their associations, who are not required to contribute to the association's operating or code development costs. This is in addition to associations' core workstream of engaging in Government consultations, over which we have no control over the volume nor the timing. These are issues that need to be further explored with associations with experience of code development.

7. Align with global norms & account for Australia-specific differences

Discussion paper consultation question: To what extent should a new framework in Australia align with those in overseas jurisdictions to promote regulatory alignment for global digital platforms and their users (both business users and consumers)? What are the key elements that should be aligned?

7.1. As noted, DIGI does not believe a broad new framework of consumer protection rules is needed; however, in general, we believe that regulatory frameworks in relation to digital platform services in Australia should align with established global standards. Any differences from those global standards should be grounded in evidence of differences in relation to the Australian context that necessitates a departure.

7.2. For example, DIGI supports interoperability between equivalent global privacy regimes in order to provide greater legal certainty to companies, and consistency of experience for consumers who regularly interact with services being offered outside of Australia. This both serves to promote innovation and engenders trust in a digitally enabled economy that increasingly relies on cross border trade that, either directly or indirectly, utilises data that is sometimes personally identifiable. As the OECD notes, the significant increase in flows of personal data requires a globally coherent approach that includes national privacy strategies that can act to further privacy interoperability[19]. The EU's General Data Protection Regulation (GDPR), introduced on May 25, 2018, was landmark legislation that

[18] Attorney General's Department (2021), *Online Privacy Bill Regulatory Impact Statement*, accessed at https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-regulation-impact-statement.pdf

[19] OECD, *Interoperability of privacy and data protection frameworks*, available at http://goingdigital.oecd.org/data/notes/No21_ToolkitNote_PrivacyDataInteroperability.pdf

has served as the new global standard for privacy legislation that thousands of companies with a global presence have implemented.

7.3. While DIGI welcomes alignment with GDPR in the updated Privacy Act, the Australian Government would also be justified in proposing a departure from the established global norm on the basis that the digitisation of its economy lags behind that of other nations, as it currently has the second smallest technology sector in the OECD[20].

7.4. DIGI cautions against a sole focus on emerging regulatory developments in overseas jurisdictions to justify domestic regulation, without consideration of the Australian regulatory context. This can lead to bias toward a view that new regulation is required to address consumer concerns, rather than filling any gaps to address emerging trends in existing Australian frameworks.

Summary of recommendations in relation to Chapter 7

J. Law reform should be staged to address specific harms sequentially as they are identified and assessed. The Privacy Act Review and the Stage 2 Review of the Model Defamation Provisions provide useful law reform models to explore, and speak to the complexity of the harms on digital platform services that would not lend themselves to connection under a single framework.

K. DIGI encourages several key considerations that should be considered in all regulatory tools aimed at digital platform services, as detailed above.

L. DIGI encourages the Australian Government to develop "a digital economy assessment framework" where foundational and emerging policies across a range of departments can be evaluated against agreed principles, such as those above, and as other Governments have done. and for their impact on Australia's goal to be a leading digital economy by 2030.

M. Targeted promotion of regulatory tools to relevant industry participants should be a baseline requirement upon finalisation, and awareness in key audiences should be assessed.

N. There should be a minimum period where a regulatory tool is in force (e.g. 18 months) and a review process that assesses the effectiveness of the tool in solving the defined policy problem.

O. Thet DP-REG might consider a role in relation to assisting the coordination of various code development processes to avoid duplication in content, and overlapping timelines.

P. The ACCC should further explore further novel approaches such as codes in consultation with associations with experience of relevant code development.

Q. Regulatory frameworks in relation to digital platform services in Australia should align with established global standards, developed by like-minded Governments. Any differences from

[20] AlphaBeta (2019), *Australia's Digital Opportunity*, accessed at: https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf

those global standards should be grounded in evidence of differences in relation to the Australian context that necessitates a departure.

Chapter 8: Potential new rules and measures

8. Addressing data advantages

Discussion paper consultation question:. A number of potential regulatory measures could increase data access in the supply of digital platform services in Australia and thereby reduce barriers to entry and expansion such as data portability, data interoperability, data sharing, or mandatory data access. In relation to each of these potential options:
a) What are the benefits and risks of each measure?

...
d) What types of safeguards would be required to ensure that these measures do not compromise consumers' privacy?

Proposals have major privacy implications

8.1. The proposals advanced in this section of the Discussion Paper have significant implications for user privacy, as the Discussion Paper notes in its statement that: "Consumer and privacy impacts should be carefully considered before implementing proposals to increase data access, including the extent of consumer controls and the types and extent of data to be shared." This demonstrates a level of conflation between consumer harms, competition and privacy law. We therefore believe that questions relating to data access should primarily be considered as part of the Privacy Act Review.

8.2. There are fundamental implementation questions in relation to the proposals around interoperability of services and data access in relation to their technical feasibility, as well as consumer privacy concerns. The digital platform services market is not homogenous, and features are not always standardised in the way they might be in other markets (e.g. banking).

8.3. Additionally, mandating data sharing across platforms may be at odds with user expectations of privacy, and digital platform services' privacy policies.

8.4. We would recommend a specific consultation focus with industry on these proposals, assessing both technological feasibility, competition and privacy concerns.

Data analysis rather than data volume confers advantage

8.5. In relation to "excessive online tracking", the Discussion Paper posits that:

> *Data often confers a competitive advantage in the supply of some digital platform services. As such, digital platforms have an incentive to collect large amounts of data on consumers' online and offline activities.*

DIGI challenges this premise as we believe that *the quality of data analysis* provides more competitive advantage than the *volume* of data collected.

8.6. An argument that more data equates to more advantage is akin to arguments that "data is the new oil", which have been refuted by economists because it is not a scarce commodity, is nonrival, and cannot be monopolised. As the Progressive Policy Institute states in a report titled *The Economic Impact of Data: Why Data Is Not Like Oil*:

> *The analysis conventionally used to assess the value of physical commodities does not effectively capture the value of data. Unlike physical commodities, data can be reused, is not scarce, cannot be controlled and monopolized by a small number of owners, and has little inherent value alone (without being analyzed). These characteristics affect the design of privacy rules*[21].

8.7. Academic Peter Leonard, from UNSW Business School, further argues that:

> *Valuation of so-called 'data rich' businesses is sometimes confused by failure to distinguish between the quantity and range of data sets that a business holds, and the capabilities (or lack thereof) of a business to transform those data sets into actionable insights or other sustainable business advantage*[22].

The ACCC may consider further testing its hypothesis of causal relationship between data volume and competitive advantage.

9. Harms and additional measures identified by the ACCC

Discussion paper questions: What additional measures are necessary or desirable to adequately protect consumers against: a) the use of dark patterns online b) scams, harmful content, or malicious and exploitative apps?

Tracking is a privacy issue

9.1. Without a clear connection to competition (as explored above), DIGI believes that "excessive online tracking" is best considered as a data protection issue within the Privacy Act review. Data protection reform is the appropriate forum to contemplate such issues, rather than consumer protection and competition reform.

9.2. To that end, we encourage the Attorney General's Department and the OAIC to further explore the threshold of "excessive", 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 "excessive online tracking".

---

[21] Progressive Policy Institute (2019), *The Economic Impact of Data: Why Data Is Not Like Oil*, accessed at https://www.progressivepolicy.org/wp-content/uploads/2017/07/PowerofData-Report_2017.pdf

[22] Competition Policy International (2019), *Dynamic Competition In Dynamic Markets: A Path Forwards* (conference summary), accessed at https://www.competitionpolicyinternational.com/wp-content/uploads/2020/04/post-conference-summary-1.pdf

Transparency and control over data are privacy issues

9.3. Similarly, DIGI believes that questions of user transparency and control over how their data is used are also privacy issues. We believe that the current Privacy Act Review provides an important opportunity to advance these objectives, and is the appropriate forum for related questions to be advanced.

9.4. Several privacy-related harms that the ACCC identifies in the Discussion Paper would be addressed through recommendations advanced in the October 2021 Discussion Paper released by the Attorney General's Department in relation to the Privacy Act Review. For example, the Discussion paper identifies risks to consumers from increased profiling of children, both of which would be addressed through the following Privacy Act Review recommendation, which DIGI supports:

> *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.*[23]

9.5. DIGI believes that innovative pro-privacy practices are critical to the long term success of an Australian digitally-enabled economy, and DIGI's members believe that such practices go beyond merely providing privacy policies and notices, and extend to strong accountability-based practices and user controls. They continue to make extensive investments in the privacy of their users, including: having cross-functional privacy experts and teams who ensure that privacy is built into their products and services ('privacy by design'); providing information and tools to provide people with transparency, choices and control in relation to their personal data; and recognising their customers' rights to access, delete, correct and control personal data as part of global data protection frameworks including the Australian Privacy Act and the GDPR.

---

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

9.6. From this standpoint, DIGI refutes the argument made in the Discussion Paper that: "A lack of transparency in data practices and meaningful consumer control over their user data are just some examples of the consequences of a lack of competition and information asymmetries present in digital platform markets." 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 – and the control and transparency provided to users – 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. This underscores the importance of economy-wide privacy reform in giving all Australian baseline standards of transparency and control, no matter what product or service they are using.

9.7. Therefore, we do not believe the Discussion Paper successfully prosecutes a strong connection between privacy issues and competition issues, and we encourage the consideration of privacy matters to continue to fall with the relevant regulator, the OAIC, and the Attorney-General's Department who are leading the reform of the Privacy Act.

Online scams

9.8. DIGI acknowledges the emergence of new types of financial fraud and scams in digital services and the harm they cause victims. This is a complex crime and solutions must be holistic, involving relevant digital and financial services providers as well as functions of the state, including law enforcement and criminal justice. Consumer awareness raising is a vital part of this effort.

9.9. We recognise that scams are a consumer issue, and it is important that the next phase of the ACCC's inquiry examines where online scams are most prevalent and carefully designs and consults on potential interventions to target the heart of the issue and deliver positive outcomes.

9.10. As noted in Table 1, relevant DIGI members also have restrictions on organic as well as paid content in relation to scams, spam, fraud and other deceptive conduct. This includes phishing, impersonation and misrepresentation. In addition, many of them work closely with various organisations including ACCC's Scamwatch to both identify and act on trends in scams and criminal behaviours.

9.11. Where a platform's reporting or other protection measures are not utilised by a consumer, or they are not successful in offering consumers redress in relation to a scam, regulators and Government agencies should provide consumers with a safety net through which to escalate their concern. As well as the ACCC's Scamwatch program, there is an extensive dispute resolution infrastructure across State Offices of Fair Trading.

9.12. An assessment of customer awareness and existing regulatory avenues, with attention to both their capability and cooperation in addressing complaints related to scams, would serve to meaningfully advance the question posed in the Discussion Paper around how consumer protection in relation to scams can be improved.

9.13. It is worth pointing out that digital platform services are naturally limited from enacting their consumer protection measures if a consumer chooses to leave the platform and

interact directly with the entity propagating the scam. While some digital platform services work to direct consumers away from this "off-platform" activity – such as through restrictions to stop buyers and sellers attempting to complete or facilitate outside transactions or connections – the outright prevention of such activity may equally cause consumer complaints and competition concerns.

9.14. It is also worth noting that mainstream platforms and brands often have their names misused and cited in scams in an effort to convince consumers of their veracity. For example, the ACMA has reported a sharp rise in scammers falsely purporting to represent eBay[24]

9.15. In addition to platform measures, Government safety nets and cooperation, DIGI believes that a long term solution here is to improve digital literacy across the community to reduce susceptibility to scams no matter where they present. DIGI welcomes the community information and education provided on scams on both the ACCC Scamwatch website[25], and the Office of the eSafety Commissioner website[26]. DIGI would encourage the proactive provision of such information through targeted communications campaigns that reach at risk populations who may not be actively seeking the information, and would be happy to explore with our members how such efforts could be supported.

"dark patterns online"

9.16. As noted, we believe that further exploration of "dark patterns online" should be addressed in Privacy Act reform. This reform process is contemplating proposals for how to improve individuals' privacy rights and user-facing privacy notices, which will be an important transparency and redress tools in this context.

9.17. DIGI agrees that consumers should be able to make informed choices in their online interactions and be protected from exploitative or manipulative. However, we do not believe the Discussion Paper makes a clear case as to what constitutes a "dark pattern online" to differentiate this activity from marketing that occurs in an online and offline environment. Is a "dark pattern online" analogous to a supermarket placing low-priced consumer items at the checkout counter to entice further purchases? Is it analogous to a clothing store offering a discount at the checkout counter if customers provide an email address to be added to their mailing list, without providing a printed privacy policy to the consumer? Such practices are common in a retail environment, and we believe that further analysis and differentiation of this "dark patterns" concept needs to occur, with a focus on consumer harm.

"harmful content"

9.18. DIGI points to Table 1 in mapping harmful content and responses on digital platform services, and its recommendations in Section 1 as to what additional measures can be taken.

---

[24] ACMA (2021), *Scam alert: ACMA warns of eBay scam phone calls*, accessed at https://www.acma.gov.au/articles/2021-03/scam-alert-acma-warns-ebay-scam-phone-calls
[25] ACCC, About Scamwatch, accessed at https://www.scamwatch.gov.au/about-scamwatch
[26] Office of the eSafety Commissioner, *Online scams and identity theft*, accessed at https://www.esafety.gov.au/key-issues/staying-safe/online-scams-identity-theft

"malicious and exploitative apps"

9.19. It is worth pointing out that the OSA codes, detailed in Table 1, must cover the industry sections of app distribution services (i.e. app marketplaces) and designated internet services (i.e. apps). To the extent that exploitative apps may contain Class 1 content or Class 2 content, they will soon have enforceable measures once the codes are registered by the eSafety Commissioner.

9.20. Additionally, the Basic Online Safety Expectations (BOSE) also covers all "designated internet services", which includes apps. Under the BOSE, such providers must have terms of use and clear and readily identifiable mechanisms that enable end-users to report, and make complaints about, breaches of the service's terms of use. It also includes obligations to make information about these available to the eSafety Commissioner on request. This instrument can also be used to address malicious and exploitative apps.

10. Dispute resolution

Discussion paper consultation question: Should specific requirements be imposed on digital platforms (or a subset of digital platforms) to improve aspects of their processes for resolving disputes with business users and/or consumers? What sorts of obligations might be required to improve dispute resolution processes for consumers and business users of digital platform services in Australia?

10.1. In its analysis of dispute resolution on digital platforms, the Discussion Paper quotes the press release from recent research conducted by the Australian Communications Consumer Action Network (ACCAN) has found that nearly three in four Australians would like better complaints handling from digital platforms[27]. The press release states "digital platforms such as Facebook, WhatsApp, eBay, and Service NSW" and that "Digital platforms were defined as websites and apps such as social media, Government online services, job search sites, dating apps, messaging apps and online marketplaces." This means that the data includes Australians' interactions with Government services such as ServiceNSW and myGov, many of which were being used more frequently during the pandemic. Therefore, this data does not provide a conclusive picture of Australians' experiences of dispute resolution on privately-owned digital platform services. We note that this is the only data provided in this Discussion Paper that labels dispute resolution as "ineffective", and therefore question the veracity of the conclusion.

10.2. Digital platform services have a range of processes to resolve disputes, online mechanisms for Australian consumers to report breaches of consumer law, scams and spam and online safety regulations; and collaborations with relevant regulators. There is an extensive dispute resolution infrastructure across Australian consumer and online safety law, and regulatory bodies such as the OAIC, the ACMA, the Office of the eSafety Commissioner and the State Offices of Fair Trading. While the Discussion Paper advocates for a new ombudsman scheme, it does not consider whether there are gaps in

[27] Australian Communications Consumer Action Network (ACCAN), Media release 29/11/21, *New research finds nearly three-quarters of Australians want better complaints handling from digital platforms*, accessed at https://accan.org.au/media-centre/media-releases/1942-new-research-finds-nearly-three-quarters-of-australians-want-better-complaints-handling-from-digital-platforms#:~:text=New%20research%20from%20the%20Australian,%2C%20eBay%2C%20and%20Service%20NSW.

the current *capabilities* and *capacities* of Australian regulators in providing Australians with a suitable safety net when the dispute resolution processes within digital platforms do not operate as intended. As an illustrative example, the Office of the eSafety Commissioner has said that many victims come to them after an unsuccessful experience with the police. This anecdotal experience would suggest that consumers may need to approach multiple agencies or channels within government before they are able to resolve their issue.

10.3. Furthermore, under the relevant laws, regulators have significant powers to take strong enforcement action in the courts on behalf of consumers where necessary. Australia has a wide variety of alternative dispute resolution mechanisms including small claims tribunals that deal effectively with a range of consumer issues. If consumers are unsatisfied with the outcome they receive from a complaint to a regulator, or in a tribunal or a court, it does not necessarily mean the system has failed, nor does it equate to a gap in the system. This same principle should apply to the perception of complaints made to digital platforms.

10.4. We would argue that an analysis of assessment of customer satisfaction of these existing regulatory avenues, and their capability in addressing complaints that have a digital dimension, would complement the analysis being undertaken on digital service platforms, and together would serve to meaningfully advance the policy questions behind this work. If such data is not readily available, the ACCC might consider a consumer study that explores their experience of these regulatory avenues for the escalation of disputes.

10.5. DIGI is also concerned that the exploration of "dispute resolution" does not appear to be predicated on a clear definition of how a "dispute" or "complaint" is defined. A lack of definitional clarity may equate a "complaint" or "dispute" with other issues requiring customer service support. Furthermore, a high volume of customer inquiries can be indicative of a range of things, including responsive customer service.

10.6. A "dispute" and "complaint" may include any objections that consumers might have about viewpoints lawfully expressed by other users that do not contravene platforms' Terms of Service or regulations that are designed to address societal harms. For example, platforms often experience a high volume of user reports on content that is not violative of their terms of service, in situations where there are impassioned or polarised views. The scope of these kinds of disagreements is infinite; the ACCC should be wary of suggesting that all issues between Australian consumers and platforms -- regardless of their cause or nature, whether or not they concern a product, service or platform user -- represent a policy problem that requires a response from the Government, particularly in cases where comparable "disputes" offline would not be subject to any government intervention.

10.7. On this point, in 2014 the Productivity Commission released a report into Access to Justice examining the role, gaps and capabilities of ombudsman services, amongst other issues[28]. While the Productivity Commission found that ombudsmen generally deliver dispute outcomes at far lower cost than courts, visibility and co-ordination between the various services remains challenging. The ACCC should consider reviewing Chapter 9.3 of this report to explore whether improvements have been made in the intervening years.

[28] Productivity Commission, *Access to Justice Arrangements Productivity Commission*, accessed at: *Inquiry Report Volume 1*, available at https://www.pc.gov.au/inquiries/completed/access-justice/report/access-justice-volume1.pdf

10.8. DIGI is concerned that an independent ombudsman scheme has the potential for considerable overlap and contradictory decision-making with other regulators. More channels does not necessarily mean better consumer outcomes. Conversely, more channels may create greater consumer confusion as users are given the "runaround" to call different agencies to resolve a single issue. DIGI therefore suggests that focus be placed on co-operation mechanisms and consumer communication about existing dispute resolution avenues. In practice, this might take the form of a website that maps the avenues available to consumers in relation to different harms. It may also take the form of a memorandum of understanding between relevant regulators around the triaging and direction of consumer complaints relating to other portfolio areas.

10.9. In relation to an ombudsman scheme, we would question the capability and capacity of a single ombudsman to effectively address the wide range of consumer concerns and online harm that arise in the digital world. Many consumer concerns relate to the contextual application of a digital platform's services in a variety of sectors; centralised bodies may lack the necessary subject matter and technical expertise to meaningfully assist consumers. Improving the ability of all relevant government agencies and regulators to address both harms and consumer issues that have a digital dimension becomes extremely important as people live more of their lives online, especially as we move towards the Government's stated goal of Australia becoming a leading digital economy. Ensuring this capability across Government is in line with consumer expectations in a digital economy.

11. Algorithmic transparency

16. In what circumstances, and for which digital platform services or businesses, is there a case for increased transparency including in respect of price, the operation of key algorithms or policies, and key terms of service?

11.1. DIGI agrees that digital platform services' terms of service and other key user-facing policies should be transparent.

11.2. DIGI does not believe that requirements to disclose specific technical details of the way in which algorithms operate, such as detailed information on the signals and predictions used, would not provide meaningful transparency to Australians. They may serve to enable third parties to more easily game the system. For example, in the case of algorithms that are used to detect and remove harmful content, making them public would allow bad actors to manipulate posts to evade algorithm changes. In the immediate aftermath of the terrorist attacks in Christchurch in March 2019, platforms reported an unprecedented number of people actively manipulating the livestreamed footage of the attacks to avoid detection by algorithms.

11.3. Instead, DIGI is supportive of regulatory approaches to mitigate against defined harms, rather than those that are focused on specific technologies such as algorithms or AI. A harms-based approach reflects that the majority of potential problems associated with AI lie in the contextual application of the technology in a variety of sectors, and we caution against recommendations focused solely on reviewing the technology of AI itself.

Summary of recommendations in relation to Chapter 8

R. Data access proposals, dark patterns online, excessive online tracking and questions of data transparency and control should be addressed as part of the Privacy Act Review.

S. As scams present in a variety of mediums and often “off-platform”, regulatory safety nets where consumers can escalate scams are crucially important in complementing platform-level efforts. This is relevant to scams, and dispute resolution more broadly. An assessment of both customer awareness and cooperation between relevant regulators would serve to meaningfully advance the question posed in the Discussion Paper around how consumer protection in relation to how both scams and dispute resolution redress can be improved.

T. DIGI recommends that a long term solution here is to improve digital literacy across the community to reduce susceptibility to scams no matter where they present.

U. DIGI recommends a focus on regulatory approaches that mitigate against defined harms, rather than those that are focused on specific technologies such as algorithms or AI.

Appendix: Overview of digital platform service issues, platform & regulatory responses

Table 1[29]

Description of issue	Trends in platform responses	Australian regulatory responses
Individual harms		
12. Cyberbullying material directed at an Australian child	12.1. All relevant DIGI members have strict policies to prohibit and rapidly remove the cyberbullying of Australian children and minors. These policies are regularly updated to ensure they reflect emerging patterns of abuse, in consultation with experts. 12.2. They provide reporting tools where content can be reported for cyberbullying. Such messages are reviewed by teams of human moderators, and addressed as quickly as possible. Enforcement actions include the removal of cyberbullying content, and the suspension or removal of accounts that have instigated it. 12.3. This enforcement infrastructure is often complemented with proactive technology detection that detects problematic content and flags it for human review.	12.6. The Enhancing Online Safety Act 2015 (EOSA) allowed Australian minors who are the target of cyberbullying material, and those representing them, to complain to the Office of the eSafety Commissioner (the Commissioner). The Commissioner can direct a request for removal to the social media service, and the service must remove the content within 48 hours. The Online Safety Act (OSA), which entered into force on January 23, 2022, reduced the timeframes that a social media service must respond to 24 hours. 12.7. The Basic Online Safety Expectations (BOSE), which came into effect with the OSA on January 23, 2022 includes core expectation of the BOSE is that a provider of a service must take reasonable steps to minimise the extent to which cyberbullying material targeted at an Australian child or adult is available, and to make reports about the provider's related activities available to the Commissioner. **The BOSE contains a broad-ranging set of expectations for all social**

[29] DIGI wishes to emphasise that industry approaches will differ based on the services they provide, their users and their size. Not all services will experience the full range of issues, and the way that different online harms present themselves on each service will differ, necessitating variations in approach. It is simply a brief summary in order to provide an indication of the industry approach, and is by no means comprehensive.

	12.4. Relevant members provide blocking tools where any user can be blocked from sending further unwanted messages, and provide tools to enable people to leave or hide group forums. 12.5. Industry's policies and enforcement are complemented with a range of initiatives, partnerships and social programs aimed at providing minors with wider support from professionals, parents and teachers in relation to cyberbullying.	**media services, messaging services and websites available in Australia, and DIGI is concerned that its release in January was not promoted to all of these services, nor has the text of the BOSE been made prominently available to industry, raising questions around whether all affected service providers are aware of their new compliance obligations**[30]. 12.8. The EOSA and OSA children's cyber bullying schemes enable the Commissioner to issue end-user notices that require a person who posts cyberbullying material to remove the material, refrain from posting any cyberbullying material targeting the child, and/or apologise to the child for posting the material. 12.9. Section 474.17(1) of the Criminal Code 1995 (Cth) creates an offence of using a carriage service to menace, harass or offend another person.
13. Cyberbullying material targeted at an Australian adult	13.1. All of the measures outlined above from 12.1 to 12.5 (policies, tools, enforcement teams and technology) apply to the approach to cyberbullying material targeted at an Australian adult. 13.2. Digital platforms often have granular considerations when assessing the cyberbullying of adults, such as whether the content concerns public opinions or actions that impact others, and the extent to which the content relates to a person in authority or a public figure. The questions a	13.3. The OSA includes an adult cyber-bullying scheme where Australian adults who are the victims of seriously harmful online abuse can complain to the Office, if the online service providers have failed to act on reports to them. The Office can direct a request for removal to the social media service, and the service must remove the content within 24 hours. 13.4. The BOSE and Section 474.17(1) of the Criminal Code 1995 (Cth) detailed above in 12.7 and 12.9 also apply to adult cyberbullying.

[30] A page about the BOSE exists on the Office of eSafety Commissioner's website under "who we are". However, it does not contain a direct link to the BOSE. An industry participant must search the Federal Register of Legislation to find the final text of the determination. See: https://www.esafety.gov.au/about-us/who-we-are/basic-online-safety-expectations A web page exists on the The Department of Infrastructure, Transport, Regional Development and Communications' website about the BOSE, but only appears to contain a copy of the draft instrument. See: https://www.infrastructure.gov.au/have-your-say/draft-online-safety-basic-online-safety-expectations-determination-2021-consultation

	provider may ask will necessarily differ based on the service, and provide important checks and balances for platforms to appropriately consider the freedom of expression, and political communication, implications of a takedown decision.	13.5. In relation to end users, the Australian Government made an election commitment May 5, 2019 to increase maximum penalties for end-users who use a carriage service to menace, harass or cause offence to five years of imprisonment[31].
14. Child sexual abuse material (CSAM)	14.1. DIGI members have zero tolerance for CSAM. They have strict policies against child exploitation and the sexualisation of children. These policies are enforced through human review teams who undergo extensive training on the appropriate protocols for the handling of CSAM material, often with machine learning and other technology that surfaces content for review. 14.2. When CSAM is detected it is removed and reported, DIGI members report to the National Center for Missing & Exploited Children (NCMEC) in the United States which refers cases to law enforcement all around the world, including in Australia. They also directly cooperate with Australian law enforcement operations. 14.3. Relevant DIGI members are active in several coalitions, such as the Technology	14.5. The Online Content Scheme (Schedules 5 and 7 of the Broadcasting Services Act 1992) enables the eSafety Commissioner to investigate and take action on complaints about prohibited online content such as child sexual abuse material (CSAM). 14.6. The OSA, and the EOSA that was previously in force, include a removal scheme for child sexual exploitation material. The Commissioner can direct a request for removal to the social media service, and the service must remove the content within 24 hours. 14.7. The AVM Act, detailed above, covers CSAM depicting rape or toruture, which has been the subject of 98% of notices served under the Act[32]. 14.8. Furthermore, the OSA Codes (detailed earlier in this submission and above in 23.10 and 23.11), relate to "Class 1" and "Class 2" materials under Australia's classification code. The list of Class 1

[31] See media release: Prime Minister The Hon Scott Morrison MP, Attorney-General The Hon Christian Porter, Senator The Hon Mitch Fifield Minister For Communications And The Arts, Joint Media Release (05/05/2019), "Keeping Australians Safe Online", accessed at https://www.liberal.org.au/latest-news/2019/05/05/keeping-australians-safe-online
See also transcript: Prime Minister The Hon. Scott Morrison MP (05/05/2019), Transcript Remarks, Campaign Rally Central Coast, accessed via CCH alerts, see quote: *"But the other thing we're going to do for all Australians, is we're going to increase the penalties for those who have been found to be bullying people online, causing those injuries. You won't go to jail for three years, you'll go to jail for five years."*

[32] Parliamentary Joint Committee on Law Enforcement, *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019*, report released December 2021, accessed via CCH political alerts.

	Coalition, the ICT Coalition, the WeProtect Global Alliance, and INHOPE and the Fair Play Alliance, that bring companies and NGOs together to develop solutions that disrupt the exchange of child sexual abuse materials online and prevent the sexual exploitation of children. 14.4. Relevant DIGI members deploy industry-developed and licensed technological tools such as Photo DNA (developed by Microsoft to identify known CSAM in still images) and CSAI Match (developed by YouTube to detect known video-based CSAM).	materials includes CSAM. 14.9. The BOSE, which came into force with the OSA on January 23 2022, contains a specific expectation in Section 8 that service providers that use encryption with their services will implement processes to detect and address material or activity on the service that is unlawful or harmful.
15. Non-consensual sharing of intimate imagery	15.1. Relevant DIGI members have strict policies that do not allow the sharing of non-consensual intimate images, and work to rapidly remove these. 15.2. These policies form part of broader policies to remove content that promotes sexual violence, sexual assault or sexual exploitation. 15.3. As with other policy areas described above, these policies are enforced through a combination of human review, proactive machine learning technology and enforcement teams. 15.4. Some platforms have also introduced preventative measures that use image hashing technology to prevent the spread of known image-based abuse images, in order to prevent the reliance on user	15.5. The OSA includes a removal scheme where people who are the victims of the sharing of non-consensual intimate images may complain to the Commissioner if online service providers have failed to act on reports to them. The Office can direct a request for removal to the social media service, and the service must remove the content within 24 hours. 15.6. A core expectation of the BOSE is that a provider of a service must take reasonable steps to minimise the extent to which non-consensual intimate images are available, and to make reports about the provider's related activities available to the Commissioner.

	reporting.	
16. Minors' access to pornography and other age-inappropriate content	16.1. All members have strict content policies in relation to pornographic content. On social media and content platforms, there are policies in their community guidelines restricting nudity, pornography and sexually explicit content. On search engines, sexual and violent terms are removed from auto-complete and pornography is demoted in search results unless the user is clearly searching for it. These policies are enforced through a combination of human moderation and machine learning that detects high numbers of flesh coloured pixels. 16.2. These policies are also reflected in members' advertising policies. For example, Google Search does not allow hyperlinks that drive traffic to commercial pornography sites, nor does it allow pornography ads to be placed within its search engine, nor does it run Google ads against pornographic websites. On social media and content platforms, all members have strict controls on pornography, adult products and services, and nudity. 16.3. 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	16.5. 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. 16.6. 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. The OSA Codes will contain commitments from industry to minimise the risk of harm to Australian minors due to the accessibility of Class 2 materials online. 16.7. Additionally, when the OSA entered into force on January 23, 2022, it was accompanied by a new Restricted Access System (RAS) which requires that social media services, messaging services and websites limit access to certain age-inappropriate material through the implementation of an access control system. This

	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. 16.4. 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	will replace the 2014 Restricted Access System declaration[33]. 16.8. In addition, the eSafety Commissioner is currently conducing a roadmap on age verification (AV Roadmap) that was a result from Government's parliamentary inquiry into age verification for online wagering and online pornography. We understand that consultations are continuing and that the AV roadmap will be presented to the Government in 2022[34]

[33] Office of the eSafety Commissioner (2021), *Restricted Access System Declaration Online Safety Act 2021 Discussion Paper August 2021*, accessed at https://www.esafety.gov.au/sites/default/files/2021-08/OSA%20-%20Restricted%20Access%20System%20discussion%20paper_0.pdf

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

	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.	
17. Advocacy of suicide and self-harm	17.1. Relevant DIGI members have policies prohibiting the advocacy of suicide and other self-harm. These policies extend beyond the rapid removal of such content, but aim to provide those at risk with links to services that may assist them. For example, searches relating to suicide on platforms link to Lifeline and other relevant support organisations. Flags for suicide and self injury are escalated and addressed with urgency. 17.2. Relevant larger platforms partner with mental health organisations in Australia to produce or promote a range of training and other support resources. 17.3. Such policies and partnerships also extend to material that glorify eating disorders such as anorexia nervosa, and bulimia.	17.4. Australia was the first country to criminalise pro-suicide websites in 2006 through the Criminal Code Amendment (Suicide Related Material Offences) Act 2005. 17.5. It is possible that the aforementioned OSA codes to be registered in 2022 pertaining to Class 2 content cover such content in scope. As noted, Class 2 content has been defined as including "themes" that include "social Issues such as crime, suicide, drug and alcohol dependency, death, serious illness, family breakdown and racism."
18. Defamation	18.1. Relevant DIGI members have policies that restrict the usage of their services for the defamation of others. 18.2. They have complaints handling processes in place to action defamation requests received by Australian users, which are	18.3. Defamation laws differ by state and territory in Australia, however the Model Defamation Provisions have played an important role in harmonising state-based defamation laws that existed prior to 2005. These provisions were not written for a digital age, and the Council of Attorneys-General Defamation Working Party on

	actioned in accordance with Australian law. These policies seek to balance allowing individuals to protect their reputations without placing unreasonable limits on the discussion of matters of public interest and importance. Given that defamation is a civil matter and can depend on whether the originator of a comment has a lawful defence for posting the comment, it can be challenging for platforms to make assessments in the absence of judicial or independent determinations.	the Review of Model Defamation Provisions (MDPs), with a "Stage 2" process currently well underway to ensure these provisions are fit for a digital age. DIGI is supportive of modernising these provisions to offer better solutions for Internet users and online intermediaries with regard to defamation. 18.4. From recent engagement with this defamation law reform process, DIGI understands that the NSW Law Reform Commission is considering a complaints notice process, debating using Section 5 of the UK 2013 Defamation Act as a starting point.
Collective harms		
19. Hate speech	19.1. All relevant DIGI members have strict policies to prohibit and address hate speech or conduct, which is generally defined as speech that maligns people or a group of people based on their protected characteristics, e.g. race, gender, sexuality. 19.2. These policies have and continue to evolve to capture emerging patterns and themes in hate speech or hateful conduct. Additionally, relevant members consult with a wide range of organisations and individuals who guide them in their policy decisions. 19.3. All of the measures outlined above from 12.1 to 12.5 (policies, tools, enforcement	19.5. DIGI members take the aforementioned actions on hate speech under their own policies, despite no explicit and comprehensive legal protections for Australians under Australian law for hate speech. 19.6. Australia continues to adopt a narrow approach to hate speech under anti- discrimination laws that are aimed at protecting individuals rather than groups based on their protected characteristics. **19.7. Identified gap: DIGI identifies hate speech as a policy gap, and has and continues to encourage the Australian Government to develop a clearer legislative framework that defines hate speech[35]. This will also serve to help relevant stakeholders, including digital platforms, to better report, review and remove content that meets a defined**

[35] DIGI, Submission to Department of Communications on the Online Safety Charter (2019), accessed at https://digi.org.au/advocacy/#:~:text=Online%20Safety%20Charter%20%7C%20Submission%20to%20Department%20of%20Communications

	teams and technology) apply to the approach to hate speech. 19.4. Industry policies and enforcement are complemented with a range of initiatives, partnerships and social programs aimed at preventing and addressing hate speech.	**Australian legal threshold.**
20. Pro-terror material and the incitement of violence	20.1. DIGI members comply with Australian law and swiftly remove content that violates it, across a range of subject matter areas, including pro-terror content. They also work to report such content to law enforcement, where appropriate. 20.2. Their policies prohibiting illegal pro-terror content form part of broader policies that prohibit the incitement or glorificaiton of violence, and they rapidly remove content that may result in the credible risk of physical harm or direct threats to public safety. 20.3. These policies are enforced through reporting tools, where end-users can escalate policy-violating content, and often through machine learning technology that proactively identifies potentially problematic content before many people have consumed it, both of which generally trigger a human review. 20.4. With regard to pro-terror content specifically, several relevant DIGI members created a shared industry database of unique digital fingerprints, known as	20.7. The Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (AVM Act), passed in April 2019 requires content, internet and hosting providers to, within a reasonable time, report to the Australian Federal Police abhorrent violent conduct that is happening in Australia and accessible through their services, or hosted on their services. 20.8. Additionally, the AVM Act requires the expeditious removal of abhorrent violent material, and provides the eSafety Commissioner the power to notify service providers that abhorrent violent material is available on their services. These notices create a presumption that the provider is aware of the material and puts providers on notice that such material should be removed[38]. 20.9. The OSA also includes blocking notices for Internet Service Providers for abhorrent violent conduct, alongside requirements for the takedown of other prohibited material detailed elsewhere in Table 1. **Identified gap: For clarity and to aid compliance across the breadth of in-scope companies, DIGI recommends the AVM Act be incorporated into a consolidated Online Safety Act.** 20.10. Furthermore, under the OSA, industry associations

[38] Attorney-General's Department, *Abhorrent violent material*, accessed at https://www.ag.gov.au/crime/abhorrent-violent-material

	"hashes", of known violent terrorist imagery or terrorist recruitment videos that had been removed from their services. Today, that database is used by thirteen companies that are members of the Global Internet Forum to Counter Terrorism (GIFCT). Companies rapidly used this database within hours of the Christchurch terrorist attacks adding over a thousand visually-distinct videos related to the attack to it. Crucially, these hashes were shared with smaller businesses to help stop the proliferation of this content on platforms that may not otherwise have the technology and resourcing of larger companies. 20.5. This hash database is one example of industry collaboration that is occurring through the Global Internet Forum to Counter Terrorism (GIFCT), an NGO founded by several DIGI members that aims to (i) build shared technology to prevent and disrupt the spread of terrorist content online (ii) conduct and funding research by international experts, and (iii) share information and best practices with businesses of all sizes to assist them in managing this content on their platforms. Since 2017, GIFCT's membership has expanded beyond the founding companies, and it has become an independent organisation. 20.6. As one of several of its workstreams, the	have been asked to develop the new mandatory codes of practice to regulate all online services and websites available in Australia. These OSA codes are intended to be registered in 2022[39]. On September 29, 2021, the Office of the eSafety Commissioner released a position paper[40] outlining expectations for the OSA codes. 20.11. In subject matter, the OSA codes will relate to "Class 1" and "Class 2" materials under Australia's classification code. The list of Class 1 materials includes pro-terror content. While there are specific requirements outlined in the position paper, at a high level, the OSA 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. 20.12. Following the devastating Christchurch terrorist attacks, the Australian Government established the Taskforce to Combat Terrorist and Extreme Violent Material Online (the Taskforce). Relevant DIGI members participate in the Taskforce, which provided 30 recommendations on practical, tangible and effective measures and commitments to combat the upload and dissemination of terrorist and extreme violent material, including the development of Australia's Domestic Online Crisis Response Protocol (the Protocol). The Protocol aligns with the GIFCT CIP, and is seen as a domestic implementation of the Christchurch Call to Action[41]. **20.13. Identified gap: DIGI recommends the Australian**

[39] *Online Safety Act 2021*, see Part 9, Division 7, accessed at: https://www.legislation.gov.au/Details/C2021A00076
[40] Office of the eSafety Commissioner, *Development of industry codes under the Online Safety Act: Position Paper*, accessed at https://www.esafety.gov.au/about-us/consultation-cooperation/industry-codes-position-paper
[41] *Christchurch Call to Eliminate Terrorise & Violent Extremist Content Online*, available at https://www.christchurchcall.com/call.html

		GIFCT has developed The Content Incident Protocol (CIP) to respond to emerging and active terrorist events, and assess any potential online content produced and disseminated by those involved in the planning or conducting of the attack. When the GIFCT declares the CIP is in force, all hashes of an attacker's content are shared among the GIFCT's members, and a stream of communication is established between them. The first CIP was activated on October 9 2019, following the shooting in Halle, Germany[36]. In the wake of this shooting, the UN organisation Tech Against Terrorism confirmed[37] that measures taken by mainstream digital platforms resulted in a reduction in the virality of the livestreamed footage from Halle and observed that the footage was proliferating in smaller, less moderated forums.		**Government provide further legal clarity by reviewing the protocol for listing terrorist organisations in response to the growing threat from the far right and consider whether new organisations should be added. This might be similar to the FBI list of Foreign Terrorist Organisations and the UK's list of proscribed terrorist groups.**
21.	Misinformation and disinformation	21.1.	Relevant DIGI members have policies and processes to remove or otherwise address the spread and scale of harmful misinformation and disinformation online. As with other policy areas described above, these policies are enforced through a combination of human review, proactive machine learning technology and enforcement teams.	21.9.	DIGI developed the ACPDM in response to Australian Government policy announced in December 2019: "*The Government will ask the major digital platforms to develop a voluntary code (or codes) of conduct for disinformation and news quality. The Australian Communications and Media Authority (ACMA) will have oversight of the codes and report to Government on the adequacy of platforms' measures and the broader impacts of disinformation. The codes will address concerns regarding disinformation and credibility signalling*
		21.2.	To provide a public, consistent and		

[36] Global Internet Forum to Counter Terrorism (GIFCT) website, accessed at https://gifct.org/about/
[37] Tech Against Terrorism (2019), *Analysis: What can we learn from the online response to the Halle terrorist attack?*, accessed at https://www.techagainstterrorism.org/2019/10/15/analysis-what-can-we-learn-from-the-online-response-to-the-halle-terrorist-attack/

	transparent framework for addressing the harm of mis- and disinformation to Australians, in February 2021, DIGI launched the *Australian Code of Practice on Disinformation and Misinformation* (ACPDM). 21.3. Eight major technology companies have adopted the code to date, and signatories have agreed to safeguards to protect Australians from harmful misinformation online. That includes the mandatory commitment (#1) of: 21.3.1.1. Publishing and implementing policies on their approach. 21.3.1.2. Providing a way for their users to report content that may violate those policies. 21.3.1.3. Implementing a range of scalable measures that reduce its spread and visibility online. 21.4. Another mandatory commitment (#7) is releasing annual transparency reports about those safeguards in order to improve public understanding of these challenges over time. The first set of reports were released in May 2021, and are available for anyone to read at digi.org.au. 21.5. The code contains opt-in commitments that have been widely adopted that entail (#2) Addressing disinformation in paid	*for news content and outline what the platforms will do to tackle disinformation on their services and support the ability of Australians to discern the quality of news and information. The codes will be informed by learnings of international examples, such as the European Union Code of Practice on Disinformation. The Government will assess the success of the codes and consider the need for any further reform in 2021."*[43] 21.10. The ACMA provided their report on the effectiveness of the code to the Government on June 30, 2021, per the timeline requested by the Government, which was recently released publicly on March 21, 2022. Alongside the release of the report, the Government announced the strengthening of the ACMA's powers in line with their recommendations to formally oversee the ACPDM, continue to report on its effectiveness, and have formal information gathering powers, and reserve powers to register industry codes and create standards as needed. DIGI supports all of the ACMA's key recommendations in principle, and understands that the Government intends to consult on the specifics of these expanded powers in the coming months. Prior to this announcement, the ACMA was not empowered with a formal, long-term role in relation to misinformation and disinformation on digital platform services; **DIGI believes that it is important that different regulators and Government departments are resourced to continue to specialise in their respective areas of expertise as they relate to digital platform services.** 21.11. Misinformation and disinformation relating to

[43] Australian Government (2019), *Regulating in the Digital Age: Government Response and Implementation Roadmap*, accessed at https://treasury.gov.au/publication/p2019-41708

	content. (#3) Addressing fake bots and accounts.(#4) Transparency about source of content in news and factual information (e.g. promotion of media literacy, partnerships with fact-checkers) and (#5) political advertising and (#6) partnering with universities/researchers to improve understanding. 21.6. In October 2021, DIGI announced the strengthening of the code with the appointment of an independent Complaints Sub-Committee comprised of Dr Anne Kruger, Victoria Rubensohn AM and Christopher Zinn to resolve complaints about possible breaches by signatories of their code commitments. DIGI launched a portal on its website for the public to raise such complaints. 21.7. In addition, DIGI appointed an independent expert Hal Crawford to fact check and attest signatories' annual transparency reports going forward under the code, in order to incentivise best practice and compliance[42]. 21.8. DIGI intends to conduct a review of the code in the coming months, where we intend to proactively invite views from the public, civil society and Government about how it can be improved. This review will take into account the ACMA's findings in its recently released report on the code.	elections is covered under the ACPDM however, additionally, DIGI has been working with representatives from the Electoral Council of Australia and New Zealand (ECANZ) on a protocol to reflect how electoral law is achieved on relevant digital platform services.

[42] DIGI Media Release (11/10/21), *Australian disinformation code of practice strengthened with independent oversight and public complaints facility*, accessed at https://digi.org.au/in-the-media/australian-disinformation-code-of-practice-strengthened-with-independent-oversight-and-public-complaints-facility/

Consumer		
22. Advertising of illegal and potentially harmful goods and services	22.1. Relevant DIGI members have broad-ranging advertising policies that prohibit or restrict a long list of illegal and potentially harmful goods and services. These policies are adapted to jurisdictions including Australian law. These policies include, but are not limited to, topic areas such as online wagering, adult goods and services, alcohol and tobacco sales. 22.2. These policies include the prohibition of deceptive, misleading, or harmful business propositions, including restrictions on misleading, false, or unsubstantiated claims during the promotion of a product or service. 22.3. They also have varying restrictions on political advertising, and work with Federal, State and Territory electoral offices to prevent electoral interference, as well as more traditional electoral offences. 22.4. Furthermore, there are restrictions on discrimination in the targeting of advertising to prevent discriminate against legally protected categories of customers. 22.5. Relevant members work hard to ensure that age-regulated advertising content, such as those for alcohol, are not served to minors. 22.6. Advertising requires pre-registration and is reviewed and approved before publishing, and non-compliant ads may be disproved	22.7. Australian Consumer Law applies to digital platforms, and has prohibitions on false and misleading statements, unfair contract terms and provisions relating to consumer guarantees, product safety. This law is administered by the ACCC and the State and Territory consumer protection agencies. 22.8. In relation to online gambling, the ACMA administers the Broadcasting Services (Online Content Service Provider Rules) 2018 (the Rules). The Rules apply to online content service providers who provide gambling promotional content on online content services in conjunction with live coverage of a sporting event. 22.9. There are state and federal electoral laws that apply to digital content. DIGI has been working with representatives from the Electoral Council of Australia and New Zealand (ECANZ) on a protocol to reflect how electoral law is achieved on relevant digital platform services.

	or removed, and repeat offender accounts may be suspended.	
23. Scams, spam and deceptive conduct	23.1. As well as the restrictions on advertising content, relevant members also have restrictions on organic as well as paid content in relation to scams, spam, fraud and other deceptive conduct. This includes phishing, impersonation and misrepresentation. 23.2. All of the measures outlined above from 12.1 to 12.4 (policies, tools, enforcement teams and technology) apply to the approach to scams, spam and deceptive conduct.	23.3. As noted in 12.7, Australian Consumer Law applies to digital platforms, and has prohibitions on false and misleading content. 23.4. The ACCC's Scamwatch program enables consumers to complain to the ACCC that take action where appropriate, including working with industry. Scamwatch provides information to consumers and small businesses about how to recognise, avoid and report scams. State and Territory consumer protection agencies also have reporting and educative functions.[44] 23.5. Relevant DIGI members prohibit scams under their Terms of Service. There are accountability measures built into the Basic Online Safety Expectations (BOSE) which covers all "designated internet services" (i.e. websites accessible to Australian users), "Relevant electronic services" (i.e. email, online messaging and gaming services, including text messages) and "social media services". Under the BOSE, such providers must have terms of use and clear and readily identifiable mechanisms that enable end-users to report, and make complaints about, breaches of the service's terms of use. It also includes obligations to make information about these available to the eSafety Commissioner on request.
Privacy		

[44] NSW Fair Trading, *Scams and cybercrime*, accessed at https://www.fairtrading.nsw.gov.au/buying-products-and-services/scams

24. Privacy intrusion	24.1. 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 includes notifications and privacy communication. Many provide privacy tools to provide people with transparency, choices and control about how their data is used. They have dedicated teams focused on privacy and cross-functional review processes for new products to ensure "privacy-by-design" before they are released. 24.2. Where applicable, they apply the strictest default privacy settings for minors; for example, ensuring that location-sharing is always off by default. 24.3. 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 European Union's General Data Protection Regulation (GDPR) requirements in this area.	24.4. The Privacy Act and the Australian Privacy Principles apply to digital platforms, and DIGI welcomes the current review of these being led by the Attorney General's Department. We see this review as an important opportunity to standardise privacy protections in a digitising economy, and to ensure consumers have a baseline expectation of control and choice when it comes to their privacy. **24.5. There are important recommendations in the Privacy Act Review that the ACCC should monitor closely as part of this inquiry, as they may go some way to address issues of concern. For example, DIGI recommends that the Privacy Act Review proceed with its recommendation that entities that collect or use personal information for activities including automated decision making, direct marketing including targeted advertising identify privacy risks, and implement measures to mitigate those risks[45].** 24.6. Additionally, the Government has released for consultation an exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (OPB). The OPB applies to social media services, large online platforms and data brokerage services.
25. Hacking & threats to cyber security	25.1. DIGI members make extensive investments in personnel and systems to ensure the cyber security of their users. End-to-end encryption is often seen as a core pillar of effective cyber security. 25.2. They work to address a broad range and	25.3. In relation to cyber security, the Department of Home Affairs is currently advancing work on Australia's cyber security regulations and incentives. Most recently, it released options by way of a discussion paper titled *Strengthening Australia's cyber security regulations and incentives*. Options include a mandatory cyber

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

	scale of cyber security threats, including micro threats that typically target individuals -- such as identity theft or phishing scams to macro threats -- to macro threats such as hacking and attacks of institutions that have large volumes of data. Such micro threats require a combination of consumer awareness and encouraging industry best practice, through initiatives by Government and industry and collaborations between them. Certain macro threats, such as those that are state-sponsored will require a range of Government-led mitigation and response efforts in combination with industry efforts.	security standard for smart devices in Australia and/or cyber security labelling. 25.4. On 3 September 2020, the Australian Government released a voluntary code of practice *Securing the Internet of Things for Consumers (Code of Practice)*. This code contains thirteen principles that signal Government expectations to manufacturers about the security of smart products[46]. 25.5. It is not clear today where the responsibilities for Australians' cyber security lie across Government, as many departments consider elements of it to fall under their remit. For example, it is understood that today responsibilities related to cyber security fall across the Australian Cyber Security Centre in the Australian Signals Directorate, the Attorney General's Department, the OAIC, the ACCC, the eSafety Commissioner, the Department of Communications and the Department of Home Affairs. **In light of this, It therefore is not apparently clear to industry nor consumers which government department would be the lead or appropriate port of call for enquiries relating to cyber security. This should be rectified through clearer public communication.**
Copyright		
26. Copyright infringement	26.1. Relevant DIGI members promptly action and address complaints relating to copyright and trademark infringement, through an enforcement infrastructure that	26.2. In Australia, copyright law is governed by the Copyright Act 1968 (Cth) (Copyright Act), and is administered by the Department of Infrastructure, Transport, Regional Development and

[46] Department of Home Affairs, *Voluntary Code of Practice: Securing the Internet of Things for Consumers*, accessed at https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice

	includes human review teams and is often supplemented by technological detection.	Communications. 26.3. This law has been undergoing a reform process for several years with the most recent reform proposal, released in December 2021, was the Copyright Amendment (Access Reforms) Bill 2021[47]. **To date, DIGI has been disappointed that proposals have not extended safe harbour schemes to digital platforms services, nor has a fair use provision been enacted. Such provisions would better reflect how consumers use digital services, and future proof the Copyright Act for innovation in Australia's digital economy.**

[47] Department of Infrastructure, Transport, Regional Development and Communications (2021), *Have your say on draft copyright reform legislation*, accessed at https://www.infrastructure.gov.au/have-your-say/have-your-say-draft-copyright-reform-legislation