THE LAW SOCIETY
OF NEW SOUTH WALES

Our Ref: PDL: EEin1639193

8 February 2019

Mr Jonathan Smithers
Chief Executive Officer
Law Council of Australia
DX 5719 Canberra

By email: natasha.molt@lawcouncil.asn.au

Dear Mr Smithers,

ACCC Digital Platforms Inquiry – Preliminary Report

Thank you for the opportunity to contribute to a submission on the Australian Competition and Consumer Commission's ("ACCC") *Digital Platforms Inquiry Preliminary Report* ("Preliminary Report").

The Privacy and Data Law Committee of the Law Society of New South Wales has contributed to this submission.

The Law Society of NSW acknowledges that the complex and rapidly evolving nature of the digital platform marketplace is reconstituting the power and knowledge relations between consumers, digital platform providers, digital intermediaries, media organisations and advertisers. Data about activities, preferences and interests of individuals has become a new currency which consumers knowingly or otherwise trade for services offered over digital platforms. These changes have significant implications for data regulation of transparency, choice, unambiguous consent, reciprocity of benefits, and data handling practices of many entities, including providers of digital platforms. This is an important emerging area for privacy regulation in Australia.

The Law Society welcomes the contribution that the Preliminary Report makes to addressing pertinent issues in this emerging area of regulation and law reform. We strongly agree with the ACCC's position that privacy and data protection laws have a role to play in increasing consumer protection and potentially enhancing competition between digital platforms. The business practices of a range of business entities impact the depth, range and value of data about activities, preferences and interests of individuals that are the currency of digital platforms. Those business practices need to be scrutinised from a number of perspectives: competition policy, consumer protection, privacy regulation, advertising and marketing regulation (particularly rules protecting children and other vulnerable persons), and protection of human rights, including rules against discrimination.

In our view, regulation to date has not been entirely satisfactory in addressing some of the issues that the rise of digital platforms either create or exacerbate. However, the ACCC's preliminary findings do not demonstrate a need for fundamentally different rules or centralisation of regulatory functions in the ACCC (or in any other broadly-based regulator). Rather, the problem has been satisfactory resourcing of the regulator.

The ACCC's preliminary findings rightly suggest some refinements of data privacy laws (which we discuss further below). However, the findings underlying these refinements are not by way of changing fundamental settings of data privacy law and regulation. Privacy law and regulation remains central in addressing many consumer concerns and protecting the legitimate interests of consumers, in parallel with operation of the Australian Consumer Law[1] ("ACL") and the ACCC actively fulfilling its consumer protection mandate.

Many of the consumer protection issues identified by the ACCC as associated with activities of digital platforms could be addressed by the ACCC exercising its broad consumer protection powers and discretions under the ACL, for example, shortcomings in privacy statements and other terms of provision of digital platforms. In its Final Report, the ACCC may wish to more specifically discuss why the ACCC has elected not to more actively exercise broad consumer protection powers and discretions to date. The Law Society notes that that the U.S. Federal Trade Commission has actively used similar powers against many digital service providers and changed digital markets behaviour as a result.

We suggest that the ACCC should exercise caution in recommending the creation of a new body of laws and regulation around digital platforms, rather than more specifically identifying and addressing any defects and shortcomings in existing regulatory schemes. It is tempting to move straight from identification of new issues caused by the rise of digital platforms to advocacy of new regulatory powers and functions centralised in a competition and consumer regulator. There is a significant danger that an inquiry rightly focussed upon the effect of a few very large digital platforms upon creation and distribution of news in Australia may become a vehicle for additional narrowly based regulation and further centralisation of powers in one regulator, rather than a spur towards improving existing regulation and the level of cooperation and coordination between existing regulatory agencies.

We have limited our comments to the ACCC's preliminary recommendations 8, 9 and 10 and to proposed areas for further analysis and assessment 4, 7 and 8 as they are most relevant to privacy considerations. In the final section of our comments we propose additional issues for the ACCC to consider.

Preliminary Recommendation 8 – Use and collection of personal information

We note the ACCC's concerns that the current regulatory framework does not effectively deter data practices that exploit the information asymmetries and bargaining power imbalances that characterise the relationship between digital platforms, intermediaries and consumers. We understand that the ACCC proposes to recommend that the *Privacy Act 1988* (Cth) ("Privacy Act") be amended to enable consumers to make informed decisions and to have greater control over privacy and the collection of their personal information.

The discussion as to the bounds of "personal information about individuals", de-identification and use of data linkage and de-identified data does not cite, and appears to have had little regard to, the extensive analysis and guidance of the OAIC on these topics. The discussion does not consider how data linkage may be conducted under appropriate,

[1] Schedule 2, *Competition and Consumer Act 2010* (Cth).

reliable and verifiable controls and safeguards that enable minimisation of use of personal information about individuals. The ACCC does not discuss how empowering data intermediaries to use de-identified data subject to appropriate, transparent, reliable and verifiable controls and safeguards can provide benefits to consumers and enable data intermediaries to capture value that otherwise accrues only to the operators of the major digital platforms themselves. Of course, any such benefits must be fairly shared with individuals. Benefits may not be identified and shared unless there is greater transparency as to such data practices and better understanding of consumers and other stakeholders as to what are fair and reasonable uses of data about individuals (whether or not those individuals are identified or identifiable to the relevant entities using that data). This transparency requires better engagement of digital service providers and data custodians with affected individuals about fair and reasonable uses of data about individuals. Engagement with consumers as to what is fair and reasonable is more likely to change market behaviour quickly and pervasively, as compared to the slower processes of formulating, enacting and adapting regulation.

Notification and consent

The ACCC proposes to recommend that Australian Privacy Principle ("APP") 5 be amended to impose greater notification requirements when personal information of consumers is collected or disclosed.[2] Additionally, the ACCC proposes to recommend that the definition of consent in the Privacy Act be amended to include "*only* express consent"[3] (emphasis added).

Notification and consent are increasingly problematic. Many data collections are intermediated by devices, such as the Internet of Things ("IoT") devices, where the affected individual is not the person notified or providing consent. Consumers may already be overwhelmed or fatigued by information. Provision of more, or even better, information places the onus upon the consumer to then read, assimilate and evaluate that information. Often a consumer may think, rightly or wrongly, that they need the service and they don't really have a choice. We recommend that there is greater emphasis upon trust marks and other industry regulatory initiatives that encourage digital service providers to act in ways that nurture trust, rather than burdening consumers with more information, however well condensed, curated and presented that information may be. We suggest that, given the increasing pervasiveness of IoT devices, the default assumption should become that device-intermediated collections of information from individuals should not require consumers to read or understand particular disclosures or to provide active consents, where such collections (and subsequent uses and disclosures) comply with registered codes that set out fair and reasonable data handling practices for particular devices or applications or particular industry sectors.

There is often a misconception amongst consumers that organisations require consent from the individual to collect, use and disclose their personal information. This misconception is compounded by the fact that many organisations require consumers to "agree" to their privacy policy in the registration process. The Preliminary Report elaborates on the inadequate nature of consumer consents as a result of being poorly informed; not freely given; exercised in response to "clickwrap agreements", "bundled consents" and subject to unilateral or "take-it-or-leave-it" terms.[4]

---

[2] See proposed recommendation 8(a), Australian Competition and Consumer Commission, *Digital Platforms Inquiry Preliminary Report,* December 2018 (hereafter ACCC, *Preliminary Report*) at p. 227.
[3] Proposed recommendation 8(c), ibid p. 229.

[4] See ACCC, *Preliminary Report* Chapter 5.

We note that, although there may be some overlap in their contents, the requirements for privacy policies pursuant to APP 1 and collection notices pursuant to APP 5, are two separate requirements under the Privacy Act. Neither APP 1 nor APP 5 require a consumer to consent to a privacy policy or collection notice. While the Preliminary Report lists the limited circumstances in which consent is required under the Privacy Act, the discussion of consent and privacy policies is confusingly combined.[5] Further, the Preliminary Report does not coherently explain the interaction between privacy policies and collection notices under the Privacy Act, nor does it make recommendations to dispel the misconception that consent is required for organisations to collect, use and disclose personal information.

The ACCC may wish to consider whether it can use its consumer protection powers in circumstances where the ACCC is concerned that data platform operators and other digital service providers are misleading or confusing consumers or imposing unfair contract terms through lack of transparency as to relevant data handling practices.

Erasure of personal information

In circumstances where consumers have withdrawn their consent and their personal information is no longer necessary to provide the consumer with a service, the ACCC proposes to recommend that APP entities be obliged to erase the personal information of individuals.[6]

The Law Society supports this proposal. We note it would bring Australia's privacy laws more closely into line with the GDPR's article 17 "right to erasure (right to be forgotten)". We also share concerns that with technological developments in data analytics, consumers are increasingly at risk when information provided at one point in time when consent was given could be used in the future in ways the consumer had not envisaged when they gave their consent.[7]

Third-party certification scheme

The ACCC proposes to recommend the introduction of a third-party certification scheme that would require audits of the data practices of certain APP entities.[8] The ACCC proposes that the APP entities required to obtain third-party certification would be those entities "that meet an identified objective threshold" (e.g. by collecting the personal information of a certain number of Australian consumers).[9]

The Law Society considers that an independent third-party certification scheme as outlined in preliminary recommendation 8(b) would bring Australia's privacy law more closely into line with the approach taken under the GDPR. We note that the full scope and requirements of the GDPR certification scheme is yet to be determined. It therefore remains to be seen how effective a third-party certification will be, whether it is necessary to prove compliance or whether it is enough that the law requires compliance and that there be effective mechanisms that address non-compliance.

Additionally, an important concern to take into consideration is the potential increase in costs that obtaining the certification will have on businesses and whether these additional costs are necessary to demonstrate compliance with privacy legislation.

---

[5] See ACCC, *Preliminary Report* Section 5.3 at pp. 175-181.
[6] ACCC, *Preliminary Report*, Proposed Recommendation 8(d), p. 231.
[7] Ibid.
[8] ACCC, *Preliminary Report*, Proposed Recommendation 8(b), p. 227.
[9] Ibid.

Increased penalties

The ACCC proposes to recommend that the maximum penalty for serious or repeated interference with privacy be increased to whichever is the higher of $10 000 000, three times the value of the benefit received or, if a court is not able to determine the benefit obtained from an offence, 10 per cent of the entity's annual turnover in the last twelve months.[10]

The Law Society considers that increased penalties, as outlined in preliminary recommendation 8(e), would encourage businesses, including digital platforms, to take privacy protection seriously. The ACCC's proposed recommendation to bring the penalties for severe or repeated interferences with privacy into line with the new civil pecuniary penalties under the ACL would elevate the status of privacy law and increase the deterrence effect of the requirements under the Privacy Act. An increase in penalties under the Privacy Act should be accompanied by an increase in the resources of the OAIC to effectively apply to the courts for civil penalties for serious or repeated interferences with privacy.

Direct rights of actions for individuals

The ACCC considers that remedies for invasions of privacy under the current regulatory framework are inadequate and proposes to recommend that individuals be given the right to bring a direct action for breaches of the Privacy Act.[11]

The Law Society supports, in principle, a direct right of action for individuals (or a group of claimants in a class action) to seek injunctions and compensatory damages for harm suffered as a result of an infringement of the Privacy Act as outlined in preliminary recommendation 8(f). We note that such a right would be separate from preliminary recommendation 10 to introduce a statutory tort of serious invasions of privacy.[12]

While the rationale for the recommendation seeks to provide consumers with a direct avenue to seek redress from a court without having to rely on representation by the OAIC,[13] the Law Society emphasises that the creation of such a right and corresponding remedies should not detract from the powers and resources afforded to the OAIC in its investigative and enforcement roles.

Increased resources for the OAIC

Considering the increasing volume, significance and complexity of privacy-related complaints, the ACCC proposes to recommend that the OAIC's resources be increased to support its further enforcement activities.[14]

The Law Society strongly supports preliminary recommendation 8(g) and continues to advocate for increased resourcing of the OAIC. As the proposed recommendations expand the functions of the OAIC, increasing its resources will be necessary for the OAIC to effectively carry out its duties and for the proposed recommendations to be effective. We particularly support the proposal to facilitate the OAIC's development of an enforcement focus.

---

[10] ACCC, *Preliminary Report*, Proposed Recommendation 8(e), p. 231.
[11] ACCC, *Preliminary Report*, Proposed Recommendation 8(f), p. 232.
[12] Ibid pp. 235-236.
[13] Ibid p. 232.
[14] ACCC, *Preliminary Report*, Proposed Recommendation 8(g), pp. 232-233.

Preliminary Recommendation 9 – OAIC Code of Practice for digital platforms

The ACCC proposes to recommend that the OAIC establish a digital platform-specific Privacy Code. The ACCC envisages that such a code would "contain specific obligations on how digital platforms must inform consumers and how to obtain consumers' informed consent, as well as appropriate consumer controls over digital platforms' data practices".[15]

The Law Society considers that an enforceable code, as proposed, may supplement the relevant provisions of the Privacy Act as they apply to digital platform providers and offer greater transparency to consumers regarding the handling of their information. Further, an enforceable code could encourage compliance with privacy requirements by digital platform providers by establishing greater regulatory oversight.

If the OAIC is to be the developer of a code of practice for digital platforms,[16] the Law Society considers that it should be adequately resourced for its involvement in the development, administration, investigation and enforcement of the code. We consider that it would be appropriate for the ACCC to participate in the development of such a code in consultation with the OAIC, privacy and data law experts and relevant stakeholders. Given the ACCC's expertise, it is suitably placed to offer a consumer protection focus and advise on the potential alignment of the prescribed code requirements with existing ACL requirements.

However, we also have some important reservations about a proposed code. The Law Society notes that the concerns raised about data practices that exploit information asymmetries and power imbalances between service providers and consumers are not exclusive to digital platform providers. Noting the importance of privacy protection in the consumer sphere more broadly, we suggest that consideration be given to whether a privacy code should have a broader reach. Should the ACCC recommend that an enforceable code is necessary, we suggest that an enforceable code may be more effective if it were to apply to the media and information services, marketing and advertising industry more broadly, rather than being solely limited to digital platforms.

We suggest that consideration also be given to whether an enforceable code of practice for digital platforms may be burdensome on the entities to which it applies as well as the OAIC and if it is indeed necessary in view of the other proposed recommendations to improve the data practices of digital platforms.

Preliminary Recommendation 10 – Serious invasions of privacy

Separate from the direct cause of action proposed in preliminary recommendation 8(f), the ACCC proposes to recommend that a statutory cause of action for serious invasions of privacy be adopted as recommended by the Australian Law Reform Commission.[17]

The Law Society has previously expressed support for a statutory tort of serious invasions of privacy.[18] The Law Society supports, in principle, the introduction of a statutory cause of action for serious invasions of privacy, covering intrusion upon seclusion and misuse of private information. Such a statutory cause of action could also have the potential to enable

---

[15] ACCC, *Preliminary Report*, p. 233.

[16] Ibid p. 234.

[17] Ibid pp. 235-236. See also Australian Law Reform Commission *Serious Invasions of Privacy in the Digital Era, Final Report,* June *2014*
<https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf>

[18] Law Society of NSW, "Submission 122", *Australian Law Reform Commission Serious Invasions of Privacy in the Digital Era*, 12 May 2014
<https://www.alrc.gov.au/sites/default/files/subs/122._org_the_law_society_of_nsw.pdf>

consumers to take action, especially where unauthorised surveillance and serious privacy concerns need to be addressed.

It is our firm view that any proposed statutory development for such a cause of action be subject to a rigorous consultation process including careful scrutiny of the detail of proposed legislation. We reiterate that in drafting the legislation it will be necessary to strike the appropriate balance between protection of privacy, freedom of expression and communication and national security, and that courts will be empowered to weigh up the public interest in privacy against any other countervailing public interests.

Proposed areas for further analysis and assessment

Proposal 4 - A digital platforms ombudsman

The ACCC is considering whether complaints about digital platforms could be handled by an ombudsman.[19]

The Law Society does not consider that a digital platforms-specific ombudsman is necessary.

We note that the powers proposed by the ACCC for a digital platforms ombudsman could potentially overlap with areas that are already handled by existing regulatory bodies. For example, preliminary recommendations 4(b) disputes relating to scams[20] and 4(d) disputes relating to false or misleading advertising[21] may sit within the operations of the ACCC, while 4(c) "disputes from media companies relating to the surfacing and ranking of news content" may potentially fall within the scope of the Australian Communications and Media Authority's ("ACMA") regulatory activities. If the ACCC proceeds to recommend a digital platforms ombudsman, we suggest that potential areas of overlap between regulatory authorities be reviewed to avoid duplication, minimise confusion, enable streamlining of resources and provide clarity of the complaint avenues, processes and expected outcomes for consumers.

The Law Society's preferred view, however, even where existing avenues for complaints about privacy breaches do not exist, is that existing regulatory bodies, (e.g. the ACCC, ACMA, OAIC or even the Australian Human Rights Commission), should be given the appropriate powers and resources to deal with those complaints, rather than creating a new ombudsman. We consider that it may not be necessary to have a designated digital platforms ombudsman if appropriate and effective avenues for complaint about the privacy breaches of data practices, more broadly, exist. This would also be an argument in further support of increasing the resources of the OAIC to handle the growing area of complaints arising from the data practices of digital platforms in line with the ACCC's preliminary recommendation 8(g).

Proposal 7 - Deletion of user data

The ACCC is considering whether a consumer's data should be deleted either once they stop using the digital platform's services or automatically after a set period of time.[22]

---

[19] ACCC, *Preliminary Report*, p. 16.
[20] Ibid.
[21] Ibid.
[22] Ibid p. 17.

The Law Society acknowledges that this proposal would go further than preliminary recommendation 8(d) which appears to specifically place the onus on the consumer to withdraw their consent in order for their personal information to be erased. It would align with the GDPR's article 17 "right to erasure (right to be forgotten)", which could be a useful guide for further development of this proposal. APP 11.2, which requires an entity to destroy or de-identify information that the entity no longer needs for any purpose, should also be taken into consideration.

Proposal 8 - Opt-in targeted advertising

In addition to strengthening consent requirements, the ACCC is considering whether express, opt-in consent should be required for targeted advertising.[23]

The Law Society supports this proposal in principle, subject to further details being developed, including how the mechanism would ensure ease of understanding and informed consent. We acknowledge that this proposal would align with the consent requirements under the GDPR and consider that the European Union's ePrivacy Directive[24] could offer useful guidance in the development of this proposal, particularly Article 5(3), which requires prior informed consent for storage or for access to information stored on a user's terminal equipment.

With respect to profiling, the Law Society suggests that the ACCC consider implementing a right similar to Article 22 of the GDPR which affords the data subject "the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or significantly affects him or her."[25] We note that there are certain limitations for this right, for example, if the decision is necessary for entering into, or for performance of, a contract between the individual and the organisation or if the decision is based on the individual's explicit consent.[26]

Further Recommendations for Consideration

"Personal information"

We note that section 5.4.2 of the Preliminary Report discusses the different definitions and interpretations of "personal information" and how this creates significant confusion for consumers of digital platforms. We suggest that it would be appropriate to include a recommendation to amend, or to seek further consultation on the amendment of, the definition of "personal information". This would have the benefit of clarifying the preliminary recommendation to enable the erasure of personal information[27] and considerations of deletion of user data.[28]

Privacy regulation in Australia is generally concerned with whether information falls under the category of "personal information". Section 6 of the Privacy Act defines "personal information" as:

---

[23] Ibid.

[24] Directive 2002/58/EC of the European Parliament and the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communication Sector (Directive on privacy and electronic communications), 12 July 2012 < https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:PDF>

[25] GDPR Article 22 "Automated individual decision-making, including profiling."

[26] GDPR Article 22(2).

[27] ACCC, *Preliminary Report*, Proposed Recommendation 8(d), p. 13.

[28] ACCC, *Preliminary Report*, further analysis issue 7, p. 17.

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

The definition covers two categories of information. The first, and perhaps less controversial, is information about an identified individual. This would include information such as name, address, phone number etc., which explicitly identifies an individual. The second category is information about an individual who is reasonably identifiable. The issue for ascertaining whether privacy law applies, concerns whether the individual is "reasonably identifiable" by the information. There is little guidance provided by the Privacy Act as to the nature or scope of information in this category.

The GDPR adopts the concept "personal data" which is defined by article 4(1) as:

> ...any information *relating to* an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an *identification number*, *location data*, *an online identifier* or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person... (emphasis added).

Notably, the GDPR provides a non-exhaustive list of the types of information relevant to the regulation, and particularly types of information that would be appropriate for privacy regulation in a digital platforms context. This guidance is beneficial for individuals as well as businesses and organisations that would be required to be compliant with the regulation. We suggest that the ACCC take into consideration a proposed recommendation for the review and potential amendment of the definition of "personal information" under the Privacy Act to provide greater clarity to consumers and digital platform service providers.

Extending privacy protection to the broader consumer sphere

We suggest that the ACCC consider whether making digital platform-specific recommendations will be beneficial for the information services industry in the long term. We welcome the ACCC's interest in bolstering privacy protection and suggest that the ACCC's recommendations with respect to privacy and data use extend to consultations on improving the privacy practices in the consumer sphere more broadly.

Should you have any questions in relation to this submission, please contact Ida Nursoo, Policy Lawyer, on 9926 0275 or email ida.nursoo@lawsociety.com.au.

Yours sincerely,

Elizabeth Espinosa
President