14 April 2022

Australian Competition and Consumer Commission Digital Platform Services Inquiry

By email: digitalmonitoring@accc.gov.au

Submission on ACCC Digital Platform Services Inquiry - Discussion Paper released for the fifth report

About us

The **UNSW Allens Hub for Technology, Law and Innovation** ('UNSW Allens Hub') is an independent community of scholars based at UNSW Sydney. As a partnership between Allens and UNSW Law and Justice, the Hub aims to add depth to research on the diverse interactions among technology, law, and society. The partnership enriches academic and policy debates and drives considered reform of law and practice through engagement with the legal profession, the judiciary, government, industry, civil society and the broader community. More information about the UNSW Allens Hub can be found at http://www.allenshub.unsw.edu.au/.

About this Submission

The UNSW Allens Hub is grateful for the opportunity to make a submission on **the Digital Platform Services Inquiry – Discussion Paper for the fifth report** ('DP5'). This submission reflects my view as a researchers; it is not an institutional position. This submission can be made public.

The submission's main points are focussed on consumer protection issues relating to:

- the adequacy of the ACL;
- data access and limitation;
- dark patterns; and
- dispute resolution.

Specific recommendations are highlighted in the discussion below. (Note that this submission does not consider the very substantial competition issues raised by the DP5.)

CQ1 Consumer harms

This submission agrees wholeheartedly with the ACCC's detailed and comprehensive description of consumer harms arising from digital platform services set out in Chapter 5. Research undertaken by members of the Hub supports the potential for harm, particularly

in the areas of reduced privacy[1] and data security,[2] increased profiling, discrimination and exclusion,[3] vulnerable consumers,[4] 'dark patterns'[5]/consumer manipulation,[6] and lock-in.[7]

The rise in the use of connected devices (other than conventional computers and smartphones) is likely to exacerbate the likelihood of harm, as they provide to the digital platforms opportunities as both additional data collectors (with a much greater volume, intimacy and personalisation of data) and additional channels by which digital platforms (and third parties) can influence and manipulate consumers.[8]

Data aggregation by the platforms themselves is not the only problem to be addressed. The rise of the data broker industry,[9] and the development of sophisticated tools both to reidentify data and target micro-segments of consumers without reidentification at the individual level, are also factors which increase the risk of consumer harm.

CQ2 Adequacy of the ACL and need for reform

The ACL has some areas of strength in relation to addressing consumer harms arising from digital platform services in Australia. These include provisions in sections 18 and 29 prohibiting misleading and deceptive conduct, and false or misleading representations (and related provisions). Additionally, the current Bill before Parliament addressing reforms to unfair contract terms - Sch 4, *Treasury Laws Amendment (Enhancing Tax Integrity and Supporting Business Investment) Bill 2022* - has the potential to address several harms outlined by the ACCC in Chapter 5, if it is passed in its current form.

However, the ACL is currently inadequate to deal with all of the harms set out in Chapter 5.

CQ8-10 Data access and data limitation

Any discussions about data access and data limitations be conducted in conjunction with the current Privacy Act Review.

However, this submission offers some preliminary thoughts on this issue.

---

[1] Kayleen Manwaring, Katharine Kemp and Rob Nicholls, '(mis)Informed Consent in Australia (Report for iappANZ, 31 March 2021)', UNSWorks.
[2] Ibid. 104-105
[3] Katharine Kemp, 'Concealed data practices and competition law: why privacy matters' (2020) 16(2-3) *European Competition Journal* 628-672; Zofia Bednarz and Kayleen Manwaring, 'Hidden depths: The effects of extrinsic data collection on consumer insurance contracts' (2022) 45 *Computer Law & Security Review* 105667; Zofia Bednarz and Kayleen Manwaring, 'Keeping the (good) faith: implications of emerging technologies for consumer insurance contracts' (2021) 43(4) *The Sydney Law Review* 455.
[4] Kayleen Manwaring and Cachelin Hall, 'Legal, social and human rights challenges of the Internet of Things in Australia. Input paper for the Horizon Scanning Project' (2019, Input paper on behalf of the Australian Council of Learned Academies), www.acola.org, <https://acola.org/wp-content/uploads/2021/02/acola-iot-input-paper_legal-social-and-human-rights-challenges_manwaring-hall.pdf>.
[5] Kemp (n 3).
[6] Kayleen Manwaring, 'Will emerging information technologies outpace consumer protection law? The case of digital consumer manipulation' (2018) 26(2) *Competition and Consumer Law Journal* 141.
[7] Kayleen Manwaring, 'Emerging information technologies: challenges for consumers' (2017) 17(2) *Oxford University Commonwealth Law Journal* 265-289.
[8] Manwaring, 'Will emerging information technologies outpace consumer protection law? The case of digital consumer manipulation' (n 6).
[9] Manwaring, Kemp and Nicholls (n 1) Ch 5 (by Katharine Kemp).

Data access

A data access regime with the purpose of enabling data portability and interoperability for consumer services provided by digital platforms and third parties would be desirable. However, appropriate privacy safeguards would be essential, such as requiring that data was only allowed to be used for that purpose.

A data access regime should also be accompanied with a 'right to be forgotten' ie the ability for consumers to have their data deleted on demand, and by default when they move to another service provider.

Data minimisation

The larger the amount of data held by platforms and their partners, the larger the risk of privacy harms, including but not limited to increased risks of data breaches.

An overarching principle of data minimisation of consumer data acquired and held by the digital platforms should be encouraged by legislation, to minimise this risk of harm.

In an earlier submission to the Department of Home Affairs on personal information and cyber security, the UNSW Allens Hub recommended a strict liability regime for data breaches with penalties dependent on the number of Australians affected by a data breach.[10] This type of scheme would not only encourage good cyber security practice, but also good data minimisation practices, such as limited collection and regular deletion of data.

Such a strict liability scheme with penalties based on amount of data held, or people affected by harm, should be introduced.

CQ3 Staging of law reform/CQ4 Regulatory tools/CQ11 Dark patterns/CQ16 Transparency

UNSW Allens Hub members have completed significant research on exploitative and manipulative conduct (including what is referred to as 'dark patterns' in DP5) by digital platforms and others providing digital services.[11] It is generally known (and recognised by the ACCC) that commercial entities and their third-party contractors conduct a large amount of experimentation on consumer behaviour in response to stimuli in the digital environment in order to use that experimental knowledge to improve profit outcomes, but the detail this is usually kept confidential.[12] It is counterproductive for service providers to disclose to consumers when and how they use dark patterns or other 'digital consumer manipulation'

[10] Lyria Bennett Moses et al, *Submission on Australia's Cyber Security Regulations and Incentives* [2021] *UNSWLRS* 85 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4066114

[11] Kemp (n 3); Manwaring, 'Will emerging information technologies outpace consumer protection law? The case of digital consumer manipulation' (n 6).

[12] Anthony Nadler and Lee McGuigan, 'An impulse to exploit: the behavioral turn in data-driven marketing' (2018) 35(2) *Critical Studies in Media Communication* 151, 156.

techniques.[13] This is because it *may* reduce the techniques' effectiveness[14] and/or cause reputational damage due to a consumer backlash. The employment and job descriptions of behavioural psychologists, and algorithm writers, is not something most suppliers will willingly reveal to consumers. The very design of such techniques is intended to prevent self-discovery by consumers.

Without a working understanding of the data collected, the inferences drawn from that data, and what companies know about the effects of behavioural advertising, there is every chance that consumers will not realise what has actually happened to them, other than experiencing a case of buyer's remorse. They will ask themselves the question 'why did I do something so irrational or so harmful?' without having any idea that someone is to blame other than themselves.

As the use of data analytics increases, and transparency decreases, the likelihood of disbenefits for consumers and other data subjects is likely to increase. The new activities now made possible by hyper-personalised profiling, algorithmic microtargeting of marketing campaigns, and the growth of new data collectors and marketing media via connected devices and environments may lead to an opaqueness unprecedented in the consumer space: in other words, a mass inability to know our own minds.

While transparency is important, the effectiveness of disclosure and consent models in preventing harm to consumers has been robustly challenged,[15] including by the ACCC.[16] This lack of effectiveness may actually be worse when dark patterns are used, as the nature of behavioural advertising tactics is such that they 'may not be able to be defused by raising users' awareness or knowledge of how they operate.'[17]

However, there are other approaches to disclosure that may assist.

Better targeting and framing of disclosure are tactics that should be investigated for their potential for increased effectiveness.

The ACCC has mentioned several foreign law approaches in the DP.[18] In addition to these, a bipartisan Bill relating to digital platforms and dark patterns, originally introduced during the US Trump presidency, was recently re-introduced to the US Senate and House of Representatives. The Bill, entitled 'Deceptive Experiences to Online Users Reduction Act'

[13] Defined as '*the use of personalised consumer data collected, processed and/or disseminated by digital technologies, combined with insights from behavioural research, to exploit consumers' cognitive biases, emotions and/or individual vulnerabilities for commercial benefit'* Kayleen Manwaring, 'Surfing the third wave of computing: Consumer Contracting with eObjects in Australia' (PhD Thesis, University of New South Wales, 2019) 202.
[14] Eliza Mik, 'The erosion of autonomy in online consumer transactions' (2016) 8(1) *Law, Innovation and Technology* 1-38, 8.
[15] For example, Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton UP 2014); Elena D'Agostino, *Contracts of Adhesion Between Law and Economics: Rethinking the Unconscionability Doctrine* (Springer 2015) 50.
[16] Australian Competition and Consumer Commission, *Digital Platforms Inquiry Final Report* (2019) 394-422, 449-51.
[17] Nadler and McGuigan, 'An Impulse To Exploit: The Behavioral Turn in Data-Driven Marketing' (n 12) 160.
[18] DP5 97-8.

(**DETOUR Bill**)[19] is intended to 'prohibit the usage of exploitative and deceptive practices by large online operators and to promote consumer welfare in the use of behavioral research by such providers'.[20] Part of the DETOUR Bill mandates:

- regular disclosure to users and to the public of any behavioural or psychological research undertaken for 'the purpose of promoting engagement or product conversion';[21] and
- the appointment of an Independent Review Board registered with the FTC for each operator, whose purpose is to oversee any behavioural or psychological research conducted by large online operators.[22]

The first of these is a powerful provision. However, the Bill has its shortcomings, at least when considered in an Australian context. First, there remains a question as to competency and power of the proposed disclosees (ie consumers) to act appropriately on such disclosure, and second, whether simply the nature of the research constitutes sufficient disclosure to readily avoid harm. Additionally, there is the question of whether supposedly independent review boards paid for by the operators will devolve into mere 'ethics-washing' or 'ethics-shopping' exercises.[23]

Targeted disclosure

A preferred alternative scheme could provide for:

* detailed and specific disclosure of use of data;

* *inferences* made from that data; and

* the nature and specific outcomes of behavioural research undertaken, commissioned or used by corporates.

However, in order to overcome some of the objections of non-consumer stakeholders, this disclosure could be made commercial-in-confidence (to prevent a contested disclosure of trade secrets) to an educated *regulator* or other agency[24] with a remit to investigate the desirability or appropriateness of particular conduct. This approach may be more fruitful in preventing serious harms to consumers while still balancing an interest in robust competition.

Robust disclosure mechanisms are important to assist in overcoming the problems of corporate secrecy discussed above**.** However, disclosure and consent mechanisms *on their own* are likely to be insufficient in protecting consumers against real harms, particularly in light of the significant limitations on consent and disclosure models as a protection against consumer harm. It should be acknowledged that one of the major strengths of Australian consumer protection law is in its recognition that consumers in some circumstances need to

[19] S.3330/H.R.6083, 117th Congress (2021-22).
[20] S.3330/H.R.6083, 117th Congress (2021-22) recital.
[21] S.3330/H.R.6083, 117th Congress (2021-22), § 3(b)(1)-(3).
[22] S.3330/H.R.6083, 117th Congress (2021-22) §§ 3(b)(5)-(6).
[23] Ben Wagner, 'Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping?', in Emre Bayamlioglu and others (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press, 2018).
[24] Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880, 1802.

be protected against seller misconduct even when they have ostensibly 'consented' to a transaction.[25]

Considering the limitations of disclosure and consent models, the value of specific regulation targeting inappropriate *conduct*, such as particular forms of behavioural advertising, or inappropriate recommendations, should be explored. Such a response could be narrowly targeted, such as in the case of the door-to-door selling regime in the ACL, which is helpful in that it recognises that a particular form of conduct is likely to lead to a type of 'situational vulnerability',[26] that cannot be overcome by ostensible 'consent' at the moment of sale.

The proposed US DETOUR Bill attempts to prohibit 'unfair and deceptive acts and practices relating to the manipulation of user interfaces' by large online operators in addition to its disclosure and consent provisions. Section 3 prohibits:

- design, modification or manipulation of a 'user interface' that:
  - obscures, subverts or impairs 'user autonomy, decision-making, or choice to obtain consent or user data'[27] and,
  - is directed to a child, 'with the purpose or substantial effect of causing, increasing or encouraging compulsive usage'.[28] 'Compulsive usage' is defined as

    > any response stimulated by external factors that causes an individual to engage in repetitive, purposeful, and intentional behavio[u]r causing psychological distress, loss of control, anxiety, depression, or harmful stress responses;[29] and

- dividing consumers into groups for 'behavioral or psychological experiments or research' without informed consent.[30]

However, narrowly targeted and/or technologically specific changes to legislation such as this can quickly become out-of-date. For example, the drafting of the DETOUR Bill, with its emphasis on user interface design may be appropriate for website menus, but may not apply to manipulation undertaken in other ways by connected devices, such as on time of day, location, proximity to certain other individuals or blood sugar levels, or systems that rely for their manipulative effect on *several* separate parties and 'interfaces'.

Many advocates have suggested that a much more general prohibition against 'unfair conduct' is warranted.[31] However, Hub research analysing the utility of existing general provisions around misleading, deceptive and unconscionable conduct in the context of digital consumer manipulation has indicated that 'technologically neutral' or generally applicable legislation, even when combined with the 'flexibility' of a common law precedent system, is not adequate to address many problems of regulatory disconnection and

---

[25] Manwaring, 'Surfing the third wave of computing: Consumer Contracting with eObjects in Australia' (n 13).
[26] Productivity Commission, *Review of Australia's Consumer Policy Framework: Productivity Commission Inquiry Report* (30 April 2008) <http://www.pc.gov.au/inquiries/completed/consumer-policy/report#contents>. vol 2, 13.
[27] S.3330/H.R.6083, 117th Congress (2021-22) § 3(a)(1).
[28] S.3330/H.R.6083, 117th Congress (2021-22) § 3(a)(3).
[29] S.3330/H.R.6083, 117th Congress (2021-22) § 2(4).
[30] S.3330/H.R.6083, 117th Congress (2021-22) § 3(a)(2).
[31] 15 USC § 45.

reconnection in the face of sociotechnical change. Consequently, the adoption of a general 'unfair conduct' approach, without more, may be insufficient to deal with this problem.

When sociotechnical change occurs, legislatures and courts, and doctrinal scholars tend to rely heavily on judicial interpretation of existing common law and general legislative principles, at least those that are prima facie 'technologically neutral'. Development of specific principles from very general statutory formulations is then left up to the judiciary.[32]

Judicial interpretation of statutory principles is an essential part of the process of law 'keeping up' with sociotechnical change. However, there are limits with this approach in the context of sociotechnical change, and it is not a complete substitute for necessary and active intervention by legislative and regulatory authorities.

It is often *uncertain* how general legislative or judicial principles will apply in the face of sociotechnical change. In particular, businesses and consumers may suffer from a lack of *ex ante* guidance as to what constitutes acceptable business conduct in a rapidly changing environment**.** Additionally, there is a danger that attempts to continually expand the interpretation of general legal principles to emerging sectors, where those principles emerged in reaction to a vastly different context, can have the effect of overstretching existing doctrines beyond manageability or sense.[33]

However, greater specificity leads to problems with an appropriately *timed* response to sociotechnical change. It is essential that any framework must consider mechanisms for swifter responses by legislators and regulators, in forms amenable to quick review and assessment to keep the response up to date.

Any solution must then deal with the too general/too specific problem, and the timing problem. UNSW Allens Hub research has suggested a structure along the lines of:

*a general prohibition supported by a 'blacklist', or examples of specific unfair conduct (such as seen in Annex I to the EU provisions on 'unfair commercial practices'[34], or the specific examples of unfair contract terms provided in section 25 of the ACL) PLUS

*stop-and-review powers,[35] combined with the use of rule-making capabilities by regulators to make changes to the blacklist; PLUS

*funded technology assessment panels; PLUS

*enforced disclosure of corporate practices (as discussed above).[36]

[32] *Commonwealth Bank of Australia v Kojic* [2016] FCAFC 186 per Allsop CJ [58].
[33] Manwaring, 'Surfing the third wave of computing: Consumer Contracting with eObjects in Australia' (n 13).
[34] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market 2005 ('Unfair Commercial Practices Directive (EU)').
[35] Similar to ASIC's powers to issue stop orders on fundraising under section 739 of the *Corporations Act 2001* (Cth).
[36] Manwaring, 'Surfing the third wave of computing: Consumer Contracting with eObjects in Australia' (n 13). This analysis was developed further in a conference presentation: Kayleen Manwaring, 2020, 'Digital consumer manipulation and alternatives to consent', presented at Consent and Consumer Manipulation - Principles and Rules for a Fairer Platform Economy (Paper Workshop, ANU HMI/UniMelb CAIDE), Virtual, 16 September 2020.

The 'blacklist' should include specific examples of conduct by suppliers that is considered unfair: eg in the context of dark patterns or digital consumer manipulation, it has the effect or purpose of impairing a consumer's autonomy or decision-making capabilities, or attempts to exploit or create a particular vulnerability.

This solution may aid in speeding up responses to sociotechnical change in general, and manipulative practices specifically. The legislative provisions could provide as much *ex ante* guidance as is practically possible, and the disclosure of new corporate practices as they emerge could be responded to more quickly under rule-making capabilities of regulators. As an alternative to direct changes to the ACL, co-regulatory initiatives[37] such as *enforceable* statutory Codes of practice may also be helpful, at least where the views of stakeholders beyond industry and government are appropriately integrated.[38]

The use of technology assessment panels or specialist agencies to assist regulators in this exercise or to act as stand-alone review panels (possibly with a 'stop-and-review'[39] power) for new uses of technology or data may also assist.[40] The utility of such bodies would also be assisted where they are granted power to compel detailed disclosure by individual corporate entities of their confidential practices. The horizon-scanning,[41] expertise location, and awareness-raising functions of such a body are likely to be helpful.[42] Australia has no such central body, but some of its functions are exercised, albeit usually ad hoc by bodies commissioned to undertake such research.[43]

---

[37] Australian Communications and Media Authority, *Optimal Conditions for Effective Self- and Co-regulatory Arrangements* (Occasional Paper, June 2015) 10–11; Australia, Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation* (March 2014) 28.

[38] Roger Clarke and Lyria Bennett Moses, 'The Regulation of Civilian Drones' Impacts on Public Safety' (2014) 30 *Computer Law and Security Review* 263, 278.

[39] Derek Morgan, 'Technology in the Age of Anxiety: The Moral Economy of Regulation' (2009) 29 *Legal Studies* 492, 508.

[40] Solove (n 24), 1902; Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford University Press, 2008) 288–90; Brad A Greenberg, 'Rethinking Technology Neutrality' (2016) 100(1495) *Minnesota Law Review* 1495-1562, 1547; Lyria Bennett Moses, 'Regulating in the Face of Sociotechnical Change' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *Oxford Handbook of Law and Regulation of Technology* (Oxford University Press, 2017) 590–91. A recent example of the functions of such a committee can be found in the UK discussion on the establishment of a Digital Authority: see House of Lords Select Committee on Communications, *Regulating the Digital World* (2nd Report of Session 2017–19, HL Paper 299, 9 March 2019) [238]. Such a body is somewhat reminiscent of the now-defunct US Office of Technology Assessment.

[41] See also David Rejeski, 'Public Policy on the Technological Frontier' in Marchant, Allenby and Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: the Pacing Problem* (n **Error! Bookmark not defined.**) 51-53.

[42] Centre for Data Ethics and Innovation (CDEI) <https://www.gov.uk/government/groups/centre-for-data-ethics-and-innovation-cdei> accessed 9 May 2019.

[43] For example, ACOLA's horizon scanning role for particular projects. Australian Council of Learned Academies (ACOLA), 'ACOLA Receives ARC Funding to Undertake Two New Horizon Scanning Projects on AI and IoT' (Media Release, 21 May 2018) <https://acola.org/artificial-intelligence-internet-of-things/> accessed 12 September 2019.

Additionally, this inquiry should consider whether the current behavioural experimentation undertaken by commercial entities should be subject to the same ethics review procedures that are currently required by research involving human subjects in university settings.[44]

CQ12 Which digital platforms should any new consumer protection measures apply to?

All platforms.

CQ13 Monitoring of app marketplaces

Digital platforms should be obliged to take down malicious/exploitative third-party apps in their app marketplaces in response to takedown notices by fair trading agencies and the ACCC. They should also be required to pass on consumer complaints that they receive about malicious/exploitative apps to the regulator.

CQ15 Dispute resolution

Any reforms must also account for the difficulties of achieving redress for consumers, and in particular problems of cost and speed of litigation.

This submission supports the ACCC's recommendation for an independent ombudsman scheme, minimum internal dispute resolution standards and the employment of dispute resolution staff in Australia.[45]

This type of capacity is likely to be more useful for individual consumers than the expense and delay of formal litigation. However, funding for continuing robust regulatory intervention should also be prioritised.

As the right to litigate should not be excluded, and where representative actions are feasible can be a powerful deterrent to misconduct, specific prohibitions on exclusive jurisdiction clauses, compulsory arbitration clauses (especially those confined to a particular physical place) and choice of law clauses should be introduced.

Under section 18 of the ACL and its predecessors, competitor actions have provided significant impetus to enforcement of the misleading or deceptive conduct provisions.[46]

Competitor actions against unfair conduct should also be allowed.

Yours sincerely,

Kayleen Manwaring

[44] This was suggested in a slightly different context in Lyria Bennett Moses et al *Submission to the Office of the National Data Commissioner on the Data Sharing and Release Legislative Reforms* (8 Oct 2019), 2-3.
[45] DP5 100-101.
[46] See for example, *Hornsby Building Information Centre Pty Ltd v Sydney Building Information Centre Ltd* [1978] HCA 11; *Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd* [1982] HCA 44; *Campomar Sociedad Limitada v Nike International Ltd* [2000] HCA 12; *Telstra Corp Ltd v Singtel Optus Pty Ltd* [2014] VSC 35.