12 September 2019

The Treasury of Australia
By online submission

DIGITAL PLATFORMS INQUIRY – BSA SUBMISSION ON ACCC FINAL REPORT

BSA | The Software Alliance is grateful for this opportunity to make a submission on the final report that the Australian Competition and Consumer Commission (**ACCC**) released on 26 July 2019 (**Final Report**)[1] regarding the Digital Platforms Inquiry (**Inquiry**). Our submission focuses on the recommendations in the Final Report (**Recommendations**) with respect to copyright take-down (Recommendation 8), privacy and personal information protection (Recommendations 16 to 20), and internal dispute resolution (Recommendation 22).

A. Statement of Interest

BSA is the leading advocate for the global software industry before governments and in the international marketplace. BSA members[2] are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things. BSA members have made significant investments in Australia and are proud that many Australian organisations and consumers continue to rely on BSA member products and services to support Australia's economy.

BSA and our members thus have a significant interest in the Final Report and the potential impact of some of the Recommendations on BSA members and the technology sector in general.

B. Recommendations

BSA and our members support the ACCC's objective of enhancing the regulatory framework for digital platforms to increase competition and consumer protection in media and advertising services. We also commend the ACCC for addressing some of the concerns we had raised in our submission of 15 February 2019[3] (**Earlier Submission**), including the incorporation of more flexible mechanisms for collecting and processing personal information.

[1] Made available at: https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

[2] BSA members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Baseplan Software, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[3] A copy of our 15 February 2019 submission to the ACCC is available on the ACCC's *Preliminary report submissions* page at: https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/preliminary-report-submissions.

However, we continue to have concerns with several Recommendations in the Final Report, which have the potential to go much further than the scope of the Inquiry and risk having negative effects on the wider digital economy in Australia. In particular, we are concerned about the broad scope of entities that could be affected by the Recommendations, as well as the Recommendations relating to the mandatory copyright take-down code (Recommendation 8), privacy and personal information protection (Recommendations 16 through 20), and internal dispute resolution (Recommendation 22). We provide below further details of our concerns, and some recommendations for the Australian government's consideration.

Scope of Entities Affected

BSA is concerned that the Final Report fails to properly define the scope of entities that may become subject to its Recommendations. Although the Final Report acknowledges that the ACCC's inquiry focused almost exclusively on purported harms caused by two individual companies, the Recommendations would seemingly apply to any firm that falls within the broad definition of 'digital platforms' used in the Final Report, including "*online intermediaries that collect information from disparate sources and present them to consumers as a collated, curated product*"[4].

While the Terms of Reference that gave rise to the ACCC's inquiry focused narrowly on digital platforms that have an impact on the media and advertising services markets[5], the definition used in the Final Report would encompass a much broader universe of actors. By covering any platform or service that gathers information from different internal or external sources, and presents the information as a collated product, the definition would sweep in entities whose platforms have no bearing on the media or advertising services markets. It could, for instance, include platforms and services for enterprise customers relating to network security, supply chain logistics, or customer relationship management.

The Final Report's Recommendations are intended to address harms purportedly caused by two individual platforms with substantial market power. Given the prescriptive nature of many of the Recommendations, it would be inappropriate to apply them to entities that lack market power or whose services have no bearing on the media or advertising services markets. To avoid inadvertent over-regulation of entities that do not pose the types of risks that are the intended focus of the Inquiry, we recommend that the scope of 'digital platforms' be narrowly defined for the purposes of any measures or requirements that the Australian government may adopt in response to the Recommendations.

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

Consistent with our Earlier Submission, BSA has significant concerns with the proposed process for developing a mandatory take-down code. BSA members create high-value copyright works that are often the subject of online infringement. At the same time, BSA members also operate a variety of online data management and intermediary services. BSA members therefore have experience interacting with notice-and-takedown regimes from not only the perspective of rightsholders who submit large volumes of takedown notices, but also as intermediaries that must process takedown notices. Based on these dual experiences, BSA understands the critical importance of policy frameworks that appropriately balance the needs of both rightsholders and online intermediaries. We are concerned that the process set forth in Recommendation 8 will fail to achieve that balance and will ultimately fail to accomplish the goals described in the Final Report.

[4] See definition of "digital content aggregation platforms" on page 41 of the Final Report.

[5] As alluded to on page 41 of the Final Report.

As a threshold matter, it is unlikely that Recommendation 8 will achieve its stated objective of alleviating the "*difficulty, cost, and delay in enforcing intellectual property rights against overseas-based digital platforms*"[6]. To the extent that a platform is already established and operating within the Australian market, then the problems of overseas service, establishing copyright-infringing conduct within Australia, and/or enforcement of judgements mentioned in the Final Report[7], should not arise or should not operate as significant challenges to rightsholders seeking to enforce their copyright in Australia. Conversely, it is unclear how such a code would apply to platforms that are not already subject to the jurisdiction of Australian courts.

More fundamentally, we have deep concerns that the one-size-fits-all mandatory code outlined in Recommendation 8 could fundamentally deviate from international best practices regarding notice-and-takedown. For instance, Recommendation 8 suggests that the mandatory code should include obligations for digital platforms to monitor their users' activities to proactively identify potentially infringing content. While some social media platforms have voluntarily implemented such measures, an affirmative duty to monitor or filter networks would create significant privacy and confidentiality concerns if it were to apply to all service providers that fall within the Final Report's broad definition of 'digital platform'. For instance, enterprise cloud services providers (e.g., Platform-as-a-Service and Infrastructure-as-a-Service providers) often provide infrastructure-like services to their customers and therefore lack visibility into the content that their customers host. The nature of these enterprise cloud services is that only the customers have visibility and control over their data and the services that they operate, unlike with social media platforms, video streaming services, video, image, and audio sharing services. Applying a duty to monitor to such service providers could require them to fundamentally reengineer their network architecture in ways that would undermine the privacy and confidentiality commitments they have made to their enterprise customers.

Rather than creating a one-size-fits-all mandatory code under the Telecommunications Act that would ignore the many types of services that might fall within the broad 'digital platform' definition, we instead recommend reforms to Australia's existing copyright safe harbour framework. Currently, the Copyright Act provides a covered entity with a safe harbour from legal liability for infringing content posted by their users provided that the covered entity expeditiously removes the content upon receiving a notification of claimed infringement by a rightsholder. Consistent with the objectives of Recommendation 8, the safe harbour is thus a strong incentive for covered entities to develop innovative approaches for ensuring the "*effective and timely removal of copyright-infringing content*". However, the safe harbour applies only to carriage service providers; and extending it to all online services providers would create incentives for digital platforms to ensure expeditious take-down of potentially copyright-infringing content.

Modifying the Copyright Act's existing safe harbour framework would be reasonable approach, particularly as rightsholders continue to test the effectiveness of the site blocking provisions that were signed into law as part of the Copyright Amendment (Online Infringement) Act 2018. These amendments, which were made after a public consultation and industry engagement process, are already designed to protect rightsholders by expanding the remedies available to them to allow them to apply for a court order directing not only a carriage service provider but also an online search engine to block websites that have the primary purpose or primary effect of infringing copyright. Given that these amendments only came into effect in December 2018 and have yet to be tested, BSA recommends monitoring their effectiveness instead of looking to introduce further, more intrusive adjustments to Australia's copyright regime.

[6] On page 276 of the Final Report.

[7] On pages 268-269 of the Final Report.

Recommendations 16 through 20: Personal information protection – General comments

BSA continues to support the implementation of considered approaches to personal information protection that increase the transparency of personal information collection and use; enable and respect informed choices by providing governance over that collection and use; provide consumers with control over their personal information; provide robust security; and promote the use of personal information for legitimate business purposes. However, we recommend that there be substantial further consideration of Recommendations 16 through 20 relating to privacy and personal information protection.

First, we remain concerned that Recommendations 16, 18, 19, and 20 go far beyond the terms of reference for the Inquiry, which are focused on the impact of digital platforms on the state of competition in the media and advertising services markets. Implementing these Recommendations would constitute a fundamental change in the regulatory framework applicable to privacy and personal information protection in Australia, affecting organisations across all industries, and not just digital platforms and related media and advertising services.

More importantly, Recommendations 16, 18, 19, and 20 appear to depart from Australia's established approach to privacy and personal information protection regulation. Until now, Australia has largely taken a principles-based, outcomes-focused approach to privacy and personal information protection, primarily through the Australian Privacy Principles (**APP**s). Introducing a raft of highly prescriptive measures of the type envisaged by these Recommendations would significantly compromise the enabling effect that the current established, principles-based approach has on innovation and development of the digital economy in Australia.

A related concern is that the conclusions in the Final Report continue to be disproportionately based upon the results of consumer surveys. While consumer surveys can be valuable sources of information, appropriate consideration must also be given to overarching privacy principles and global best practices in privacy and personal information protection, as well as comprehensive engagement with relevant industries. It is for this reason that the BSA developed a report on Global Privacy Best Practices, available at: https://www.bsa.org/~/media/Files/Policy/Data/2018_BSA_Global_Privacy_Best_Practices.pdf.

We note that in Recommendation 17, the ACCC proposed that there be a broader reform of Australia's privacy law, to be led by the Office of the Australian Information Commissioner (**OAIC**). In making this recommendation, the ACCC also noted that "*[a]ny wholesale reform of Australian privacy law will have wide-ranging impacts across the Australian economy beyond the targeted amendments set out in recommendations 16(a) to (f), and will require considerable further consultation and analysis far beyond the scope of this Inquiry*."[8] We submit that such wide-ranging impacts would also be caused by Recommendation 16 itself and also Recommendations 18, 19, and 20. We accordingly continue to recommend that all fundamental changes to the privacy and personal information protection framework, including those under Recommendations 16, 18, 19, and 20, should be subject to a thorough public consultation process like the one envisaged in Recommendation 17.

We offer further specific comments on Recommendations 16 through 20 below.

Recommendation 16: Strengthen protections in the Privacy Act – Specific comments

(a) **Update 'personal information' definition** – BSA supports clarifying the definition of 'personal information' in the Privacy Act for greater alignment with international standards. In doing so, BSA recommends that the Australian government seek to maintain flexibility in the definition to avoid an overly rigid application of the Privacy Act. In this respect, in the example given by the ACCC of

[8] On page 476 of the Final Report.

EU case law finding that dynamic internet protocol (IP) addresses are personal information[9], there was also an important qualifier noted by the ACCC – i.e., that the dynamic IP address "*is held with additional data that can be used to identify the individual*". In other words, a dynamic IP address by itself is not personal information.

(b) **Strengthen notification requirements** – While BSA supports measures to encourage the provision of clear and accessible privacy notices, notification requirements should not be overly prescriptive and should be based on the core principles of reasonableness and proportionality. This is already reflected in the APPs, which require entities to manage personal information in an open and transparent way, have a clearly expressed and up-to-date privacy policy, and to notify individuals of relevant matters *as is reasonable in the circumstances*. If, after appropriate inquiry and consultation (as we have recommended in our general comments above), the OAIC considers that any additional guidance is required on what is reasonable in specific circumstances, it should be contained in APP Guidelines in accordance with existing practice, rather than via the introduction of another layer of prescriptive requirements.

(c) **Strengthen consent requirements and pro-consumer defaults** – We thank the ACCC for taking in our comments from our Earlier Submission with respect to having bases other than consent for processing personal information[10] and to avoid 'consent fatigue'. In this regard, we are pleased that Recommendation 16(c) recognises other important bases such as where processing of 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. We note, however, that the ACCC has decided not to include the 'legitimate interests' basis of processing personal information in its Recommendation, citing the "*considerable uncertainty and concern surrounding the relatively broad and flexible definition of [such] basis for processing personal information under the GDPR*"[11]. It is unclear how this approach, which adopts only certain flexibilities from the GDPR, and leaves out others, accords with the ACCC's stated desire to "*align Australian privacy law with international data protection laws*"[12]. BSA accordingly recommends that the Australian government consider including the 'legitimate interests' basis for processing personal information. Further, in considering Recommendation 16(c), BSA recommends that the Australian government adhere to the maximum extent to a principles-based approach to consent – namely, that consent should be provided at a time and in a manner that is reasonable and relevant to the circumstances – and also subject this matter to the broader review and public consultation process contemplated under Recommendation 17.

(d) **Increase the penalties for breach** – BSA agrees that regulators should have the tools and resources necessary to ensure effective enforcement. However, we remain of the view that the existing penalties under the Privacy Act are sufficient to incentivise compliance and drive the right behaviours. Pegging the penalties for privacy breaches to the penalties for breaches of the Australian Consumer Law (**ACL**) would be arbitrary (since consumer protection law is an entirely separate body of law from privacy law and based on very different factors). This approach risks having a chilling effect on data-driven innovation in Australia, as organisations are disincentivised from embarking on innovation projects for fear of arbitrary and disproportionate penalties.

Recommendation 17: Broader reform of Australian privacy law

BSA supports having a broader reform of Australia's privacy regime, especially to keep pace with emerging technologies such as data analytics and artificial intelligence. It would be important, as part

[9] On page 459 of the Final Report.

[10] On pages 465-466 of the Final Report.

[11] On page 466 of the Final Report.

[12] On page 460 of the Final Report.

of any such reform, to ensure that Australia's regime continues to have an enabling effect on innovation and development of the digital economy in Australia. In this respect, it would also be important to incorporate appropriate flexibilities in Australia's privacy regime for the processing of personal information, especially where such information has been de-identified, anonymised, or pseudonymised.

Recommendation 18: OAIC Code of Practice for digital platforms – Specific comments

BSA supports maintaining Australia's principles-based, outcomes-focused approach to privacy and personal information protection regulation. While we commend the ACCC's recommendation for the OAIC to consult industry stakeholders in developing an enforceable code of practice, we continue to be of the view that introducing an enforceable code of practice would be overly prescriptive and would create additional layers and costs of compliance for organisations. BSA would welcome additional *guidance* from the OAIC on privacy and personal information protection matters, but would also recommend that any such guidance should carefully weigh the need for more prescriptiveness against the need to preserve flexibility in business practices.

Recommendation 19: Statutory tort for serious invasions of privacy – Specific comments

The introduction of a statutory cause of action for serious invasions of privacy remains a concern because this concept is highly subjective, would create substantial uncertainty, and would result in organisations finding themselves subject to potentially overlapping penalties and legal processes based on the same set of underlying circumstances. The net result of this uncertainty would inevitably be that organisations would be reluctant to embark on developing new and innovative products and services in Australia which rely on large quantities of data (including personal information). Privacy-related causes of action and associated liability are already sufficiently covered under existing privacy legislation and, as outlined above in respect of Recommendation 16, any review of penalties in general should to be considered as part of a separate and comprehensive public consultation led by the OAIC.

Recommendation 20: Prohibition against unfair contract terms – Specific comments

BSA maintains that privacy should be carved out of a review of unfair contract terms under the ACL – amending the ACL is not the appropriate avenue to address concerns about privacy policies and practices. Instead, any concerns with unfair terms in the context of privacy policies should be addressed as part of the consideration of the notification requirements under the Privacy Act. If the notifications are handled appropriately and allow consumers to make informed choices, then it follows that changes to the ACL would not be required. In addition, the proposed amendments to the ACL as set out in the Final Report continue to go far beyond the terms of reference for the Inquiry, as they apply to *all* unfair contract terms and not just those relating to digital platforms. There are already sufficient consumer protections in place (for example, unconscionable conduct, misleading or deceptive conduct, and the existing unfair contract terms regime) to address power imbalances, and any changes to the regime would need to be considered as part of a separate and comprehensive consultation on consumer protection.

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

BSA notes that the ACCC has recommended that the Australian Communications and Media Authority develop internal dispute resolution (**IDR**) standards for digital platforms to comply with. The driving consideration behind this recommendation appears to be that "*neither Google's nor Facebook's IDR processes are sufficient*"[13]. Depending on how the scope of 'digital platforms' is defined (see our comments above), this Recommendation could affect a multitude of different and

[13] On page 508 of the Final Report.

unintended platforms. BSA therefore recommends that any such IDR standards should be developed in close consultation with the industry at large.

C. Conclusion and Next Steps

Given the complexity of the Final Report, the comments above are not an exhaustive list of BSA's concerns and recommendations. In particular, BSA remains concerned that there are many aspects of the Final Report which go beyond the scope of the terms of reference for the Inquiry, and should be subject to separate inquiries and consultation processes led by the appropriate regulators and involving relevant industry stakeholders.

We note that the Australian government is intending to carry out 'targeted consultation meetings' for a further 6 weeks following the close of submissions for the Final Report. We urge the Australian government to utilise the further 6-week period to engage in fuller dialogue with industry to discuss the broader issues raised, and the implications of the Recommendations made, in the Final Report.

Addressing challenges associated with the impact of digital platforms on competition and consumer protection is not an issue that is unique to Australia. BSA has been involved in discussions with governments, policy makers, and industry bodies around the world for several years on related issues. In our experience, working closely with regulators in jurisdictions around the world on best practices in legal and policy frameworks, the most successful laws are proportionate, principles-based, outcomes-focused, and not unduly prescriptive. In particular, data, privacy, consumer, and intellectual property laws should balance the rights, needs, and responsibilities of regulators, consumers, technology providers, third party stewards of data, and innovators.

BSA and our members would be delighted to further engage with the Australian government to respond to any questions and to explore ways in which BSA and our members can work with the Australian government and other stakeholders to develop effective and balanced regulatory policies with respect to digital platforms.

If you require any clarification or further information in respect of this submission, please contact Mr Darryn Lim at darrynl@bsa.org or +65 6292 0680.

BSA | The Software Alliance