Balancing the Competition, Consumer Protection and Privacy Regulation of Digital Platforms

Submission in response to the
ACCC Digital Platform Services Inquiry Discussion Paper on
Updating Competition and Consumer Law for Digital Platform Services

Dr Katharine Kemp
Senior Lecturer, Faculty of Law, UNSW Sydney
Co-Lead, Data as a Source of Market Power Research Stream,
Allens Hub for Technology, Law & Innovation

Dr Rob Nicholls
Associate Professor, UNSW Business School
Co-Lead, Data as a Source of Market Power Research Stream,
Allens Hub for Technology, Law & Innovation

18 April 2022

The views in this submission are our own, based on our research, and do not represent the official views of UNSW Sydney. This submission does not attempt to address all of the topics raised by the *ACCC DPSI Discussion Paper on Updating Competition and Consumer Law for Digital Platform Services* (February 2022) ('Discussion Paper'), but is limited to the particular proposals as specified, with a special focus on the interaction of competition, consumer protection and privacy regulation.

1. New regulatory tools

We support the view that, in some areas, new regulatory tools should be considered for the regulation of large digital platforms.[1] Having regard to the years of delay and expense inherent in the litigation of competition and consumer law contraventions under regulations based on broad principles, it is appropriate to consider proposals for certain specific *ex ante* (or upfront) rules which would improve competition and consumer protection in digital markets at the outset. For example, rules prohibiting or limiting large platforms' acquisition of default installation of their products on devices or operating systems, could increase rivalry and consumer choice while providing large platforms with greater certainty regarding compliance. In line with proposed approaches in other jurisdictions, such rules should apply to designated platforms based on the extent of their customer reach; the significance of their data practices; and their competitive significance: for example, by reference to their number of active users and 'gatekeeper' status.

With regard to the significance of platform's data practices, this may also require consideration of the reach, revenue or market capitalisation of the relevant corporate group globally if the platform shares and combines the personal data of Australian consumers with its related bodies corporate globally.[2] For example, Amazon Australia's Privacy Notice gives the company permission to share Australian users' personal information with approximately 50 subsidiaries of Amazon.com Inc, operating diverse businesses from robotics to cloud services to pharmaceuticals.[3] At the same time, it is reported that Amazon's advertising revenues in Australia tripled in 2021, making it 'the fourth largest publisher in Australia based on unique visits, with only Google, Meta and YouTube ahead'.[4] The combination of these elements of the platform's data practices has significance for its potential impact on competition, consumers and privacy in Australia.

2. Interaction of competition, consumer protection and privacy regulation

The Discussion Paper acknowledges that 'the harms associated with digital platforms extend beyond competition and consumer protection concerns' and notes that the Australian government is considering reforms in other areas such as privacy, online safety and defamation, which are being led by other parts of the Australian government or independent government agencies. In making the submissions below, we are conscious that Treasury is currently conducting a major review of the *Privacy Act 1988* (Cth) ('*Privacy Act*'), which could lead to significant privacy law reforms.

---

[1] As raised in the Discussion Paper, pp 72-73.

[2] According to the eBay Australia User Privacy Notice, eg, eBay Australia shares personal information with 'eBay Inc Corporate Family Members'. eBay's Data Protection Officer has stated that eBay Australia discloses users' personal data to the 'many companies within this eBay group of companies which change from time to time due to company re-structurings, mergers, and acquisitions'. Correspondence with eBay Data Protection Officer on file with the author.

[3] The Amazon.com.au Privacy Notice https://www.amazon.com.au/gp/help/customer/display.html?nodeId=468496&ref_=footer_privacy accessed 18 April 2022, permits Amazons Australia to share Australian users' personal information with all 'subsidiaries that Amazon.com, Inc controls'.

[4] Sam Buckingham-Jones, 'Amazon triples Australian ad revenues, media execs predict it will triple again in 2022 as juggernaut starts to roll' (Mi3 website, 22 February 2022) https://www.mi-3.com.au/22-02-2022/amazon-tripled-its-ad-business-2021-track-more-100m-revenue-2022#u=0 .

The Discussion Paper notes the ACCC's earlier findings that lack of consumer awareness of, and control over, the collection and use of their information by digital platforms result in specific consumer harms, including (in shortened terms):

- **Reduced privacy and data security** that exposes consumers that exposes consumers to increased risks of data breaches, online identity fraud and more effective targeting of scams;
- **Risks to consumers from increased profiling**, which can be used to influence consumers' behaviour and carries risks associated with manipulation and loss of autonomy;
- **Risks to consumers from discrimination and exclusion**, resulting from the increased ability of firms to create highly detailed segments of consumers to assist in automated decision-making;
- **Increased risks to vulnerable consumers and children**, increasing the likelihood of being targeted with inappropriate products or scams, discriminated against, or inappropriately excluded;
- **Reduced choice and quality of digital platform services**, as consumers' preferences for greater control and transparency over the collection and use of their data remain unmet; and
- **Reduced consumer trust in digital platform services**, compromising the free-flow of information and hinder data-based innovation.[5]

These are all accurately described, and clearly relevant, harms created by inappropriate data practices of digital platforms. At the same time, the harms listed above tend to focus on harm at an individual level and in economic terms. This is significant because the Discussion Paper continues to take account of privacy harms in these terms when considering other proposals, such as potential mandated access to data. In these areas, the Commission appears to consider that potential privacy harms could be addressed by providing individual consumers with notice and choice[6] such that individuals could decide for themselves whether they object to further disclosure or use of their personal data and the consequences of these.

This conception of privacy in largely economic terms may also influence the prioritisation of proposals. For example, the Discussion Paper devotes somewhat more attention to the possibility of increasing rivals' access to personal data held by large platforms than the possibility of limiting personal data use by incumbents, although both have significant consequences for competition and privacy.

In our view, in considering such proposals, it is important to also acknowledge the value of privacy beyond the protection of consumers on an individual level in economic terms. Privacy is also recognised as a human right and a societal good.[7] This broader understanding of the value of privacy has long been acknowledged in international instruments, commentary and case law.[8]

---

[5] Discussion Paper, pp 44-45.

[6] Eg, Discussion Paper, p 92. See further section 4 below.

[7] See, eg, Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (2009); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford Law Books, 2010) 85-88. See also Debbie VS Kasper, 'Privacy as a Social Good' (2007) 28 *Social Thought & Research* 165 (explaining a 'social good' as 'that which is necessary for the functioning of society and which is interconnected with other fundamental societal characteristics').

[8] Universal Declaration of Human Rights (UNGA 1948), Art 12; International Covenant on Civil and Political Rights (UNGA 1966), Art 17; *John Fairfax Publications Pty Ltd v Doe* (1995) 37 NSWLR 81, 97-98 (Kirby P); Australian Law Reform Commission, 'Serious Invasions of Privacy in the Digital Era: Final Report' (ALRC Report 123, June 2014) 30-36; Megan Richardson, *Advanced Introduction to Privacy Law* (Edward Elgar, 2020) 19-22.

Freedom from constant monitoring and surveillance allows individuals space to create and invent; make mistakes; understand their own identity, origins, gender and sexuality; investigate; criticise the government; take care of their health; have meaningful, intimate relationships; engage in political protest. Protecting that freedom creates benefits for our democracy and society as a whole.

As the consumer protection regulator, the ACCC has been a strong advocate for consumer privacy, and outspoken in pointing out the power of digital platforms to vastly extend businesses' monitoring of consumer behaviour, as well as the profound information asymmetries and power imbalances between large digital platforms and consumers. We argue for caution in the consideration of proposals which may inadvertently exacerbate those power imbalances in the interests of increased competition, to the detriment of both the individual consumer involved in the transaction and society more broadly.

Rules that increase rivalry in particular markets by increasing collection of, or access to, data have the potential to degrade privacy both as an individual interest and as a societal good. Without doubt, the public also has an interest in robust and open markets; efficient advertising; safety; law enforcement; medical research; free access to information; improved communication, and other technologies, which depend on access to data, and sometimes access to personal data. Where these interests conflict, an appropriate balance must be found. Where the impact at scale is substantial, the responsibility for that balance should not rest on the shoulders of individual consumers.

3 Limiting the combination and use of consumer data

We welcome the Commission's consideration of measures which would limit or prohibit some uses and disclosures of personal data by designated digital platforms that operate across numerous and diverse markets.

Digital platforms have amassed immense datasets that incorporate consumers' personal information, based on several significant and concerning trends in platform data practices, including platforms':

- Collection of personal data beyond the reasonable expectations of consumers, including collection from unrelated third parties and monitoring consumers' behaviour on third party websites and apps;[9]

[9] See, eg, Facebook Data Policy https://www.facebook.com/privacy/explanation/ accessed 18 April 2022:

> 'Advertisers, app developers and publishers can send us information through Meta Business Tools that they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs or the Meta pixel. These partners provide information about your activities off of our Products – including information about your device, websites you visit, purchases you make, the ads you see and how you use their services – whether or not you have an account or are logged in to our Products.'

- Uses of personal data for purposes beyond the reasonable expectations of consumers, including consumer profiling and use of data for the company's unrelated commercial purposes;[10]
- Disclosure of personal data to, and exchanges of personal data with, companies operating across broad corporate groups in diverse markets with no connection to the consumer's transaction;[11] and
- Disclosure of personal data, and exchanges of personal data with, other companies, beyond the reasonable expectations of consumers, sometimes based on spurious arguments that what has been shared is not strictly 'personal information' even though it adds to the individual's profile.[12]

There are reasonable arguments that significant parts of the resulting datasets have been obtained through systematic contraventions of the Australian Privacy Principles (APPs), and in some cases, contraventions of the Australian Consumer Law (ACL) where consumers have also been misled about the nature of the data practices. While the Commission has recently been active in litigating in respect of alleged privacy-related contraventions of the ACL,[13] it is impossible to disgorge the personal data firms have obtained as a result of contraventions of the ACL or the APPs and thereby undo the privacy harms.

In these circumstances, the objectives of privacy, competition and consumer regulation are aligned in proposals to limit the combination of datasets of disparate businesses of digital platforms. The excessive sharing and repurposing of personal information between businesses operating across numerous markets not only disadvantages the individual in question and degrades privacy as a societal good, but hinders smaller rivals in each market, who do not enjoy the data advantages obtained by sharing large quantities of personal data across various markets against the reasonable expectations of consumers. In some contrast to the position in the European Union,[14] even 'consent' by an Australian consumer should not currently be seen as validating such practices, given the recognised inadequacy of current standards for 'consent' under the Australian *Privacy Act*.[15]

Rivals without access to datasets of this scale and scope are disadvantaged in their ability to compete by identifying profitable potential customers and innovating in product design and development, including through the use of artificial intelligence which relies on large datasets for

---

[10] See, eg, Google Privacy Policy https://policies.google.com/privacy#whycollect accessed 18 April 2022: 'We also receive information from advertising partners to provide advertising and research services on their behalf.'

[11] See fn 2 and 3 above and corresponding text.

[12] Consider, eg, the final bullet point under Cl 6 of the Tinder Privacy Policy https://policies.tinder.com/privacy/intl/en accessed 18 April 2022, titled "With your consent or at your request", which states:

> 'We may use and share non-personal information (meaning information that, by itself, does not identify who you are such as device information, general demographics, general behavioral data, geolocation in de-identified form), as well as personal information in hashed, non-human readable form, under any of the above circumstances. We may also share this information with other Match Group companies and third parties (notably advertisers) to develop and deliver targeted advertising on our services and on websites or applications of third parties, and to analyze and report on advertising you see. We may combine this information with additional non-personal information or personal information in hashed, non-human readable form collected from other sources.'

[13] Discussion Paper, pp 59-60.

[14] See Digital Markets Act, Article 5(a).

[15] As the Commission has repeatedly explained, eg, in 'Review of the Privacy Act 1988: ACCC submission in response to the Issues Paper' (December 2020) 3, 35-36.

the purposes of machine learning.[16] Meanwhile large incumbents' market power is entrenched through their privileged access to immense and comprehensive datasets, where the scale and scope of these are attributable the collection, use and disclosure of personal data well beyond the reasonable expectations of the relevant consumers.

At a minimum, designated digital platforms should be required to take steps to demonstrate to consumers and other stakeholders how they comply with significant Australian Privacy Principles that limit the collection, use and disclosure of personal information. The platform could be required to state, for example, in a prominent, visible position in the privacy policy:

- Whether the platform collects any information about the individual from a third party where that information could have been obtained from the individual directly, and, if so, the nature of that information, and the specific reasons why the platform believes it is nonetheless impracticable or unreasonable to collect that information from the individual directly;[17]
- How the platform otherwise collects information about the individual and her activities beyond information provided by the individual on the platform's own website or app, subject to obtaining the individual's express, opt-in consent;[18]
- The specific primary or secondary purpose for which the platform's related bodies corporate will use information about the individual which the platform discloses to them, and a link to a website or webpage which clearly lists the names of all the current related bodies corporate with whom the platform may share that information.[19]

Mandating such specific, prominent disclosures would provide consumers with clear information about common practices of concern that currently remain invisible and unknown. It would also provide a basis for the ACCC and the Office of the Australian Information Commissioner (OAIC)to consider possible contraventions of the ACL or the APPs respectively; and whether more substantive rules are necessary having regard to the extent of combination of data across disparate businesses.

Further, the relevant platforms should be required to comply with a consumer's reasonable request to stop using and disclosing their personal data. A minimum set of consent obligations should be consistent with the Consumer Data Right regime.

[16] See Nur Ahmed and Muntasir Wahedx, 'The De-democratization of AI: Deep Learning and the Compute Divide in Artificial Intelligence Research' (22 October 2020) https://arxiv.org/pdf/2010.15581.pdf

[17] Collection from third parties is only lawful on the basis that it would be unreasonable or impracticable to collect the information from the individual herself: APP 3.6. Collection from the individual might be unreasonable or impracticable where, eg, the information relates to the individual's credit score or potential misconduct, but not, eg, when it relates to the consumer's demographic information, family connections, or interests.

[18] This would require information that is clear and understandable for consumers, rather than current broad, opaque statements, such as the following from the Google Privacy Policy: 'We use various technologies to collect and store information, including cookies, pixel tags, local storage, such as browser web storage or application data caches, databases, and server logs.'

[19] See *Privacy Act*, s 13B; APP 6, regarding permitted sharing by related bodies corporate.

4 Increased access to data for rivals or potential rivals

The Discussion Paper raises the possibility of addressing barriers to entry and/or expansion in the supply of some digital platform services by mandating data portability or access to certain data held by large digital platforms.[20] It refers to several examples of such measures from other jurisdictions, including the EU, the United Kingdom and Japan.[21]

The Commission states that 'any sharing and use of personal data should be accompanied by robust consumer-level controls that limit the privacy risks of data sharing and use'.[22] Further, the Commission considers that if 'consumer controls are inadequate or absent, data portability and interoperability initiative should be limited to the sharing of non-personal or aggregated data'.[23]

We have several concerns with this approach.

First, as acknowledged earlier in this submission, a substantial part of the data held by large digital platforms has likely been obtained without express or informed consumer consent and well beyond consumers' reasonable expectations. Mandating disclosure of this data to further entities for proliferating purposes could well work against the objectives of privacy and consumer protection regulation, even if it allowed a dominant firm's rivals to obtain an advantage in competing against the incumbent. Our chief concern should be that personal data is used and limited – and in some cases, deleted – for the benefit of consumers.

Second, the other jurisdictions mentioned above have significantly stronger privacy and/or data protection regulations than those currently in place in Australia. These regulations are also much more actively enforced in the respective jurisdictions relative to enforcement in Australia. Consider, for example, that the Office of the Australian Information Commissioner (OAIC) has brought only one case alleging serious or repeated interference with privacy before the Federal Court of Australia in the 9 years in which the OAIC has had the power to do this. This is not because Australia is uniquely immune to serious interferences with individuals' privacy. Rather, the OAIC has been a much less active regulator, overseeing weaker privacy regulation and widely regarded as under-resourced, particularly in light of the growing demands on a privacy regulator in the digital era. It is not yet clear whether or how the *Privacy Act* will be substantially amended in light of the Privacy Act Review. Any proposal that significantly increases the exposure of personal data should be considered after the outcomes of these reforms are certain.

Third, the Discussion Paper notes the possibility of mandating access to non-personal or aggregated data if consumer controls are inadequate. This could assist in offsetting the entrenched market power of a dominant incumbent in data-intensive markets. However, it would be necessary to define non-personal information with a great deal of care and set stringent standards for de-identification, bearing in mind the need for clarification of the existing definition of

[20] Discussion Paper, pp 79, 92.

[21] Discussion Paper, p 91.

[22] Discussion Paper, p 92.

[23] Discussion Paper, p 92.

'personal information' under the *Privacy Act*, and the ever-increasing ease with which de-identified data can be re-identified.

Fourth, to the extent that proposals to increase access to personal data are limited to requiring data portability at the instigation of the individual consumer (as opposed to any mandated access),[24] in our view, this should only be implemented where the Privacy Safeguards incorporated in the Consumer Data Right regime are in place.

Measures such as these would work towards ensuring that, where a balance must be found between the interests of privacy and consumer protection, and efficient and profitable uses of data by suppliers, the responsibility for that balance should not rest on the shoulders of individual consumers lacking in information, representation, resources and choices.

[24] An alternative approach is an access regime that allows rivals to access data based on consumer consent: Christopher Marsden and Rob Nicholls, 'Interoperability: A Solution to Regulating AI and Social Media Platforms' [2019] (October) *Computers and the Law*. However, the first and second concerns above remain in respect of such an approach.