LAW INSTITUTE VICTORIA

T 03 9607 9311
F 03 9602 5270
lawinst@liv.asn.au
Date 28 February 2023

Committee Secretariat
Senate Standing Committees on Economics
PO Box 6100
Parliament House
Canberra ACT 2600

Inquiry into international digital platforms operated by Big Tech companies – Issues Paper

Dear Committee Secretariat,

The Law Institute of Victoria (LIV) is Victoria's peak body for lawyers and those who work with them in the legal sector, representing over 18,000 members. The LIV has a long history of contributing to, shaping, and developing effective legislation. The LIV welcomes the opportunity to provide feedback in relation to the Senate Economics References Committee's Issues Paper for the Inquiry into International Digital Platforms Operated by Big Tech Companies (the Inquiry).

The Inquiry seeks to consider the nature and extent of Big Tech companies exerting power and influence over markets and public debate, to the detriment of Australian democracy and users. Under the terms of reference, the Inquiry addresses the market shares of such platforms, the transparency of algorithms relative to public interest, the collection and processing of children's data, the adequacy and effectiveness of recent regulatory efforts and the broader impact of the concentration of market power on consumers, competition and macro-economic performance.

The LIV has consulted with members of the LIV Technology & Innovation Section to inform this submission.

General Comments

The LIV recognises that large overseas-based multinational technology companies play an important and influential part in the Australian economy, due to the multiple digital services and products developed by these organisations which are accessible to Australian users.

The LIV notes that the scope of the Inquiry is limited to the 'Big Five' tech companies in the United States, namely Google (Alphabet), Apple, Facebook (Meta), Amazon and Microsoft. However, non-western companies, such as Baidu, Alibaba, Tencent and Xiaomi, yield significant social and economic influence, which can also be expected to increase in Australia. While language barriers may minimise the number of English-speaking users who access non-western technology services (which tend to be provided in languages other than English), Australia's multilingual communities are likely to be impacted by the lack of regulation for non-western companies, particularly in circumstances where these companies use onerous terms and conditions or unsatisfactory privacy policies. The LIV therefore recommends that the scope of the Inquiry be expanded to include non-western Big Tech companies operating in Australia.

Market Concentration

1. **What impact does the market power of big tech companies have on the economy, society and small businesses?**

The LIV acknowledges that Big Tech companies generally have considerable market power within their respective fields. LIV members note that Big Tech companies are able to collect, store and mine data to their advantage by deriving user activity insights to inform their corporate strategies and services. Similarly, Big Tech companies generally have the resources to purchase the products or services created by

potential competitors,[1] or create similar features within their own systems to attract and maintain users.[2] LIV members are concerned that new market entrants are unable to compete with Big Tech companies, particularly where Big Tech companies are likely to have substantial financial resources.

2. What regulatory measures could be put in place to address the adverse impact of big tech companies? What other non-regulatory interventions could governments take to reduce the market power of big tech companies?

The LIV considers it important that Australia has an efficient regulatory framework which can respond quickly and effectively to new technology and corporate strategies. While supportive of holistic reform in relation to the regulation of Big Tech companies, however, the LIV cautions against reform which has the effect of limiting entrepreneurship or technological and small business innovation within Australia. The LIV supports reform which has the effect of creating opportunities for new market entrants to succeed or existing smaller technology organisations to grow.

The LIV recommends that any regulatory framework distinguish between Big Tech companies with significant market power and smaller tech companies by determining a threshold based on net profit or the number of users.

The LIV further recommends the introduction of a new government regulatory authority, or the establishment of a collaborative team across existing regulatory bodies, tasked with overseeing the regulation of Big Tech companies specifically.

---

[1] 'Facebook buys Instagram for $1 Billion' The New York Times (9 April 2012), accessible at <https://archive.nytimes.com/dealbook.nytimes.com/2012/04/09/facebook-buys-instagram-for-1-billion/>; 'Microsoft announces new multibillion-dollar investment in ChatGPT-maker OpenAI' CNBC (7 Feb 2023), accessible at <https://www.cnbc.com/2023/01/23/microsoft-announces-multibillion-dollar-investment-in-chatgpt-maker-openai.html>.

[2] 'Snapchat was an existential threat to Facebook' Business Insider (7 April 2020), accessible at < https://www.businessinsider.com/how-developer-mark-zuckerberg-invented-instagram-stories-copied-snapchat-2020-4>.

However, LIV members note that any such body would need to be sufficiently resourced in order to provide any meaningful opportunity for appropriate regulation.

Algorithm Transparency

1. **Akin to the Federal Trade Commission in the US, should an oversight body be established in Australia to undertake similar regulatory activities?**

The LIV supports this proposal, however, cautions that a new regulatory body requires sufficient resourcing to be effective.

The LIV also notes that a framework for the regulation of algorithms must consider the transparency and the 'interpretability' of the algorithm. While transparency refers to the sources of data used, evidence of decision-making and the assumptions made in learning, interpretability is the concept that a machine learning model and its output can be understood by a person in a logical way. This includes the purpose of an algorithm and why it is being used over human ability or other technology.

As the use of algorithms and artificial intelligence processes become more prevalent in both government and private entities, creating a regulatory framework which maintains transparency and interpretability in these processes is important for increasing public confidence in decisions made by government or private bodies. Individuals may not be aware that a decision is being made through an automated process, whether there is human oversight of the decision, what factors are being considered by the decision maker, and finally, whether any correspondence they receive amounts to a decision at all.

Further, the LIV submits that scrutiny must be applied to algorithmic processes to ensure conclusions reached amount to 'decisions' under the relevant legislation and encourage public confidence. Examples of wrongfully made decisions by government agencies, including the circumstances surrounding Centrelink's Robo-debt and the

Pintarich v Deputy Commissioner of Taxation (Pintarich) decision,[3] identify a need for improved regulation and oversight of automated decision-making processes more broadly.

In terms of interpretability of decision-making, the LIV expresses its concerns with 'black box' machine learning algorithms where the reasoning behind decisions cannot be traced or adequately explained. Decisions being made by opaque algorithms without explanation is 'analogous to evidence offered by an anonymous expert, whom one cannot cross-examine'.[4] The LIV suggests that any regulation must specifically articulate an obligation for manufacturers and organisations to avoid algorithms which do not allow an ability to assess or test the impact of unconscious, conscious, or other bias on its decision-making.[5]

The LIV recommends that any regulatory body be empowered to seek disclosure where companies seek to use algorithms. The scope and extent of any such disclosure should be guided by relevant factors, including the size of the company, the potential impact of the algorithm, the potential profit to be gained from the use of the algorithm and the likely impact on individuals.

3. **Similarly, are there other jurisdictions, such as the UK, EU and Japan, that also have applicable concepts that could be usefully incorporated into Australian law?**

Algorithms and automated decision-making tools are used increasingly in private and public administrative processes to increase efficiency and consistency in decision-making. However, the LIV is concerned that these tools are being implemented and

---

[3] [2018] FCAFC 79.

[4] Michael Brooks, Artificial Ignorance (2017) 238 (3146) *New Scientist*, 28–33; Frank A. Pasquale Glyn Cashwell, Four Futures of Legal Automation (2015) 63 *UCLA Law Review Discourse*, 26–48 <www.uclalawreview.org/wp-content/uploads/2015/06/Final-ALL.pdf>.

[5] European Commission, 'A Definition of AI: Main Capabilities and Disciplines', April 2019, < https://ec.europa.eu/futurium/en/ai- alliance-consultation>.

utilised globally, while regulation of these processes is governed at both the state and national level in Australia. The LIV is of the view that any approach to regulation must be consistent with internationally recognised guidelines and frameworks to effectively position Australia as a leader in digital economy regulation. This would effectively decrease the regulatory burden imposed on new and existing businesses and organisations attempting to grow or expand within the Australian economy.

The LIV proposes that regulatory efforts should consider the OECD/G20 AI principles as a principles-based and technologically neutral overarching guideline for algorithm use and automated decision-making processes in Australia. Reference to an internationally recognised overarching framework would ensure that Australian businesses and individuals are not hindered from participating in global markets, while international organisations will be encouraged to expand business operations in Australia. The LIV would welcome further consultation concerning whether adherence to regulatory guidelines or principles should be voluntary for individuals, private organisations and government entities.

The LIV has previously expressed concern that the implementation of the 'do no harm' principle in the Department of Industry, Innovation and Science's ('DIIS') AI and Ethics Framework was overly narrow by requiring only that artificial intelligence systems must not be designed to harm or deceive people and should be implemented in ways that minimise any negative outcomes. In particular, the principle does not address harm caused by negligent or reckless design. As a result, the LIV is concerned that there is insufficient accountability and liability for causing harm or damage to a consumer. Therefore, the 'do no harm' principle should be extended to cover negligent or reckless harm and be prioritised as the first principle, above the 'generate net benefit' principle.

Data & Privacy

1. **What benefits would arise from introducing a legal mechanism to allow people to seek compensation for privacy breaches in Australia (e.g. the establishment of a statutory tort for serious invasion of privacy)?**

The LIV supports the introduction of a statutory tort for serious invasion of privacy, as recommended in ALRC Report 123.[6] The LIV acknowledges the recent release of the Privacy Act Review Report 2022 by the Attorney-General's Department which proposes the introduction of a statutory tort in the form recommended by ALRC Report 123.[7]

2. **Would stronger penalties levied by government regulation act as an effective disincentive to prevent data leaks and hacks in the future? What should be the size and scope of any such penalties?**

The LIV generally supports an increase in financial penalties to incentivise Big Tech organisations to address potential privacy risks. In October 2022, the LIV provided feedback on the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022, which sought to increase financial penalties for cyber incidents at a percentage of an organisation's revenue, and received royal assent on 12 December 2022. The capping of penalties at a percentage of revenue would seek to incentivise regulatory compliance in industry, whilst ensuring that small and medium companies are not disproportionately affected by overwhelming penalties.

However, further reform is required to incentivise companies and directors to prioritise compliance and proactively engage with data security and privacy protection. The LIV welcomes future consultation on strategies to encourage directors, companies and organisations to participate in improving internal privacy and cyber security strategies.

---

[6] Australian Law Reform Commission, 'Serious Invasions of Privacy in the Digital Era: ALRC 123 Summary Report (2014). Available at https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-123-summary/recommendations-18/.
[7] Attorney-General's Department, 'Privacy Act Review Report 2022' (2022). Available at https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf.

3. **Do further changes to privacy laws in Australia need to be made to better protect Australians and change corporate attitudes regarding data collection and management?**

The LIV recognises that Australia's current privacy framework consists of different and overlapping pieces of legislation, resulting in a lack of consistently defined terms and obligations. The existing privacy framework in Australia is primarily covered by three key pieces of legislation, including the *Privacy Act 1988* (Cth) ('the Privacy Act'), the *Corporations Act 2001* (Cth) ('the Corporations Act') and the Australian Consumer Law ('the ACL'). In comparison, the European Union's ('EU') General Data Protection Regulation ('GDPR') is more developed and comprehensive in scope.

The LIV recommends that an overarching framework for digital privacy in Australia be introduced to respond to the gaps and inconsistencies in the current legislative framework. This new framework ought to consider existing issues in relation to the definition of personal information under the Privacy Act; the ambiguity around digital products and its coverage under the ACL's goods and services definitions; the ACL's 'reasonable consumer' test; the scope of misleading and deceptive conduct provisions in the digital context; and the absence of clear guidance for directors' duties in the context of cyber security.[8]

LIV members consider that the lack of standardised terms, coherent regulatory standards and mechanisms for enforcement means there is little appetite to strengthen corporate governance of cyber security risk. Big Tech corporations must be incentivised to improve their approaches to cyber security risk and to promote a secure-by-design approach. Company directors must be incentivised to take a certain level of responsibility for cyber security risk to decrease the siloed nature of cyber expertise within organisations. Following the enactment of the GDPR, European businesses became compliant under the regulations to avoid the risk of substantial fines and reputational damage. The LIV is of the view that Big Tech companies could be motivated to strengthen their corporate governance of cyber

---

[8] *Corporations Act 2001* (Cth), s 180(1), 181.

security risk through a deterrent approach in the short-term, with a reasonable amnesty period to allow corporations to adapt their systems and policies.

The LIV welcomes the opportunity to contribute to any consultations on a framework designed to encourage businesses to simply 'sight' identity documents for verification purposes, rather than storing the sensitive identity data of customers.

If you require further information, please contact Sarah Cooney, Technology & Innovation Section Lead,

Yours sincerely,

Adam Awty
Chief Executive Officer