March 1, 2019
By email: platforminquiry@accc.gov.au

Dear Commissioner,

Thank you for the opportunity to provide a submission in response to the ACCC's preliminary report as part of its inquiry into digital platforms.

By way of background, the Digital Industry Group Inc. (DIGI) advocates for the interests of the digital industry in Australia. Its members include Google, Facebook, Twitter, Amazon and Verizon Media whose services range from search engines, content and communications platforms, and online stores. DIGI advocates for a balanced approach to regulating the online world that harnesses the tremendous social and economic opportunities digital services bring to Australia and globally, while also ensuring these services are used in a positive and beneficial way.

DIGI members recognise the importance of the issues raised in the preliminary report. We note that some individual members of DIGI have provided their own submissions to respond to the representations made in the preliminary report about specific companies, and the questions the preliminary report raises in relation to journalism in particular. In this submission, DIGI will focus on the implications of the preliminary recommendations for the broader economy, including the impact on digital service providers, organisations that rely upon digital services to market goods and services in Australia, and consumers of online services in Australia.

DIGI looks forward to further engaging with this inquiry in advance of the release of the final report. Should you have any questions or wish to discuss any of the representations made in this submission further, please do not hesitate to contact me.

Best regards,

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

Introduction

The terms of reference of the ACCC's inquiry into digital platforms are to investigate the state of competition in the media and advertising services markets, particularly in relation to news and journalistic content. However, the preliminary report advances recommendations and areas for further consideration that go far beyond this stated purpose, proposing changes that would have significant effects on a wide range of stakeholders, including:

1) every company with a digital presence that is data-driven, including startups, small businesses and digital service providers;
2) the wide range of organisations that rely upon digital advertising to market their goods, services and causes, including small to medium businesses (SMBs) and not-for-profit organisations (NFPs);
3) the wide range of free digital services that are financially sustained through online advertising;
4) Australian consumers, whose choice and quality of digital products available in the Australian market could be negatively affected. Such outcomes would be contrary to the ACCC's larger objectives to promote competitive markets and ultimately the purpose of Australia's Competition and Consumer Act, which is to enhance consumer welfare.

Looking at the wide range of impacts on a multitude of stakeholders, the specific policy problem that the ACCC inquiry is working to solve is unclear. Is it protecting the future of journalism? Is it preventing perceived anti-competitive behaviour by providers of digital services? Or is it increasing consumer understanding of how personal information is used in a data-driven economy? While DIGI recognises the importance of these questions, they each represent a challenge that requires targeted solutions. The Australian Government Guide to Regulation

requires that new regulations be accompanied by an assessment that defines the problem, considers whether the problem is best addressed by government, considers all viable solutions to it. It then considers the cost of the regulation, including to consumers and other parties, and whether it is greater than the benefit[1]. DIGI urges the ACCC to further define the problems it is working to solve, rigorously analyse the evidence base for those problems, and weigh the benefits of its preliminary recommendations against the costs to the aforementioned stakeholders, particularly Australian consumers who benefit from digital services. To that end, DIGI looks forward to further engaging with the ACCC as it refines its analysis and recommendations.

Badging & certification systems

The preliminary report offers several recommendations or areas for further analysis that incorporate "badging" or other certification systems. In its first area for further analysis relating to supporting choice and quality of news journalism, the ACCC has stated it is exploring the idea that "*digital platforms would be required to signal, in their display of content to consumers, content from news media businesses that have signed up to certain standards for the creation of news and journalistic content by complying with registered codes of journalistic practice. This signalling could be by way of a 'badge' on the news content as it appears in search results or a user's news feed."*

We fully appreciate the intent behind this area for further analysis, noting that many of the challenges facing the production of news and sustainable journalism are due to factors that long pre-date the emergence of digital service providers, including shifts in technology and consumer behaviour. That said, several DIGI members are advancing initiatives with similar objectives to protect and promote quality journalism, improve media literacy, and prevent the proliferation of fake news. However, we believe this area for further analysis is out of step with consumer behaviour online and is not conducive to supporting consumer choices. When seeking news and current affairs, Australian consumers are interested in i) content from Australian news media business as well as ii) user-generated commentary iii) blog posts from websites that are not news media businesses and iv) news content produced outside of Australia. Requiring digital service providers to signal, and therefore in a way promote, content from Australian news media businesses will falsely imply that content from other sources is inaccurate or otherwise unworthy of attention. In some ways, this detracts from competition in relation to news and current affairs content, as it devalues content that is regulated under overseas schemes or responds to a consumer need that larger media businesses in Australia cannot meet.

Preliminary recommendation 8b also incorporates a certification scheme where "*certain businesses, which meet identified objective thresholds regarding the collection of Australian consumers' personal information, undergo external audits to monitor and publicly demonstrate*

[1] Australian Government, *The Australian Government Guide to Regulation*, March 2014, p. 2, https://www.pmc.gov.au/sites/default/files/publications/Australian_Government_Guide_to_Regulation.pdf.

compliance with these privacy regulations, through the use of a privacy seal or mark. The parties carrying out such audits would first be certified by the OAIC."

Firstly, we note that this recommendation is inconsistent with the EU's General Data Protection Regulation (GDPR), which contemplates a voluntary scheme, rather than making certification compulsory for certain entities. We also note that this preliminary recommendation appears to apply to "certain APP (Australian Privacy Principles) entities", not just digital service providers; we welcome the acknowledgement that privacy-related issues are relevant economy-wide, rather than limited only to a handful of highly digitised businesses. Businesses across a diverse range of industries are utilise customer data to improve and tailor their products and services, for example supermarket and airline loyalty programs, and banking and financial service providers. These industries generally 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[2].

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[3].

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[4].

---

[2] Deloitte, *Deloitte Australian Privacy Index 2018*, May 2018, at https://www2.deloitte.com/au/en/pages/risk/articles/deloitte-australian-privacy-index.html

[3] 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

[4] 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, https://www.dataprotection.ie/sites/default/files/uploads/2018-11/DPC%20annual%20Report%202018_0.pdf

As noted throughout this submission, DIGI cautions against policy measures that will serve to discourage digital companies expanding their operations or content in Australia and thereby ultimately negatively affect consumer choice. Furthermore, we would also welcome further research and an evidence base in the ACCC's final report for how the audit process would serve to improve user understanding of data protection and assist people in gaining more control over their personal information.

Enforceable code of conduct & ombudsman

In addition to the certification scheme proposed in Preliminary Recommendation 8b, Preliminary Recommendation 9 recommends an OAIC "*enforceable code of practice under Part IIIB of the Privacy Act to provide Australians with greater transparency and control over how their personal information is collected, used and disclosed by digital platforms."* Many of the areas the ACCC outlines in relation to this code are broadly consistent with DIGI's members practices, and we welcome further discussion on how such a code could drive best practice across all digitised businesses. DIGI members include global businesses who have made amendments to their privacy policies and practices to comply with relevant requirements of the EU's General Data Protection Regulation (GDPR). In many cases, Australian users are already benefiting from these amendments.

We note that, as one of its areas for further analysis, the ACCC is exploring the possibility of a "Digital Platforms Ombudsman". DIGI seeks to clarify how such a role would differ in scope or complement rather than duplicate the existing responsibilities of the OAIC, the eSafety Commissioner or the State Offices of Fair Trading. For example, the ACCC has noted that such an ombudsman may resolve disputes from consumers relating to scams and the removal of such content, which we understand currently falls under the scope of the eSafety Commissioner and the ACCC's own Scamwatch program. The proliferation of regulatory bodies on a market-by-market basis would serve as a barrier to entry in the Australian market; such measures may have an anti-competitive effect, as only the larger companies will be able to resource the administration.

Any new regulatory frameworks proposed by the ACCC should recognise the increasing digitisation of businesses across the economy. As noted previously, businesses across a diverse range of industries utilise considerable volumes of customer personal information to improve and tailor their products and services, for example supermarket and airline loyalty programs, and banking and financial service providers. To the extent the ACCC identifies clear evidence of consumer detriment in how customer data is being utilised, DIGI would urge the Commission to focus on targeted solutions to solve specific problems that are applied consistently across the economy -- rather than ring-fenced to a small number of 'digital platforms' -- to ensure that consumer detriment is effectively addressed.

User consent & targeted advertising

All DIGI members are committed to privacy, compliance with data protection regulation and to empowering users to control how their data is used. This is an area where all of our members have made longstanding investments and continue to do so. However, DIGI believes that the preliminary recommendations 8a and 8c in relation to consent require further analysis and stakeholder consultation by the ACCC.

We believe the final report would benefit from a more nuanced understanding of the wide range of reasons digital service providers collect data, outside of targeted advertising. The ACCC states *"digital platforms may passively collect data from users, including from online browsing behaviour across the internet, IP addresses, device specifications and location and movement data. The user data collected can enable digital platforms to create more detailed segmented user profiles, for use by advertisers wishing to target advertisements."*

Firstly, it is important to understand that certain data must be collected in order to ensure the basic operation of digital services. For example, the collection of a user's IP address ensures that content can be delivered to a user's device, that a digital service is displayed in the user's language, and reflects content relevant to their country. The collection of their browser or other device specifications ensures that the correct version of the service can be displayed to ensure basic legibility and size. This information must be collected in order to simply display a website in the correct format, language and to comply with all applicable laws and it is in the legitimate interests of the provider and to do so; requiring consent for such basic data collection would negate the ability to provide consumers with operational digital services.

Secondly, data collection and algorithm use is central to how digital service providers guard the safety and security of Internet users. In fact, there are best practice recommendations, often encouraged by Australian government departments, that encourage data use for this specific goal. Best practice in safety-by-design and privacy-by-design include the use of behavioural and content signals can be used to identify risky users, behaviour and content, even at the point of upload or contact. For example, Twitter uses behavioural signals to identify users who target others with abuse or harassment and limits the visibility of their tweets[5]. Similarly, a core commitment of the Global Internet Forum to Counter Terrorism, of which Facebook, Google and Twitter and members, is that digital businesses use machine learning technology to proactively detect terrorist content.

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; in the EU's General Data Protection Regulation (GDPR), consent is only one of six "lawful bases" for

[5] Harvey, D., & Gaska, D., "Serving healthy conversation", *Twitter Blog*, at https://blog.twitter.com/en_us/topics/product/2018/Serving_Healthy_Conversation.html

data processing[6], which include “legal obligation”, “vital interests”, “public task” and “legitimate interests”. In the EU, consent is only therefore required in certain circumstances recognising that this would make the provisions of many digital services unworkable and unsafe. Arguably, an over-reliance on consent mechanisms could contribute to “notice fatigue” where users do not pay adequate attention to consent mechanisms. We therefore welcome the fact that the ACCC is inviting stakeholder feedback on whether it would be appropriate to implement specific exemptions to the proposed notification requirements that are focused on consent, for example where personal information is collected for non-commercial purposes and in the public interest. As noted above, this is absolutely necessary to ensure the basic functionality, safety and security of digital services.

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 all members have comprehensive resources in place to inform and enable users to both better understand and manage their data use. However, DIGI is concerned about the economy wide implications of Preliminary Recommendation 8c in relation to consent that proposes to “*amend the definition of consent to require express, opt-in consent and incorporate requirements into the Australian Privacy Principles that consent must be adequately informed (including about the consequences of providing consent), voluntarily given, current and specific. This means that settings that enable data collection must be pre-selected to ‘off’.* DIGI is also concerned about the proposals to *”make legislative amendments that prohibit entities from collecting, using, or disclosing personal information of Australians for targeted advertising purposes unless consumers have provided express, opt-in consent.”*

This recommendation will have an impact on the whole economy, for every company or other organisation -- large and small -- that maintains an email list and markets goods, services or public interest causes on the Internet. 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 inquiry.

Firstly, such a recommendation will see the loss of revenue for a wide range of advertisers. Default disabling of ads personalisation would cost publishers a significant percentage of their revenue and result in a loss of content for users. As the U.S. Federal Trade Commission noted in comments to the U.S. Department of Commerce’s request for information on privacy: *“[C]ertain controls can be costly to implement and may have unintended consequences. For example, if consumers were opted out of online advertisements by default (with the choice of opting in), the likely result would include the loss of advertising-funded online content.”*[7] This

[6]Information Commissioner’s Office, “Lawful basis for processing”, *Guide to the General Data Protection Regulation (GDPR)*, at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[7]Federal Trade Commission, Staff Comments to National Telecommunications and Information Administration, In the Matter of Developing the Administration’s Approach to Consumer Privacy, 9 November 2018, p. 15, at

expected loss of advertising-funded online content would arguably extend to a wide range of online content and advertising types, including display advertising on media websites. Businesses across Australia use the Internet to connect with their customers and reach out to new customers. AlphaBeta has found that Australian SMBs attribute around $90 billion of income to the Internet, and 1 in 3 SMBs receive orders via online platforms[8]. An estimated 8.2 million Australians have purchased from, or visited, an SMB after seeing content relevant to the business on Facebook alone.[9]

Secondly, Preliminary Recommendation 8c works from a false assumption that targeted advertising is not valuable to consumers and businesses alike -- an assumption that we urge the ACCC to rigorously analyse and challenge. Advertising powers free digital services and the wide range of freely available content available to consumers. Furthermore, consumers benefit from targeted advertising as it enables a personalised experience and the discoverability of relevant goods and services often from small businesses. 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 ACCC to further examine the evidence base in its case for this preliminary recommendation, and conduct further analysis on the benefits that targeted advertising provides Australian consumers.

Thirdly, if compliance becomes overly complex and results in declining 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[10]. This is an example of how such regulation could have detrimental effects on consumer choice and access.

DIGI acknowledges that this is an extremely important area of exploration, and we look forward to further research and consultation to ensure any final recommendations in relation to user consent and targeted advertising serve the interests of consumers while enabling the growth of the increasing number of businesses that rely on revenues from online advertising.

---

https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf

[8] AlphaBeta, *Google Economic Impact, Australia 2015*, p. 25, at http://www.alphabeta.com/wp-content/uploads/2016/08/Google-ecomonic-impact-2015.pdf

[9] Facebook, *Connecting Benefits*, August 2018, p. i, at https://www.connectingbenefits.com.au/download/Connecting_Benefits.pdf

[10] 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/

Deletion of user data

DIGI members all allow their users to destroy, de-identify, access and correct their personal information in accordance with the Australian Privacy Act 1988 and where relevant they apply the GDPR's requirements in this area. However, DIGI has concerns in relation to the ACCC's area of further analysis on data deletion where *"consideration may therefore need to be given to whether an explicit obligation to delete all user data should be in place when a user ceases to use the services and/or whether data should automatically be deleted after a set period of time. This obligation would seek to go further than preliminary recommendation 8(d) as it would not require a user to actively request the deletion of the data and would prevent open ended retention of data."*

Firstly, we believe that a requirement to permanently delete a user's data when they cease to use a digital service may not be in line with consumers' expectations, particularly when most digital service providers already honour explicit requests for data deletion. In some DIGI members' experience of relevant user behaviour, it is often the case that people wish to be able to reactivate deactivated accounts, expecting their content (including photos, messages, etc) to be retained. Mandatory deletion is overly presumptuous of a users' intention when they cease to use a service.

Secondly, digital service providers are also required to retain data for a wide range of reasons. For example, companies subject to Australia's data retention and other laws must retain user data to comply with requests from law enforcement. Customer financial and tax data must be retained for certain periods to comply with tax regulations, and companies may also need to retain data necessary for the establishment, exercise, or defence of legal claims.

Finally, any final recommendations in this area should exclude the use of anonymised, aggregated or otherwise pseudonymised data that is used for analytics in order to provide users with improved services. For example, Google uses the average speed of drivers to determine peak hour traffic in Sydney, providing a useful data set for different parties to improve transport planning.

Algorithm transparency

Preliminary Recommendations 4 and 5 advance proposals for regulatory oversight of algorithms, requiring digital service providers to regularly provide information and giving the regulatory authority to publish reports.

Firstly, it is not clear how such a recommendation would serve to benefit Internet users -- in fact, the opposite may be true. The finer details of how algorithms work constitute highly sensitive commercial information. The prospect of having to disclose such sensitive information will serve as a deterrent to global digital companies and startups initiating or expanding their operations in

Australia. This could negatively affect the variety and quality of digital products and services available to Australian consumers, to the detriment of the ACCC's larger objectives to promote competitive markets and consumer welfare.

Despite this, and recognising the importance of a level of algorithmic transparency, many DIGI members are working to strike the right balance between transparency and preventing gaming, abuse and the disclosure of commercially sensitive, proprietary information. For example, Google publishes a number of resources for webmasters including a 164 page document that explains how Google determines good quality search results for the purposes of ranking organic search results, and Facebook will be announcing further initiatives in this area in 2019.

DIGI cautions that such a broad recommendation would have widespread consequences across the economy and serve as an unhelpful precedent. Crucially, it goes far beyond a proportionate solution to the specific business model challenges facing news media identified in the report's Terms of Reference. DIGI urges the ACCC to further define the problems it is working to solve in proposing general regulatory oversight of algorithms, rigorously analyse the evidence base for those specific problems, and weigh the benefits of its preliminary recommendations against the significant costs.

Mergers and acquisitions

Preliminary Recommendation 1 proposes clarifying particular factors that can be taken into account when assessing the likely competitive effects of a merger or acquisition, namely the likelihood of removing a *potential* competitor and the acquisition of data. Given the rapid pace of technological innovation and iteration within technology companies, we would question the criteria on which the regulator will be able to effectively assess the removal of a potential future competitor. We would also urge caution in assuming that access to customer data is in itself anti-competitive.

DIGI notes that unlike Preliminary Recommendation 2, Preliminary Recommendation 1 does not specify that this is about large providers of digital services only. Mergers and acquisitions in the technology sector are an important driver of innovation and investment, offering an incentive for entrepreneurs who start companies, for whom selling their company is commonly the goal. They can result in new products being brought to market, affording Australians with more consumer choice.

While DIGI members welcome effective regulation and transparency to ensure that mergers and acquisitions are not anticompetitive, the final recommendations must mitigate any unintended consequences that deter innovation, entrepreneurship and ultimately the provision of more digital services that benefit Australian consumers. A survey of technology investors in Europe found that 81% were concerned that "*the principle of designing policy and/or*

legislation in order to target specific companies (i.e. global giants) could lead to poor outcomes that inadvertently hurt or hinder tech startups"[11]. We therefore encourage the ACCC to consider ways that it can encourage local entrepreneurship, and lower barriers to access for emerging digital products and services in Australia; measures like Preliminary Recommendation 1 increase the barriers to doing business in Australia.

Copyright

In preliminary recommendation 7, the ACCC advances a proposal that "*ACMA determine a Mandatory Standard regarding digital platforms' take-down procedures for copyright infringing content to enable effective and timely take-down of copyright-infringing content. This may take the form of legislative amendments to the Telecommunications Act so that the ACMA has the power to set a mandatory industry standard applicable to digital platforms under Part 6 of the Telecommunications Act.*"

A "mandatory standard", as proposed by the ACCC, would represent a significant departure from the globally accepted standard for issuing take-down notices that is 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.

DIGI members dedicate significant resources to processing copyright removal requests. Individuals and organisations use digital service providers to express themselves and to share content; they should not be subject to a take-down regime that would have the effect of requiring platforms to remove first and ask questions later. Mandatory standards with high fines for errors will make it too risky for platforms attempt to protect the legitimate speech interests of ordinary Australians, at the expense of Australians' public dialogue and free expression.

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*

[11] Allied for Startups, *The Impact of Regulation on the Tech Sector: Informing a regulatory environment which leads to a stronger tech ecosystem in Europe*, December 2018, p. 7, http://alliedforstartups.org/wp-content/uploads/sites/3/2018/12/The-Impact-of-Regulation-on-the-Tech-Sector.pdf

online services.[12]" DIGI supports extending the Copyright Act's Safe Harbour Scheme 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.

[12] Productivity Commission, *Intellectual Property Arrangements Final Report No. 78*, September 2016, Recommendation 19.1 at p. 40, https://www.pc.gov.au/inquiries/completed/intellectual-property/report/intellectual-property-overview.pdf