September 12, 2019

To: Director
Structural Reform Division
The Treasury

Dear Director,

Thank you for opening a public consultation on the ACCC's final Digital Platforms Inquiry (DPI) report, and for the opportunity to provide a submission.

By way of background, the Digital Industry Group Inc. (DIGI) is a non-profit industry association that advocates for the interests of the digital industry in Australia, with Google, Facebook, Twitter and Verizon Media as its founding members. DIGI also has an associate membership program for smaller digital companies, such as Redbubble and GoFundMe.

DIGI's vision is a thriving Australian digitally-enabled economy that fosters innovation, a growing selection of digital products and services, and where online safety and privacy are protected. DIGI's mission is to advocate for policies that enable a growing Australian technology sector that supports businesses and Internet users, in partnership with industry, governments and the community.

We recognise the importance of the issues raised in the DPI. However, we note that its original terms of reference were to investigate the state of competition in the media and advertising services markets, particularly in relation to news and journalistic content. We are concerned that the final recommendations have unintended consequences for a wide range of digital service providers, organisations that rely upon digital services to market goods and services, consumers of online services, and for the Australian economy.

We therefore urge the Australian Government to fully consider these unintended consequences and undertake necessary broader consultation with the digital industry, as well as other affected industries, before any major reform is announced.

DIGI looks forward to further engaging with the Treasury's consultation process in relation to the DPI, and the Government in relation to any related reform. Should you have any questions about the representations made in this submission, please do not hesitate to contact me.

Best regards,

Sunita Bose
Managing Director
Digital Industry Group Inc. (DIGI)

Maximising Australia's digital opportunity

Earlier this month, a major report about Australia's technology sector called "Australia's Digital Opportunity" was released, produced by AlphaBeta and commissioned by DIGI. It quantifies the extraordinary contribution of Australia's technology sector to the national economy. Today, the technology sector contributes $122 billion each year to the national economy, or 6.6% of GDP[1].

This $122 billion a year comprises two components:

[1] All statistics in this section are from AlphaBeta (September 2019), *Australia's Digital Opportunity*, accessed at: https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf The full report has been attached to the submission as a supporting document.

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.
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.

The sector employs 580 000 workers, or 5% of Australia's working population. 66 000 of those jobs are in regional Australia, with the technology sector contributing nearly $12 billion in economic value to regional areas by enabling regional businesses, local jobs, and improving residents' access to goods and services.

While regulation of the Internet is often focused on large technology companies, the report found that 90% of technology companies are in fact small to medium enterprises (SMEs).

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.

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.

While Australia performs well with technology adoption, as Figure 2 shows, it lags relative to other OECD countries in relation to ICT service exports, among other indicators. One indicator of this is the fact that Australia has few native global scale digital firms.

Figure 1

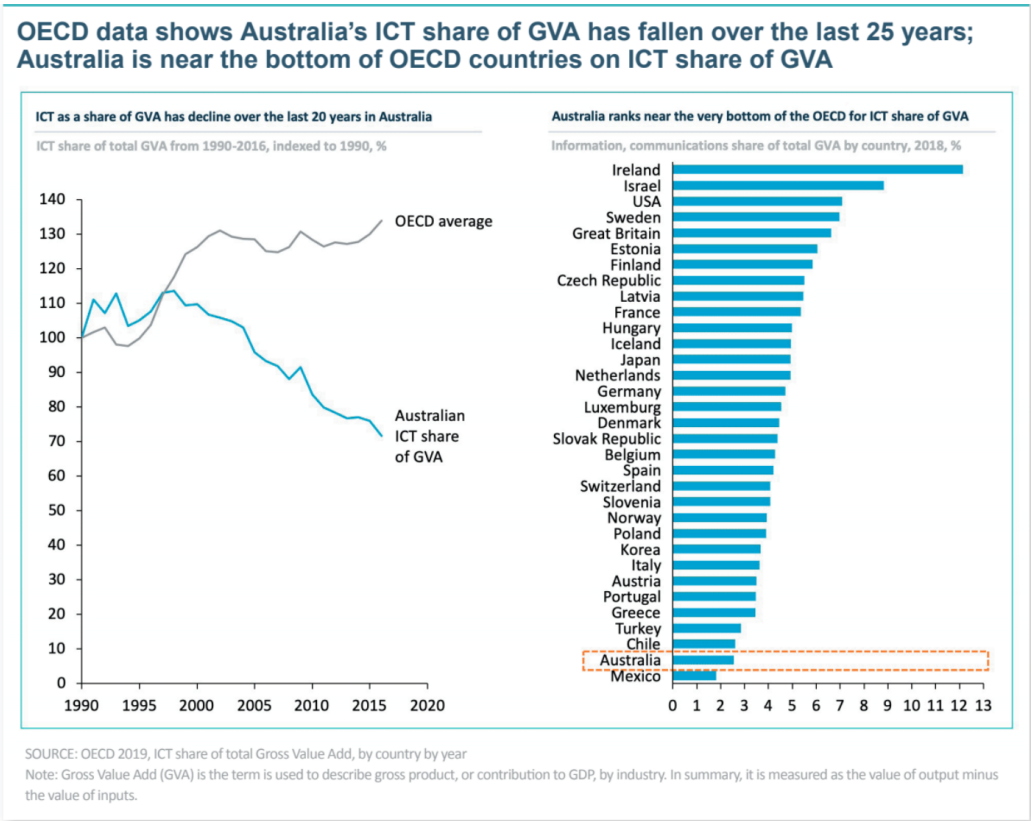
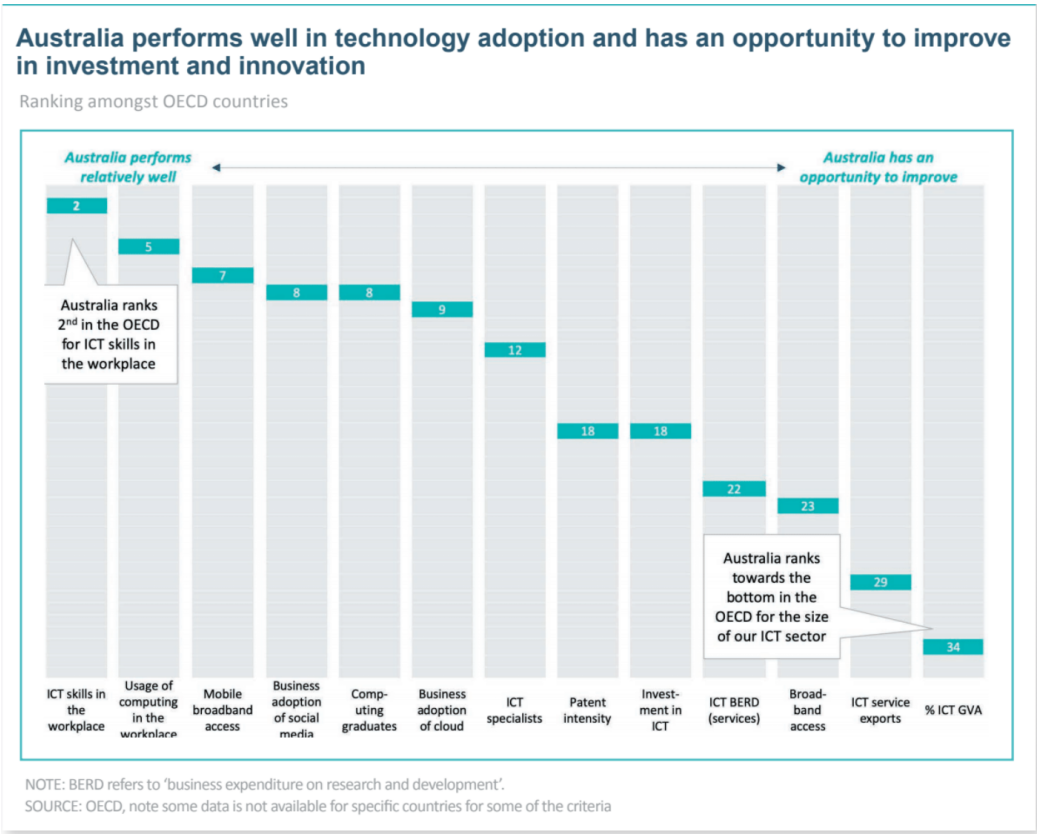


Figure 2

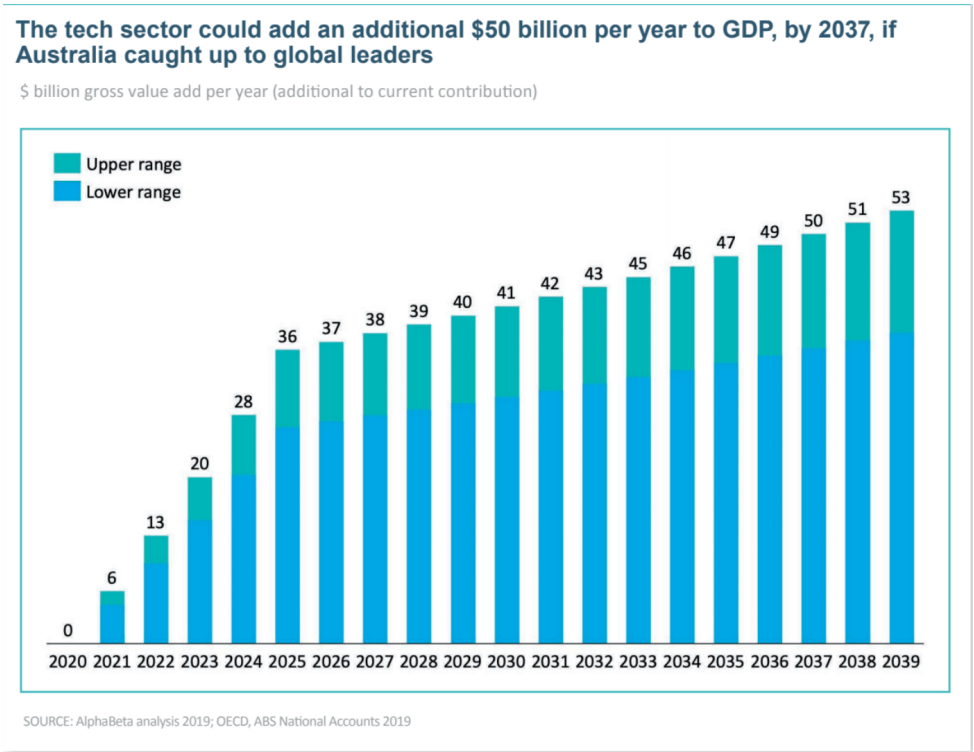


Yet, if we turn this around, the economic opportunity is immense: Per Figure 3, if Australia caught up with the growth rate of other leading countries internationally, our technology sector could be contributing $207 billion per year to GDP by 2030.

AlphaBeta's analysis of countries with successful tech sectors found their policies incentivise innovation, and have pragmatic industry regulation. It also concluded that Australia lacks a cohesive, all-of-Government strategy to grow the technology sector, and that current approaches to the sector are fragmented.

In the absence of such a strategy, proposals such as the ACCC Digital Platforms Inquiry, with its important goal of protecting the future of journalism, may appear as reasonable solutions to the problems the ACCC identifies. However, these recommendations have unintended consequences for a wide range of digital service providers, organisations that rely upon digital services to market goods and services, consumers of online services, and for the Australian economy. These unintended consequences must be robustly examined and mitigated in any policy reform proposed in response.

Figure 3[2]



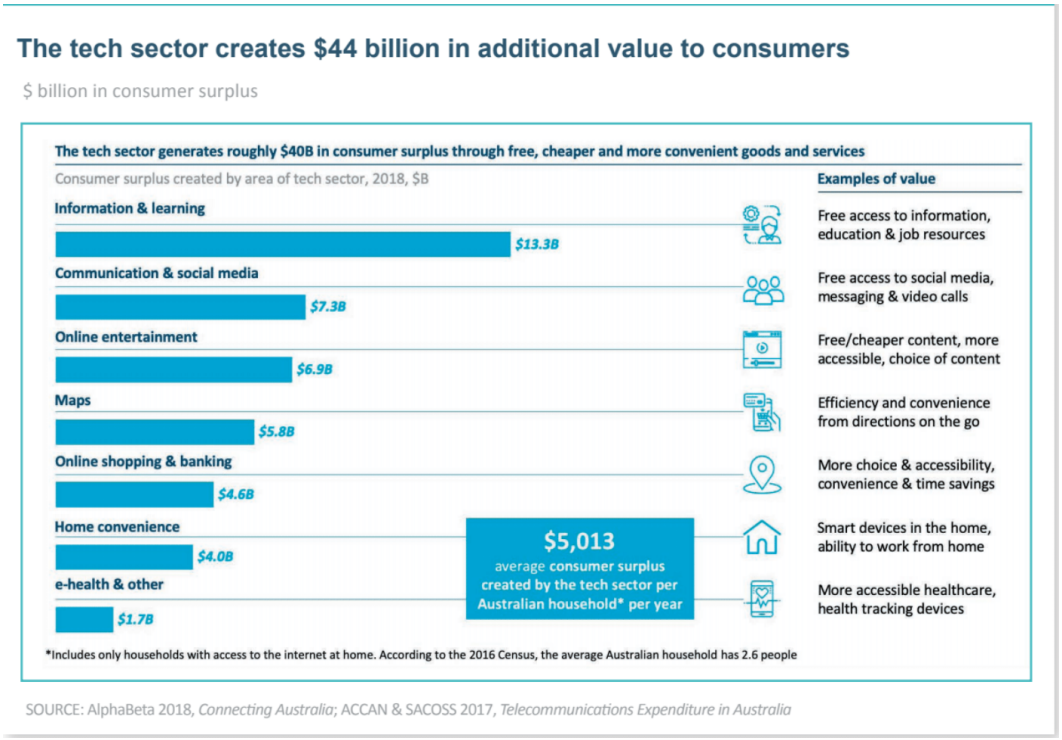
Consumer value of digital products and services

The ACCC DPI final report does not include substantive analysis, nor much more than a passing acknowledgement, of the value of digital products and services to Australian consumers.

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 4, 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. The report identifies that digital technologies unlock new consumer benefits:

"Platforms like Redbubble are allowing customers to access a wider variety of goods and services by linking independent local artists with a global marketplace. Point of sale technologies like Square enable customers to use more convenient, cashless payment methods in previously cash-only situations like markets and festivals. Video streaming and online education platforms are improving consumers' access to new knowledge, skills and qualifications. In addition, tools like mobile banking, digital government services and telehealth have made it more convenient for consumers to access these services, saving them time and improving productivity.[3]"

Figure 4



By contrast, the ACCC DPI final report over-indexes on the potential consumer harm of digital services. For example, the ACCC states:

"A lack of privacy and control over data-sharing can give a data holder economic leverage over the data subject (for example, by allowing a seller to use their knowledge of consumers to target vulnerable consumers or discriminate against customers on the basis of gender, race or sexual orientation)."[4]

Yet the only evidence that the report provides of such harmful consumer practices occurring is in the following example, where the company in question is not a digital platform:

"For example, insurance provider MLC had requested access to the medical records of a consumer indicating that she had accessed mental health services for sexual abuse she suffered as a child in the 1980s, which led to MLC excluding her from mental health coverage in her life insurance."[5]

There is no question that user data can be misused in a number of ways to negatively impact consumers, and that there must be strong consumer protections and concerted and sustained action by industry to prevent such misuse. However, as the example above from the insurance industry illustrates, such practices are not limited to digital platforms in a data-driven economy. That said, there are indeed unique issues relevant to digital products that necessitate targeted responses in areas such as data privacy, online safety and media literacy, and responsible digital services acknowledge and invest in these areas. However, the ACCC DPI final report's conclusions are generally predicated on the *potential* for consumer harm, rather than presenting substantive evidence of it. The result is many recommendations that are arguably premature and lack an evidence base. We therefore urge the Australian Government to fully consider these unintended consequences and undertake

[4] ACCC (July 2019), *Digital platforms Inquiry Final Report*, p.435
[5] ACCC (July 2019), *Digital platforms Inquiry Final Report*, p.435

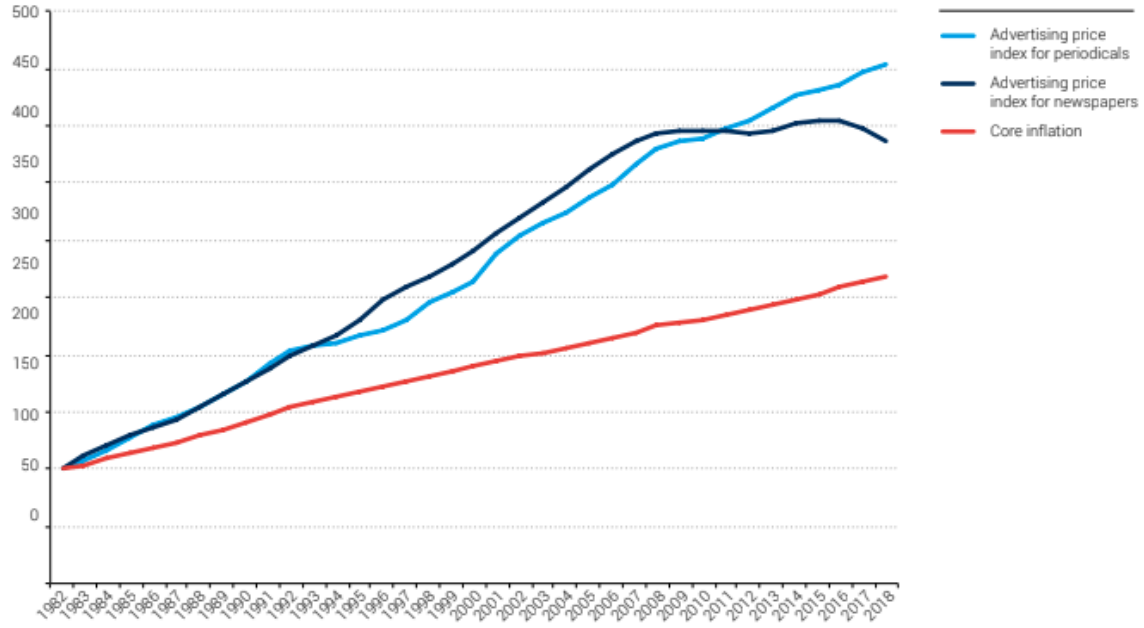
necessary broader consultation with the digital industry, as well as other affected industries and stakeholders, before any major reform is announced.

Broader trends in advertising

Michael Mandel of the Progressive Policy Institute recently released research in July 2019, analysing the price of digital and traditional media advertising, in the United States, Australia and a range of countries. This research finds:

- There has been a sustained fall in all advertising spending as a share of GDP, across the United States, Australia, and other countries.
- There has been an increase in the price of print advertising, in the United States. It found that the price of print advertising in the US steadily increased and outpaced the rate of inflation for 20 years across the 80s and 90s. See Figure 5.
- There has been a decrease in the price of Internet advertising in the United States. Since 2010, the price of Internet advertising has dropped by more than 40%, while the price of advertising with traditional media has not declined in that same period. See Figure 6.
- Since 2016, the price of Internet advertising sold by print newspapers has dropped much less than the price of Internet advertising sold by digital platforms and non-print publishers.[6].

Figure 5[7]

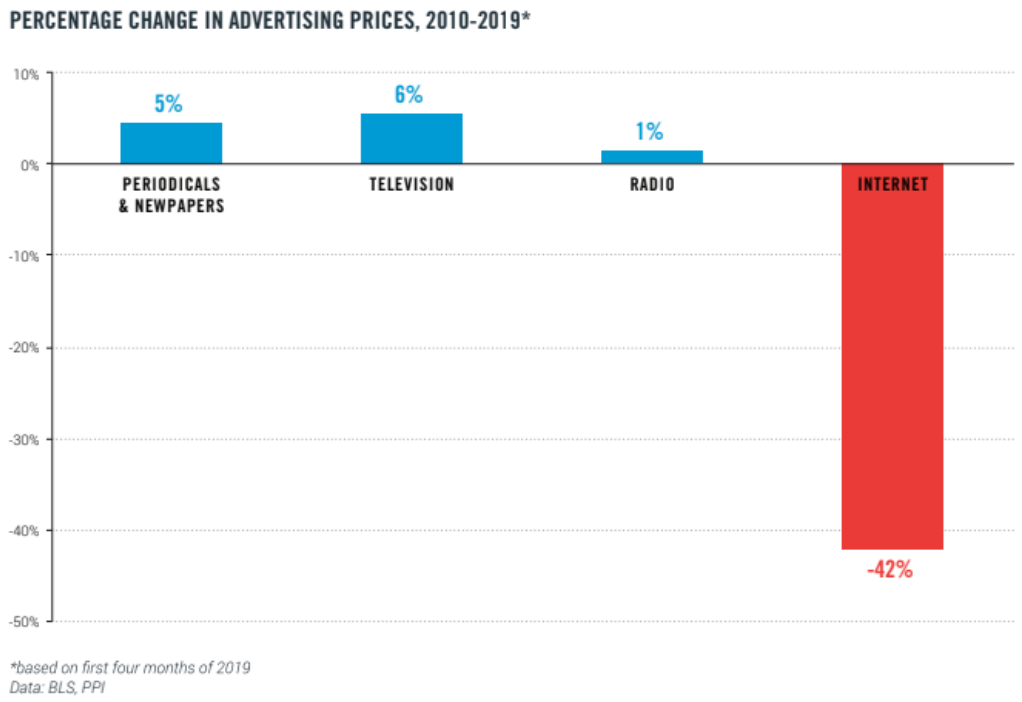


Data: Bureau of Labor Statistics, PPI

[6] Mandel, Michael, (July 2019), "The Declining Price of Advertising: Policy Implications", accessed at: https://www.progressivepolicy.org/issues/government-reform/the-declining-price-of-advertising-policy-implications-2/

[7] Mandel, Michael, (July 2019), *The Declining Price of Advertising: Policy Implications*, accessed at https://www.progressivepolicy.org/wp-content/uploads/2019/07/Advertising2019_Mandel.pdfp. 10

Figure 6[8]



Further analysis of how the forces that the Progressive Policy Institute has examined in the US might apply in Australia would provide useful insights. Mandel's conclusion from this analysis is that "advertisers are finding that they can get a bigger bang for their buck by spending their money online rather than in print," a sentiment that is also acknowledged in the ACCC's DPI report:

"In particular, digital platforms have provided a new advertising avenue for small to medium sized businesses that may not have been able to afford the advertising available on the high-reach traditional newspapers or commercial television and radio network."[9]

The ACCC acknowledges that a wide range of websites provide online ad inventory, including traditional news media businesses and other digital platforms and marketplaces. However, it does not acknowledge that some popular online services providing classified ads are owned by traditional media businesses, whereby the potential revenue could be reallocated to journalism if the company so chose. Similarly, it does not acknowledge that there are new entrants to the digital advertising market, such as supermarket chains[10].

[8] Mandel, Michael, (July 2019), "The Declining Price of Advertising: Policy Implications", p. 10
[9] ACCC (July 2019), *Digital platforms Inquiry Final Report*, p.
[10] Pash, Chris in *AdNews* (July 2019), "Why Woolworths wants to be a media business and run its own advertising arm", accessed at https://www.adnews.com.au/news/why-woolworths-wants-to-be-a-media-business-and-run-its-own-advertising-arm#sx4flApzJBQBDdRm.99

Substantive response to specific recommendations

In this section, we outline the specific recommendations that are of particular concern to DIGI in its advocacy for the digital industry at large.

Recommendation 1: Changes to merger law

Section 50(3) of the Competition and Consumer Act 2010 (CCA) be amended to incorporate the following additional merger factors:
(j) the likelihood that the acquisition would result in the removal from the market of a potential competitor;
(k) the nature and significance of assets, including data and technology, being acquired directly or through the body corporate.

It is disappointing to see this recommendation was retained in the final report, with a slight expansion of scope, without addressing the concerns raised by many in the technology industry. It is also concerning that the evidence base that the ACCC DPI final report provides for this recommendation is a chapter that does not consider the technology industry at large, nor analysis of the implications previously raised about this recommendation.

Mergers and acquisitions in the technology sector are a crucial driver of innovation and investment, as they offer an incentive for entrepreneurs who start companies, for whom selling their company is commonly the end goal. Ensuring that startups can successfully exit their venture, through acquisition from large technology companies, is key to ensuring growth and development of Australia's technology sector. Exit fees can create a virtuous cycle, where founders use that capital to create another successful company. For example, the founders and early employees of PayPal have gone on to establish a number of other successful companies such as LinkedIn, Tesla, Yammer and Yelp and are major investors in many more companies[11]. The economic impact of enabling such activity is significant, and the result for consumers of such activity can be new products being brought to market, affording Australians with more consumer choice, in a market where technology adoption is high[12].

Acquisitions of Australian companies in particular could see major sectoral growth, and resulting consumer benefit. Furthermore, such proposed regulations serve as a deterrent to global companies from investing or expanding operations in the Australian market. A thriving technology sector in Australia means creating a supportive environment for large and small companies, local and global companies, and therefore an ecosystem where the calibre of employees improves, and the networking, mentorship and business opportunities increase.

Furthermore, given the rapid pace of technological innovation and iteration within technology companies, we would question the criteria on which the ACCC will be able to effectively assess the removal of a "potential future competitor". This criteria is overly broad and subject to varying interpretation. Additionally, this sort of prediction of market factors is difficult enough for those in the industry to predict, let alone for regulators.

The Australian Government must look at this recommendation in the context of the global standing of Australia's technology industry, as outlined in the introduction, as it may disincentivise startups and other technology companies from expanding in the Australian market. As noted, Australia ranks second last in the OECD -- only to Mexico -- for the relative size of our technology sector. Given the

[11] Gelles, David (April 2015), "The PayPal Mafia's Golden Touch", *New York Times*, accessed at: https://www.nytimes.com/2015/04/02/business/dealbook/the-paypal-mafias-golden-touch.html
[12] See Figure 2, from AlphaBeta (September 2019), Australia's Digital Opportunity, pp. 20-21.

downward trajectory of ICT share of GVA for the last 20 years[13], and the need and immense potential to grow this industry, it is not an opportune time for innovation-stifling red tape to be legislated in the form of this recommendation.

Recommendation 7: Designated digital platforms to provide codes of conduct governing relationships between digital platforms and media businesses to the ACMA

Designated digital platforms to each implement a code of conduct to govern their relationships with news media businesses. Each platform's code of conduct should ensure that they treat news media businesses fairly, reasonably and transparently in their dealings with them, and contain at least the following commitments:

- *the sharing of data with news media businesses*
- *the early notification of changes to the ranking or display of news content*
- *that the digital platform's actions will not impede news media businesses' opportunities to monetise their content appropriately on the digital platform's sites or apps, or on the media businesses' own sites or apps*
- *where the digital platform obtains value, directly or indirectly, from content produced by news media businesses, that the digital platform will fairly negotiate with news media businesses as to how that revenue should be shared, or how the news media businesses should be compensated.*

The ACMA will publish guidelines regarding how the code should be developed and what should be included in the code. In performing its role under this recommendation, the ACMA shall closely consult with the ACCC.

The ACMA will also designate the digital platforms that will be required to implement a code; review and approve the content of the codes (after consulting news media businesses). The ACMA will enforce the codes and have appropriate investigative and information gathering powers and the capacity to impose sufficiently large sanctions for breaches to act as an effective deterrent. The ACMA will also have the ability to require digital platforms to amend their codes in specific ways, if it considers that the objectives of the code are not being achieved.

Digital platforms will have nine months to develop a code, and will be required to demonstrate that they have consulted fully with news media businesses in drafting their code, and carefully assessed the issues raised by them. The duration of the code will be proposed by the digital platform and subject to approval by the ACMA.

If a digital platform is unable to submit an acceptable code to the ACMA within nine months of designation, the ACMA should create a mandatory standard to apply to the designated digital platform.

While it is unclear in the ACCC DPI final report exactly the types of companies that will be considered "designated digital platforms" and will have to provide such a code to the ACMA, this recommendation raises important questions of precedent. The government must consult widely on the competition issues such codes would be intended to address and which platforms should have to provide a code.

Additionally, this recommendation raises scope and scalability questions in relation to what may be defined as news media businesses, because of the many types of businesses may fall under this

[13] See Figure 1, from AlphaBeta (September 2019), *Australia's Digital Opportunity*, pp. 20-21.

banner, including: i) mainstream major Australian news media businesses ii) publications targeted to a specific industry or demographic iii) regional and local papers iv) news content produced outside of Australia. It is unclear whether a designated digital platform would be required to provide a code in relation to all such categories, and whether any variance would be permitted depending on the category.

Nonetheless, we fully appreciate the intent behind this area for further analysis and the need to protect journalism. Several DIGI members are advancing partnerships and other initiatives with similar objectives to enhance the distribution and monetisation of quality journalism, improve media literacy, and prevent the proliferation of fake news. DIGI is also supportive of the ACCC's recommendations 9,10,11,12 and 13 that advance more targeted initiatives to promote and protect journalism.

However, DIGI cautions against market-wide interventions that will have unintended consequences for the digital industry. We urge the Government to further examine broader shifts in the economy and in consumer behaviour that are causing some of the challenges that this recommendation is designed to solve, such as the relative price and accessibility of advertising on digital platforms and news media businesses as outlined earlier. Taking into consideration these broader contextual factors, placing restrictions on the commercial arrangements of a designated set of digital platforms to submit specialised codes of conduct governing their various B2B relationships may place digital native companies at a commercial disadvantage in a rapidly shifting digital advertising market.

Recommendation 8: Mandatory ACMA take-down code to assist copyright enforcement on digital platforms

A mandatory industry code be implemented to govern the take-down processes of digital platforms operating in Australia. The code will enable rights holders to ensure the effective and timely removal of copyright-protected content from digital platforms.

The mandatory code should be enforced by the ACMA and have appropriate sanctions and penalty provisions. The content of the code should be developed by the ACMA in consultation with industry including rights holders and digital platforms, and include a framework for cooperation between rights holders and digital platforms which provides guidance regarding key issues of concern for stakeholders including:

- *Cooperation framework: a framework for cooperation between rightsholders and digital platforms to proactively identify and prevent the distribution of copyright-infringing content online, including an appropriate division of the responsibility for monitoring online content for copyright-infringement.*
- *Communication: measures to improve the ease of communications between rightsholders and digital platforms, including requirements for designated agents of digital platforms to be available during Australian business hours as well as appropriate periods where key Australian live events are broadcasted.*
- *Timeframes: reasonable timeframes for the removal of infringing content and processes targeted at the timely removal of particularly time-sensitive content such as live commercial broadcasts.*
- *Bulk notifications: mechanisms for rightsholders to make bulk notifications to address repeated infringements of the same content and to sanction users who commit multiple or regular infringements.*
- *Proof of copyright: measures to streamline the process by which rightsholders may prove copyright ownership, particularly in cases where there is joint-authorship.*

DIGI members dedicate significant resources to processing copyright removal requests. The proposed "mandatory industry code" would represent a significant departure from the globally accepted legal standards and norms for issuing take-down notices that are relied upon by online

service providers and content creators around the world. The globally accepted standard requires online service providers to respond “expeditiously” to disable access to the material that is claimed to be infringing upon notification. The “expeditious” standard is already enshrined in law in numerous other jurisdictions, and the flexibility of this standard recognises the complexity in balancing claimant and content creators’ interests in evaluating a request for removal. It is well understood that copyright cannot be enforced without the participation of the rightsholder, and cannot be self-executing as determining ownership is not always straightforward. In its submission to the ACCC’s preliminary DPI report, Redbubble outlines four complications that arise in their routine assessment of copyright claims:

- *The uploaded work may be legitimate fair dealing with the original work e.g. parody or satire and the boundaries of fair dealing are often difficult to delineate;*
- *Whilst one person may be familiar with certain referential images that reflect television show characters or brands they are aware of, another may not recognise these brands on first pass;*
- *Some users may actually own licenses to the content they are posting and be able to do so legally, even if it is referential to pop culture; and*
- *Some content owners actually want their fans to upload their content because it keeps older brands alive, so they will often instruct Redbubble to maintain images on the website even though that they may believe the images infringe their rights*[14]*.*

The requirement for platforms to “proactively identify and prevent the distribution of copyright-infringing content online” is problematic for a number of reasons. First of all, it relies on detection technologies with ample room for error, particularly when deployed in real time. Furthermore, there are few commercially available solutions and, where they exist, they function for some content types but not others. Secondly, the development of product-customized technology can be cost-prohibitive industry-wide. Larger platforms have invested in sophisticated automated technology to enable fast services while working to prevent the upload of copyright infringing content, yet such developing such bespoke software is expensive; for example, Youtube has spent approximately $USD100 million on its Content ID upload filters and other technology to prevent copyright infringements[15] and Facebook has developed a sophisticated rights manager to support rightsholders[16]. Smaller digital platforms that do not have the resources to develop such technology would then be placed at a relative disadvantage -- in this way, the ACCC’s broader intention of encouraging competition could serve to do the opposite by creating a standard that only the largest digital platforms can attempt to maintain. Finally, encouraging platforms to apply solutions at the point of upload can be out of step with consumer expectation of instantaneous digital services and can impact the user experience.

The requirements for “designated agents of digital platforms to be available during Australian business hours as well as appropriate periods where key Australian live events are broadcasted” will be challenging for global digital platforms, particularly those of a smaller size. Smaller platforms may operate their Trust & Safety Teams that manage copyright and other content complaints at a global level, supported by staff in Australia who provide local context in guiding complicated decisions, in addition to other responsibilities. It would not be feasible for overseas teams to consistently “be available during Australian business hours”. Nor is it feasible for small local teams or overseas teams to always be aware and consistently available during “appropriate periods where key Australian live events are broadcasted”. Furthermore, this requirement does not take into account companies that offer digital services available in the Australian market, but do not have a local office.

DIGI believes that any recommendations relating to Australia's take-down system should take into account the existing notice and take down regime contained within the Copyright Act and previous inquiries into the area of online copyright infringement. Australia's existing take-down system has been the subject of extensive consideration and review, most recently by the Australian Productivity Commission, which recommended "[t]he Australian Government should expand the safe harbour scheme to cover not just carriage service providers, but all providers of online services." DIGI supports extending the Copyright Act's Safe Harbour Scheme to to online service providers. An extended Safe Harbour Scheme would i) give rightsholders an efficient way to seek removal of infringing content ii) reward online service providers for collaborating with rightsholders by granting legal protection under the Scheme and iii) include protections for consumers who wish to challenge incorrect claims of copyright infringement.

Apart from isolated anecdotes, the ACCC has not provided substantive evidence of a problem that requires such a drastic solution. Individuals and organisations use digital service providers to express themselves and to share content. Mandatory codes with high sanctions for errors will result in a take-down regime that encourages platforms to remove first and ask questions later, making it too risky for platforms to attempt to protect the legitimate speech interests of ordinary Australians, at the expense of Australians' public dialogue and free expression.

Recommendation 15: Digital Platforms Code to counter disinformation

Digital platforms with more than one million monthly active users in Australia should implement an industry code of conduct to govern the handling of complaints about disinformation (inaccurate information created and spread with the intent to cause harm) in relation to news and journalism, or content presented as news and journalism, on their services. Application of the code should be restricted to complaints about disinformation that meet a 'serious public detriment' threshold as defined in the code. The code should also outline actions that constitute suitable responses to complaints, up to and including the take-down of particularly harmful material.
The code should be registered with and enforced by an independent regulator, such as the ACMA, that:

- *is given information-gathering powers enabling it to investigate and respond to systemic contraventions of code requirements*
- *is able to impose sufficiently large sanctions to act as an effective deterrent against code breaches*
- *provides frequent public reports on the nature, volume and handling of complaints received by digital platforms about disinformation*
- *reports annually to Government on the efficacy of the code and compliance by digital platforms.*

While the code should focus on addressing complaints about disinformation it should also consider appropriate responses to malinformation (information inappropriately spread by bad-faith actors with the intent to cause harm, particularly to democratic processes).
In the event that an acceptable code is not submitted to the regulator within nine months of an announced Government decision on this issue, the regulator should introduce a mandatory industry standard.
The code should be reviewed by the regulator after two years of operation, and the regulator should make recommendations as to whether it should be amended, replaced with an industry standard, or replaced or supplemented with more significant regulation to counter disinformation on digital platforms.

Addressing the harm that comes from disinformation, as well as the media literacy required to curb its spread, are incredibly important objectives where industry, government and civil society each have a role to play. Relevant digital platforms are increasingly investing in policies, procedures and product features that aim to prevent the spread of disinformation, while also balancing the complex interplay of this issue with the freedom of expression of their users. To the extent that the code is intended to deal with sophisticated disinformation campaigns (for example, those that may be state-sponsored or by

multinational criminal groups), many major digital platforms already work closely with Australian security agencies on information operations.

In general, this is an area where digital platforms will tend to make content decisions in line with i) their users' expectations ii) their operational and financial resourcing iii) their particular service offering of the platform. That is to say, an appropriate intervention for disinformation for a post on a public platform (such as content signalling or removal) may be considered as intrusive and inappropriate on a private messaging platform. An appropriate intervention on one platform (such as partnerships with third-party fact-checkers) may be cost-prohibitive and unscalable for another. Therefore, the idea of a one-size-fits-all industry code of conduct is problematic in relation to disinformation, as it does not take into account variables that impact content moderation in this area.

The ACCC states that "it should avoid the Government directly determining the trustworthiness, quality and value of news and journalism sources"[17]. But in this recommendation, the ACCC is effectively putting that burden on platforms. The ACCC indicates that the code would enable members of the public who are unsatisfied with digital platforms' handling of their complaints about disinformation or malinformation could refer these to the regulator. This effectively makes the ACMA a truth verification body, as its judgements as to whether a digital platform adequately handled the complaints speak to the regulator's own assessment of truth in relation to the matter in question.

While the ACCC attempts to set a high threshold for what might be covered under the code, in effect, it lowers that threshold by stating that "information incorrectly alleging that a public individual is involved with illegal activity"[18] would be covered. This is particularly problematic when people take to digital platforms, such as Twitter, for whistleblowing to raise awareness of injustices that have not yet been presented in court, as was seen with the #metoo movement.

It is worth emphasising that this recommendation covers a range of digital products and services in its application to services with over a million monthly active users (MAU). Such services will see vast amounts of user-generated content uploaded in real-time to their services each day. Per the introduction to this submission, Australia has a relatively small technology sector and few global digital native firms. We should be providing and incentives and encouragement for firms to grow their userbase to over a million MAU, not overly-burdening companies at this important growth milestone.

Recommendation 16: Strengthen protections in the Privacy Act

16(a) Update 'personal information' definition: Update the definition of 'personal information' in the Privacy Act to clarify that it captures technical data such as IP addresses, device identifiers, location data, and any other online identifiers that may be used to identify an individual.

16(b) Strengthen notification requirements: Require all collection of personal information to be accompanied by a notice from the APP entity collecting the personal information (whether directly from the consumer or indirectly as a third party), unless the consumer already has this information or there is an overriding legal or public interest reason.

The notice must be concise, transparent, intelligible and easily accessible, written in clear and plain language, provided free of charge, and must clearly set out how the APP entity will collect, use and disclose the consumer's personal information. Where the personal information of children is collected, the notice should be written at a level that can be readily understood by the minimum age of the permitted digital platform user.

To provide consumers with a readily understood and meaningful overview of an APP entity's data practices and as a means of reducing their information burden, it may also be appropriate for these

[17] ACCC (July 2019), *Digital platforms Inquiry Final Report*, p.370.
[18] ACCC (July 2019), *Digital platforms Inquiry Final Report*, p.370.

requirements to be implemented along with measures such as the use of multi-layered notifications or the use of standardised icons or phrases.

16(c) Strengthen consent requirements and pro-consumer defaults: Require consent to be obtained whenever a consumer's personal information is collected, used or disclosed by an APP entity, unless the personal information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.

Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). This means that any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled. Where the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian.

It may also be appropriate for the consent requirements to be implemented along with measures to minimise consent fatigue, such as not requiring consent when personal information is processed in accordance with a contract to which the consumer is a party, or using standardised icons or phrases to refer to certain categories of consents to facilitate consumers' comprehension and decision-making.

16(d) Enable the erasure of personal information: Require APP entities to erase the personal information of a consumer without undue delay on receiving a request for erasure from the consumer, unless the retention of information is necessary for the performance of a contract to which the consumer is a party, is required under law, or is otherwise necessary for an overriding public interest reason.

16(e) Introduce direct rights of action for individuals: Give individuals a direct right to bring actions and class actions against APP entities in court to seek compensation for an interference with their privacy under the Privacy Act.

16(f) Higher penalties for breach of the Privacy Act: Increase the penalties for an interference with privacy under the Privacy Act to mirror the increased penalties for breaches of the Australian Consumer Law.

DIGI acknowledges that potential changes to the Privacy Act are an important area of exploration. We welcome the fact that the ACCC recognises that the potential detriments it identifies "affect not only consumers of digital platform services, but may extend to the myriad of industries across the Australian economy that collect, use or disclose the user data of Australians[19]. It is also worth noting that many industries collect and utilise considerable volumes of personal information and do not have the same level of transparency as the digital sector, noting that the Deloitte Privacy Index 2018 has observed that digital companies provide greater transparency for their users than non-digital companies[20].

In this section, we outline a response to some of the specific elements of Recommendation 16. At a high level, it appears that this recommendation is recommending reform that exceeds the standards of the EU's General Data Protection Regulation (GDPR), which was introduced on May 25, 2018. In its consideration of such a model, we encourage the Government to fully assess the impact of the GDPR to date as to whether the regulations are operating as intended and are not unduly impacting innovation and competition in the technology sector.

[19] ACCC (July 2019), Digital platforms Inquiry Final Report, p.449.
[20] Deloitte, *Deloitte Australian Privacy Index 2018*, May 2018, at https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html

Additionally, we urge the Australian Government to engage in robust, proactive consultation with all affected industries to inform any proposed reform in response to Recommendation 16. It is reasonable to assume that not all affected industries are paying due attention to the wide scope of the ACCC's DPI recommendations, nor engaging in the Treasury consultation period. Consumers will have the same expectations of privacy, regardless of the specific company they interact with or the sector within which that company sits.

16d

DIGI is supportive of measures that give people more meaningful control over their information in a digital world, such as the recommendation under 16d in relation to data erasure requests. DIGI members allow their users to delete, access and correct their personal information in accordance with the Australian Privacy Act 1988 and where relevant they apply the GDPR's requirements in this area.

16b

DIGI is also broadly supportive of 16b, noting that its members all provide comprehensive notices that outline data use. We are supportive of attempts to improve transparency and clarity in notices to users. However, such attempts must be mindful of the nuances of providing effective notice. While we agree that notices should be transparent and straightforward for users to comprehend, these are legal documents that outline the rights and responsibilities around data use between Internet users and businesses related to the particular service offering. As a result, there can be a level of complexity in such a contractual agreement that must also hold up in a court of law if required. The prescribed solutions may in fact ultimately undermine transparency. For example, standardised iconography in a multi-layered format, as suggested by the ACCC, may actually serve to mislead consumers if the complexity of the data processing differs across different APP entities. This may provide some legal risk to companies in their efforts to simplify, particularly with the obligation for the notice to be "readily understood by the minimum age of the permitted digital platform user."

16a & 16c

Legal bases for information collection

DIGI has concerns about the economy-wide implications of recommendations 16a and 16c. Taken together, these recommendations would see Australia implement privacy reform that is stricter than the standards of the recently-enacted GDPR in the EU.

Under 16a, the ACCC considers IP addresses and device identifiers as personal information. What it does not take into account, despite DIGI raising this in its preliminary report submission and in stakeholder consultations, is that IP addresses and device identifiers are collected by websites for the basic and essential functions such as providing an online service in the user's language, based on their location, and to fit the user's chosen web browser. Arguably, almost every website requires the collection of this essential information in order to meet basic consumer expectations in relation to the services they access, and the services cannot be provided without such processing.

The combined effect of 16a and 16c is that a digital provider must obtain user consent before an IP address or device identifier is collected, resulting in a consumer being blocked with a consent screen before a page can even load. We believe that IP addresses should not be deemed to be personal information where they are not actually used to identify an individual. For example, if an IP address is used to assess the location of access so that the right local version of a web page can be loaded into a particular browser then it should not be treated as personal information in that context as it's not being used to identify any individual consumer. Furthermore, consumers expect web pages to load quickly -- they do not want to be unnecessarily blocked from obtaining the information or service they seek. While the ACCC acknowledges the potential for consent fatigue, it has not meaningfully considered the impact of its recommendations in slowing or de-personalising digital services for Australian consumers.

In this regard, the ACCC is limiting the legal bases for valid data processing. The GDPR, on the other hand, provides data controllers with six lawful bases with which they can justify their collection of information of users, summarised as consent, performance of a contract, vital interest, legal obligation, public task and legitimate interest[21]. By contrast, the ACCC recommends four legal bases, summarised as consent, legal obligation, contractual necessity or overriding public interest.

The ACCC specifically rejects legitimate interests:

> *"The ACCC notes, however, that there is considerable uncertainty and concern surrounding the relatively broad and flexible definition of the 'legitimate interests' basis for processing personal information under the GDPR.[22]"*

The ACCC's rejection of legitimate interests is wholly unfounded and premature. First, as noted, the GDPR was introduced on May 25, 2018, just over a year before the release of the ACCC's final report. At time of writing, there have been few comprehensive evaluations of the impact of GDPR on consumers and the EU economy. One of the few such evaluations was produced by the The Centre for Information Policy Leadership which, while it identifies the law's advantages, cautions against overemphasis on user consent in modern privacy laws, noting that this is "unrealistic in our data driven society and economy and not in line with the GDPR either."

Secondly, in its short analysis of "legitimate interests", the ACCC does not mention the three-part balancing test that data controllers must apply under GDPR to justify using this as a legal basis for data process. As the UK Information Commissioner's Office explains, this test includes:

> *Purpose test – is there a legitimate interest behind the processing?*
> *Necessity test – is the processing necessary for that purpose?*
> *Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms?*
>
> *...This means it is not sufficient for you to simply decide that it's in your legitimate interests and start processing the data. You must be able to satisfy all three parts of the test prior to commencing your processing[23].*

The large fines associated with GDPR disincentivise companies from not applying this balancing test, which provides a pragmatic alternative to burdening users with consent in almost every instance of personal information collection.

We therefore encourage the Government to explore an expanded set of legal bases than is offered in the ACCC DPI final report in any potential reform of Australia's Privacy Act.

Over-reliance on unbundled consent as a legal basis

DIGI fully supports the need for consumers to be informed about the use of their data, and the need for comprehensive measures to inform and enable users to both better understand and manage their data use. Yet DIGI has concerns with the guidance provided under 16c that:

> *"Valid consent should require a clear affirmative act that is freely given, specific, unambiguous and informed (including about the consequences of providing or withholding consent). This means that any settings for data practices relying on consent must be pre-selected to 'off' and that different purposes of data collection, use or disclosure must not be bundled."[24]*

---

[21] GDPR, Article 6, accessed at: https://gdpr-info.eu/art-6-gdpr/
[22] ACCC (July 2019), Digital platforms Inquiry Final Report, p. 466
[23] ICO, "What is the 'legitimate interests' basis?", accessed at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/
[24] ACCC (July 2019), Digital platforms Inquiry Final Report, p. 456

The requirements around disclosure not being bundled will effectively see consumers have to check a box for each distinct act of data processing, providing a huge burden on the average consumer. Ultimately, digital services primarily collect data to provide better services for consumers, with the understanding that better services will support business growth. For example, the crowdfunding website GoFundme collects IP addresses in order to show a user relevant campaigns in their city. They also collect a user's email address to verify an account and send transactional and email updates on campaigns. They may also temporarily collect credit card information in order to process donations or contributions, which is fundamental to charitable giving on GoFundMe where over 2 million Australians have donated over $200 million to charitable causes since 2016. These are important features for people trying to raise money or awareness for social causes in their community; in effect, such disclosures may hinder the ability of charities and individuals to fundraise online.

Effectively, the recommendations here would require each of these acts of data processing to be accompanied by a distinct consent request that would preclude the processing before the box was checked. Seeking consent for every such act of data processing that businesses undertake has been rejected in other jurisdictions, such as the EU and California, as completely impractical.

Targeted advertising

There is also an implication in recommendation 16c that any digital product or service's use of targeted advertising must be pre-selected to off. We support empowering consumers to make choices about their privacy settings. DIGI members understand the need for consumers to be informed about the use of their data in general and for the purpose of targeted advertising, and have comprehensive resources in place to inform and enable users to both better understand and manage their data use.

However, it is important to fully explore the benefits of targeted advertising to consumers. Consumers receive value and utility from targeted advertising as it enables a personalised experience and the discoverability of relevant goods and services often from SMEs. An estimated 8.2 million Australians have purchased from, or visited, an SME after seeing content relevant to the business on Facebook alone.[25] The ACCC's recommendation on the default disabling of targeted advertising works from a false assumption that targeted advertising is not valuable to consumers and businesses alike -- an assumption that we urge the Government to rigorously analyse and challenge.

Targeted advertising brings benefits to advertisers, many of whom are Australian small businesses who are now able to afford to advertise due to cost reductions driven by the entry of digital platforms into the market. Businesses across Australia use the Internet to connect with their customers and reach out to new customers. AlphaBeta has found that Australian SMEs attribute around $90 billion of income to the Internet, and 1 in 3 SMEs receive orders via online platforms[26].

A default pre-selection of targeted advertising to off will have an impact on the whole economy, for every company or other organisation -- large and small -- that advertises goods, services or public interest causes on the Internet. It will also have an impact on digital platforms that are supported by advertising -- the same business model used by many traditional media organisations. Advertising powers free digital services and the wide range of freely available content available to consumers.

The significant potential economic impact of this recommendation raises questions about whether such a recommendation is too wide in relation to the narrow terms of reference of the ACCC's inquiry. It may be the case that consumers object to targeted advertising when asked in the abstract -- in the same way that they might also express a preference for television without commercials, or newspapers without advertorials -- but we encourage the Government to further examine the evidence base in the ACCC's case for this preliminary recommendation, and conduct further analysis on the benefits that targeted advertising provides Australian consumers and businesses alike.

---

[25] Facebook, *Connecting Benefits*, August 2018, p. i, at https://www.connectingbenefits.com.au/download/Connecting_Benefits.pdf
[26] AlphaBeta, *Google Economic Impact, Australia 2015*, p. 25, at http://www.alphabeta.com/wp-content/uploads/2016/08/Google-ecomonic-impact-2015.pdf

Information collection of children

In relation to the requirement under 16c that "where the personal information of children is collected, consents to collect the personal information of children must be obtained from the child's guardian", it is worth noting that many digital products and services do not collect age-based data in order to minimise their data collection to what is absolutely necessary for the provision of the service. Where relevant to their services, such as if they are informed of a user's age through account registration or otherwise, DIGI members abide by applicable law relating to the prohibition of information collection on minors. The principle of data minimisation seems in line with the spirit of the ACCC's privacy recommendations, but may preclude platforms from knowing when their services are being used by minors.

--

The Australian Government must rigorously analyse all unintended consequences of Recommendation 16. Noting the research provided earlier i) in relation to the relative global standing of Australia's technology sector ii) its immense potential to transform the Australian economy with the right policy frameworks and iii) the significant consumer value that the industry provides, DIGI posits that Australia simply cannot afford this "GDPR plus" style privacy regulation. The ACCC "considers that strengthened privacy safeguards have the potential to encourage growth and innovation in the digital platforms market"[27], yet provides no evidence for this hypothesis. On the contrary, if compliance becomes overly complex and results in declining conversion rates and revenue, global companies and startups may withdraw or not develop products and services for the Australian market. This prospect was evidenced soon after the introduction of the GDPR in May 2018, which required a legal basis for personalised advertising. Rather than complying with the GDPR, many non-EU publishers chose to block access to content for users in Europe[28]. In this way, extremely strict privacy regulation in Australia could ultimately have detrimental effects on consumer choice and access to digital products and services.

Recommendation 17: Broader reform of Australian privacy law

Broader reform of Australian privacy regime to ensure it continues to effectively protect consumers' personal information in light of the increasing volume and scope of data collection in the digital economy. This reform should have regard to the following issues:

1. *Objectives: whether the objectives of the Privacy Act should place greater emphasis on privacy protections for consumers including protection against misuse of data and empowering consumers to make informed choices.*
2. *Scope: whether the Privacy Act should apply to some of the entities which are currently exempt (for example small businesses, employers, registered political parties, etc.).*
3. *Higher standard of protections: whether the Privacy Act should set a higher standard of privacy protection, such as by requiring all use and disclosure of personal information to be by fair and lawful means.*
4. *Inferred information: whether the Privacy Act should offer protections for inferred information, particularly where inferred information includes sensitive information about an individual's health, religious beliefs, political affiliations.*
5. *De-identified information: whether there should be protections or standards for de-identification, anonymisation and pseudonymisation of personal information to address the growing risks of re-identification as datasets are combined and data analytics*

[27] ACCC (July 2019), Digital platforms Inquiry Final Report, p.443.
[28] South, J., "More than 1,000 U.S. news sites are still unavailable in Europe, two months after GDPR took effect" at *NiemanLab blog*, August 7 2018, at http://www.niemanlab.org/2018/08/more-than-1000-u-s-news-sites-are-still-unavailable-in-europe-two-months-after-gdpr-took-effect/

technologies become more advanced.

6. *Overseas data flows: whether the Privacy Act should be revised such that it could be considered by the European Commission to offer 'an adequate level of data protection' to facilitate the flow of information to and from overseas jurisdictions such as the EU.*
7. *Third-party certification: whether an independent certification scheme should be introduced.*

17.1,17.2,17.3

As noted in our analysis of Recommendation 16, we welcome the recognition that privacy issues are economy wide, and not just a question for digital platforms, and acknowledge that potential changes to the Privacy Act is an important area of exploration. We would look forward to engaging in further consultation in relation to the objectives, scope and protections offered under the Privacy Act.

17.4 & 17.5

In its consumer survey, the ACCC found that 48 per cent of digital platform users considered inferred tastes and preferences (48 per cent) or actual (46 per cent) or inferred (45 per cent) opinions and beliefs to be their personal information[29]. While this is in fact a minority of users that held this view, it nonetheless begs the question: did the ACCC share any information about the value of inferred information in the provision of digital services?

Inferred information through data analytics fuels effective and personalised services. As mentioned, the crowdfunding website GoFundme collects IP addresses in order to show a user relevant campaigns in their city. Such information is often de-identified or in the aggregate. For example, Google uses aggregate, inferred information about the average speed of drivers to determine peak hour traffic in Sydney, providing a useful data set for different parties to improve transport planning.

Sophisticated data analytics is increasingly needed for data-driven industries to maximise their impact, and value to consumers. Having said that, DIGI acknowledges that the industry may need to do more to communicate to users how data analytics provides them with better services. As CIO magazine notes:

> *"Analytics has repeatedly demonstrated that it is a proven science, a powerful tool that generally leads to significant improvements in productivity, efficiency, sales, profits and other key business metrics and goals."*[30]

Management consultancy Bain & Co argue that opportunities for data exist in almost every industry[31], and the examples of innovative applications of data analytics are countless. In France, four hospitals are using ten years' of hospital admissions records to develop day and hour-level predictions of the number of patients expected at different times, which assists the arrangement of adequate staffing[32].

Inferred and aggregate information analysis has the potential to solve real-world social problems, and create financial value for a wide range of businesses. Any onerous restrictions on the use of such datasets should be examined in the context of this meaningful and increasing consumer value.

---

[29] ACCC (July 2019), Digital platforms Inquiry Final Report, p.479
[30] Edwards, J., (2017), "Demystifying the dark science of data analytics", accessed at: https://www.cio.com/article/3233188/demystifying-data-analytics-how-to-create-business-value-from-data.html
[31] Wegener, R. & Sinha, V., (2013), "The value of Big Data: How analytics differentiates winners", accessed at: https://www.bain.com/insights/the-value-of-big-data/
[32] Marr, B., (2016), "Big Data In Healthcare: Paris Hospitals Predict Admission Rates Using Machine Learning", accessed at: https://www.forbes.com/sites/bernardmarr/2016/12/13/big-data-in-healthcare-paris-hospitals-predict-admission-rates-using-machine-learning/#38c7a37879a2

17.6

We note there is significant overlap between the GDPR and the Australian Privacy Principles, yet one of the key differences is that the latter provides a set of principles-based standards, affording complying businesses with the flexibility to apply these to their own operations. In comparison, the GDPR is more prescriptive and detailed, and can therefore pose implementation challenges when applied to a wide array of digitised businesses.

17.7

On the certification scheme, we note that this recommendation goes beyond the standards of the EU's General Data Protection Regulation (GDPR), which contemplates a voluntary scheme, rather than making certification compulsory for certain entities. Many DIGI members already participate in third party verification schemes that promote organisational accountability and compliance; these existing schemes should not be ignored under any new recommendations. For example, Australia has signed on to the APEC Cross Border Privacy Rules (CBPR) that aim to build consumer, business and regulator trust in cross border flows of personal information[33].

That said, DIGI cautions the ACCC against a one-size-all approach that is imposed upon companies regardless of their scale and resources. Such an approach would raise barriers to market entry for technology investors, or any company or startup that may have a small number of staff in Australia and not have the same resources to host external privacy audits as larger digital service providers.

While this is a well-intentioned effort to create better conditions for competition in the market, the result may be the inverse: the measures may have an anti-competitive effect, as only the larger companies will have the resources to undergo such audits. The consumer interest may be better served by targeted audits in response to a proven breach of data protection law and measurable consumer harm, regardless of the size of the company. We note that many European Data Protection Agencies appear to be moving away from periodic routine audits, as this has proven to be too resource and time-intensive and not scalable in the long-term[34].

Recommendation 18: OAIC privacy code for digital platforms

An enforceable code of practice developed by the OAIC, in consultation with industry stakeholders, to enable proactive and targeted regulation of digital platforms' data practices (DP Privacy Code). The code should apply to all digital platforms supplying online search, social media, and content aggregation services to Australian consumers and which meet an objective threshold regarding the collection of Australian consumers' personal information.

The DP Privacy Code should be enforced by the OAIC and accompanied by the same penalties as are applicable to an interference with privacy under the Privacy Act. The ACCC should also be involved in developing the DP Privacy Code in its role as the competition and consumer regulator.

The DP Privacy Code should contain provisions targeting particular issues arising from data practices of digital platforms, such as:

[33] Australian Government Attorney General's Department, "APEC Cross Border Privacy Rules – Australia's participation" in *Consultations, reforms and reviews*, at https://www.ag.gov.au/Consultations/Pages/APEC-cross-border-privacy-rules-public-consultation.aspx

[34] In its 2018 annual report, the Irish Data Protection Commission states "targets for audit are selected by considering matters such as the amount and type of personal data processed by the organisation concerned as well as the number and nature of queries, complaints and breach notifications that we receive." Data Protection Commissioner, *Final Report of the Data Protection Commissioner of Ireland | 1 January – 24 May 2018*, at p. 25, accessed at https://www.dataprotection.ie/sites/default/files/uploads/2018-11/DPC%20annual%20Report%202018_0.pdf

1. Information requirements: requirements to provide and maintain multi-layered notices regarding key areas of concern and interest for consumers. The first layer of this notice should contain a concise overview followed by more detailed information in subsequent layers. The final layer of the notice should contain all relevant information that details how a consumer's data may be collected, used, disclosed and shared by the digital platform, as well as the name and contact details for each third party to whom personal information may be disclosed.

2. Consent requirements: requirements to provide consumers with specific,opt-in controls for any data collection that is for a purpose other than the purpose of supplying the core consumer-facing service and, where consents relate to the collection of children's personal information, additional requirements to verify that consent is given or authorised by the child's guardian.

3. Opt-out controls: requirements to give consumers the ability to select global opt-outs or opt-ins, such as collecting personal information for online profiling purposes or sharing of personal information with third parties for targeted advertising purposes.

4.Children's data: additional restrictions on the collection, use or disclosure of children's personal information for targeted advertising or online profiling purposes and requirements to minimise the collection, use and disclosure of children's personal information.

5. Information security: requirements to maintain adequate information security management systems in accordance with accepted international standards.

6. Retention period: requirements to establish a time period for the retention of any personal information collected or obtained that is not required for providing the core consumer-facing service.

7. Complaints-handling: requirements to establish effective and timely mechanisms to address consumer complaints.

The ACCC considers that this recommendation could align with the Government's March 2019 announcement to create a legislated code applying to social media and online platforms which trade in personal information.

DIGI looks forward to engaging with the OAIC about such a code, and welcomes the emphasis on industry consultation. We do however note that issues surrounding data privacy and the collection of personal information are not restricted to digital platforms, and that general economy-wide standardisation or guidance is more appropriate than a code that ringfenced to a handful of designated digital platforms. Further, we are unsure why the ACCC has said that it "should also be involved in developing the DP Privacy Code in its role as the competition and consumer regulator"; in addition to confusion for businesses with proliferation of multiple codes, this creates confusion around regulatory responsibilities across different government departments.

In the development of this code, DIGI hopes that the OAIC will enact the provisions in its *Guide to developing codes*[35]. The guidelines state:

> *Under Part IIIB of the Privacy Act, the Australian Information Commissioner (the Information Commissioner)[4] can approve and register enforceable codes which are developed by entities on their own initiative or on request from the Information Commissioner, or developed by the Information Commissioner directly.*

[35] OAIC (2013), *Guide to developing codes*, accessed at: https://www.oaic.gov.au/privacy/guidance-and-advice/guidelines-for-developing-codes/

...The Information Commissioner has the option of developing a code (ss 26G (APP codes) and 26R (CR code)):

where a code developer has failed to comply with a request to develop a code, or
where a code developer has developed a code as requested by the Information Commissioner and the Information Commissioner has decided not to register the code

As the Government has already indicated that it will be introducing such a code, per its March 24 2019 announcement[36], we encourage the OAIC to have the industry develop such a code for consideration, rather than have the Information Commissioner develop this in the first instance.

With the expectation of a further consultation on such a code, we will not provide substantive comments here in relation to the ACCC's suggestions under Recommendation 18 however will note that many of DIGI's comments made in relation to Recommendation 16 and 17 should be taken into consideration, including:

1. The requirement to provide the name and contact details for each third party to whom personal information may be disclosed, goes beyond the standards of the GDPR, which simply requires categorisation of data processing activities into legal bases, and the provision of such information upon request during information access requests.
2. The risks of over-reliance on consent, as detailed in relation to 16a and 16c. Additionally, we note the same concerns as raised in relation to 17.4 and 17.5. It is not straightford to define "the core consumer service" when user behaviour and preference varies from person to person. The value added to a service from inferred or aggregate information may constitute what a given consumer considers to be the core consumer service.
3. The value of targeted advertising to consumers and a wide range of businesses, as detailed in relation to 16c.
4. In addition, we would ask that the scope of organisations covered, in particular "content aggregation services", be properly defined.

Finally, we encourage the OAIC and the Australian Government to rigorously examine user expectation in relation to this proposed code. It is worth noting that there are a range of options for consumers to manage their privacy through a variety of formats, including dynamic tools and just in time in-service prompts. There needs to be more sophisticated user testing to inform any reform in these areas. While the ACCC's acknowledgement that different options should be user tested is welcomed, the fact that the ACCC DPI final report considers that such testing could occur in a "laboratory setting"[37] shows a concerning lack of understanding on how product testing works on digital platforms[38], and underscores the need for deeper industry collaboration in relation to any proposed reform going forward.

Recommendation 22: Digital platforms to comply with internal dispute resolution requirements

The development of minimum internal dispute resolution standards by the ACMA to apply to digital platforms. The standards should, among other things, set out requirements for the visibility, accessibility, responsiveness, objectivity, confidentiality and collection of information of digital platforms internal dispute resolution processes. They should also set out the processes for continual improvement, accountability, charges and resources.

[36] Attorney-General for Australia (2019), "Media release: Tougher penalties to keep Australians safe online", accessed at: https://www.attorneygeneral.gov.au/Media/Pages/Tougher-penalties-to-keep-australians-safe-online-19.aspx
[37] ACCC (July 2019), Digital platforms Inquiry Final Report, p.488
[38] For more information, see *Adobe* "The Top 5 User Testing Methods", accessed at https://theblog.adobe.com/the-top-5-user-testing-methods/

All digital platforms that supply services in Australia, and have over one million monthly active users in Australia, will be required to comply with the standards. Once published, relevant digital platforms will have six months to comply with the standards. Breaches of the standards would be dealt with by the ACMA, which will be vested with appropriate investigative and information gathering powers and the capacity to impose sufficiently large sanctions for breaches to act as an effective deterrent.

The proposed internal dispute resolution standards cover a range of digital products and services in its application to services with over a million monthly active users (MAU). We encourage the ACMA to engage in broad industry consultation and proactive outreach to all companies that may meet this threshold, or aspire to meet it in the future. We note that some of the recommendations in relation to these standards may not be practical for all such businesses, particularly those with no or limited staff presence in Australia. For example, the requirement to ensure that "adequate resources are dedicated to its IDR procedures in Australia"[39] raises serious questions about how subjective judgements will be made about whether resourcing levels are "adequate".

User-generated content is an increasing component of popular digital services, whether it be offered in the form of reviews, customer interaction or other forms of user expression and information sharing. Per the introduction to this submission, Australia has a relatively small technology sector and few native global digital firms. We should be providing and incentives and encouragement for firms to grow their userbase to over a million MAU in Australia, not burdening companies at this important growth milestone.

Summary of positions against all recommendations

Recommendation	Comment
Recommendation 1: Changes to merger law	See section above for detailed comment.
Recommendation 2: Advance notice of acquisitions	We note similar concerns as expressed in relation to Recommendation 1. Such proposed regulations serve as a deterrent to global companies from investing or expanding operations in the Australian market.
Recommendation 3: Changes to search engine and internet browser defaults	No substantive comment.
Recommendation 4: Proactive investigation, monitoring and enforcement of issues in markets in which digital platforms operate	We welcome the shift away from algorithmic regulation, as expressed in the preliminary report. We question the use of public funds for another "extended public inquiry" without clear goals, terms of reference, or timeframes; this has already taken place through the ACCC DPI.

[39] ACCC (July 2019), Digital platforms Inquiry Final Report, p. 508

Recommendation 5: Inquiry into ad tech services and advertising agencies	DIGI is supportive of this recommendation.
Recommendation 6: Process to implement harmonised media regulatory framework	DIGI is supportive of efforts to modernise relevant laws for a digital era, while noting that digital products and services and media business are fundamentally different offerings in a number of ways. We would look forward to contributing to the process of developing a modernised regulatory framework.
Recommendation 7: Designated digital platforms to provide codes of conduct governing relationships between digital platforms and media businesses to the ACMA	See substantive comment above.
Recommendation 8: Mandatory ACMA take-down code to assist copyright enforcement on digital platforms	See substantive comment above.
Recommendation 9: Stable and adequate funding for the public broadcasters	DIGI is supportive of this recommendation.
Recommendation 10: Grants for local journalism	DIGI is supportive of this recommendation.
Recommendation 11: Tax settings to encourage philanthropic support for journalism	DIGI is supportive of this recommendation.
Recommendation 12: Improving digital media literacy in the community	DIGI is supportive of this recommendation. Many members are already engaging in such efforts and can be useful partners in this work.
Recommendation 13: Digital media literacy in schools	DIGI is supportive of this recommendation. Many members are already engaging in such efforts and can be useful partners in this work.
Recommendation 14: Monitoring efforts of digital platforms to implement credibility signalling	DIGI expresses similar concerns raised in relation to Recommendation 15, in relation to the variation and platform-specific nature of such efforts.
Recommendation 15: Digital Platforms Code to counter disinformation	See substantive comment above.
Recommendation 16: Strengthen protections in the Privacy Act	See substantive comment above.

Recommendation 17: Broader reform of Australian privacy law	See substantive comment above.
Recommendation 18: OAIC privacy code for digital platforms	See substantive comment above.
Recommendation 19: Statutory tort for serious invasions of privacy	DIGI is supportive of the need to prevent serious and harmful invasions of privacy economy-wide.
Recommendation 20: Prohibition against unfair contract terms	The economy-wide implications needs to be rigorously assessed, including greater definition of “unfair”.
Recommendation 21: Prohibition on certain unfair trading practices	This recommendation is largely concerned with particular behaviours in relation to privacy, in addition to matters already covered by the Australian Consumer Law. See our comments on privacy under recommendations 16, 17 and 18.
Recommendation 22: Digital platforms to comply with internal dispute resolution requirements	See substantive comment above.
Recommendation 23: Establishment of an ombudsman scheme to resolve complaints and disputes with digital platform providers	DIGI seeks to clarify how the responsibilities of this ombudsman would differ in scope and avoid duplication the existing responsibilities of the OAIC, the ACMA, the Office of the eSafety Commissioner or the State Offices of Fair Trading.