
# Submission on the Digital Platforms Inquiry:

# Preliminary Report

Dr Katharine Kemp and Dr Rob Nicholls

1 March 2019

A joint initiative of

Allens › ‹ Linklaters

UNSW SYDNEY

The Allens Hub for Technology, Law and Innovation is a community of scholars at UNSW Sydney aiming to add breadth and depth to research on the interactions among law, legal practice and technological change in order to enrich scholarly and policy debates and enhance understanding and engagement among the legal profession, the judiciary, industry, government, civil society and the broader community.

This submission is made by **Dr Katharine Kemp**, Lecturer, Faculty of Law, UNSW Sydney, and **Dr Rob Nicholls**, Senior Lecturer, UNSW School of Business and Taxation, who lead the "Data as a Source of Market Power" Research Stream for the Allens Hub, in response to the Preliminary Report (Report) of the Australian Competition and Consumer Commission (ACCC) on the Digital Platforms Inquiry. We begin by making some comments on the preliminary findings made by ACCC in the Report, particularly with respect to the competition issues raised by concealed data practices and the degradation of consumer data privacy, before responding to the individual preliminary recommendations.

The views in this submission are our own, based on our research, and do not represent the official views of UNSW Sydney or Allens.

## Consumer data privacy

The ACCC has identified evidence of market and regulatory failures that prevent Australian consumers from making informed choices about the extent to which digital platforms collect and use their personal data, which may also hinder the entry of competitors with alternative business models (Report, p 224). Research reveals that consumers generally have a poor understanding of the way their personal data is actually collected, used and disclosed by digital platforms.[1] This is unsurprising, considering the lack of transparency about platforms' practices in respect of consumer data and the negligible ability of consumers to bargain for better privacy terms.

## "Concealed data practices"

Digital platforms often engage in what might be called 'concealed data practices' – a combination of overbroad use of consumer data and lack of transparency and choice for consumers. Concealed data practices may be said to occur where a platform:

- collects a broad range of consumers' personal data (including, for example, data about their activities on third party websites and location tracking information) and uses that data for a wide range of purposes (including, for example, compiling individual profiles on consumers and using those profiles for commercial gain);
- collects, uses and/or discloses consumers' personal data well beyond that which is strictly necessary to provide the consumer with the service in question;
- adopts privacy policies that are too lengthy, broadly worded and/or confusing for the average consumer to read, understand and compare with other services;[2]
- headlines privacy policies with plainly expressed, comforting statements about the value placed on consumer privacy and leaves concerning data terms until much later in the 'fine print';
- explains the issues that most concern consumers (for example, disclosure of their information to others, use for marketing purposes and transfers overseas) in vague terms, and does not identify precise uses or relevant third parties; and
- does not provide consumers with clear, actionable, unbundled choices about the extent to which their personal data is collected and used beyond what is necessary to provide the service in question.

[1] See, eg, Phuong Nguyen and Lauren Solomon, Consumer Policy Research Centre, 'Consumer Data and the Digital Economy: Summary Report: Emerging Issues in Data Collection, Use and Sharing' (Report, 2018); Jessica Rich, 'BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection' (Federal Trade Commission, 23 March 2015); Policy and Research Group, Office of the Privacy Commissioner of Canada, *Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent Under the Personal Information Protection and Electronic Documents Act* (2016); Maurice E Stucke and Allen P Grunes, 'Debunking the Myths Over Big Data and Antitrust' (May 2015) *CPI Antitrust Chronicle* 6.

[2] See A M McDonald and L F Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 *Journal of Law and Policy for the Information Society* 540.

As a result of these practices, many privacy notices seem designed to give the platform a broad licence to use consumer data, without enlightening or empowering the consumer.[3] The actual extent of use and disclosure of consumer data is often discovered through scandals in the media, rather than ex ante communication by the platform.

## Competition issues raised by concealed data practices

Concealed data practices clearly raise consumer protection concerns, but they also raise competition issues. First, concealed data practices hinder competition on the quality of privacy by obscuring the privacy quality offered by the platform relative to its competitors. Second, concealed data practices may preserve substantial market power by means other than superior performance or efficiency, including by the hindrance of competition on privacy and the accumulation and use of personal information to the detriment of consumers.

## Concealed data practices undermine competition on privacy

The first of these competition issues is relatively easily explained. Surveys reveal that consumers are increasingly concerned about their online privacy and desire options in how their personal information is treated. At the same time, rivals who attempt to compete on privacy quality have had relatively limited success. Competition on privacy quality is impeded when digital platforms make it difficult for consumers to know, let alone compare, how their personal data is collected, used and disclosed by the incumbent.

Even in markets where no player has substantial market power, competition is harmed by concealed data practices as a form of market failure. The concealed data practices prevent consumers from choosing services based on information about the privacy quality of those services. At the same time, the two-sided nature of platform markets creates incentives for platforms to further degrade consumer privacy quality to attract more advertising revenue on the other side of the platform.

Some have attempted to argue that there is a 'privacy paradox' – that the revealed preference of most consumers is in fact a *lack* of concern for privacy.[4] But the claim that consumers have a revealed preference for less privacy cannot be supported where privacy terms are offered on a take it or leave it basis, privacy practices are obscured or concealed, and consent to use data for the provision of the service is bundled with consents for data uses which are unnecessary for the provision of that service. The observed consumer behaviour is not evidence of a privacy paradox but the fact that consumers cannot make an informed choice due to the concealed data practices.

## Concealed data practices preserve existing market power

The second competition issue is that concealed data practices may preserve substantial market power. Competition laws do not generally prohibit the possession of substantial market power alone, but only anticompetitive conduct by firms that possess market power. Modern competition laws do not tend to prohibit the mere possession of substantial market power since this power may be acquired through superior efficiency to the advantage of consumers, and rivals may overtake an underperforming monopolist: the market will self-correct and create offsetting benefits for consumers.

This does not mean that substantial market power alone can do no harm. On the contrary, such power can permit a firm to raise price above the competitive level (or reduce quality below the competitive level) to the detriment of consumers. Antitrust regulators and policy-makers should be concerned when rivalry in the market is suppressed and substantial market power is maintained or extended other than by superior efficiency.[5] In these cases, substantial market power causes detriment to consumers without the offsetting benefits.

---

[3] Chris Jay Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 *UCLA Law Review* 606, 625.

[4] See Patricia A Norberg, Daniel R Horne & David A Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors ', (2007) 41 *Journal of Consumer Affairs* 7, 100; Bettina Berendt, Oliver Gunther & Sarah Spiekermann, 'Privacy in Ecommerce: Stated Preferences vs Actual Behavior' (2005) 48 *Communications of the ACM* 101.

[5] These matters are explained in more detail at Katharine Kemp, *Misuse of Market Power: Rationale and Reform* (Cambridge University Press, 2018) 55-60.

Substantial market power is preserved in digital platform markets with the aid of concealed data practices and the hindrance of competition on privacy. That is, when a dominant platform obtains users' personal data through concealed data practices, the extent of consumer data available is far greater for the dominant platform than its smaller rivals, due to the number of users it serves and direct network effects on the user side of the platform.

The dominant platform can then use users' personal data to attract advertisers keen to benefit from superior consumer profiling and consumer targeting permitted by the vast collection of consumer data. In this way, there are also indirect network effects at work to the benefit of the platform: the large number of users on one side of the platform makes the platform more attractive to advertisers on the other side. Advertising revenue is used to fund increased functionality on the user side of the platform, attracting more users, which enhances both direct and indirect network effects, and permitting the platform to benefit from further concealed data practices. This cycle continues.

The dynamics at work in these markets are quite different to those present in markets for products that were traditionally funded by advertising, such as newspapers or broadcast television. In those markets, consumers were aware of, and actively provided, the limited personal information (for example, subscription information) which the supplier obtained. By contrast, in digital platform markets, consumers are subjected to pervasive, ongoing and invisible behavioural monitoring in numerous contexts, with little awareness of the extent or consequences of that monitoring.[6]

It might be argued that, in digital platform markets, increased functionality on the user side, and increased value to advertisers from superior consumer profiling and targeting, mean that substantial market power is actually maintained by providing each of these two types of consumers (users and advertisers) with a better product. However, those benefits must be weighed against the objective detriment caused to users by concealed data practices.

## Objective detriment to consumers from concealed data practices

Consumers suffer from decreased choice, decreased privacy quality and increased privacy costs when concealed data practices hinder competition on privacy.

Further, while it is sometimes argued that the privacy quality of a service is simply a matter of subjective preference, degraded privacy can cause objective detriment to consumers. When a consumer's personal data is collected, stored, used and disclosed to a greater extent, the consumer's privacy is reduced, leading to the following detriments:

- The 'attack surface' of personal data is increased, creating increased risk that the consumer's personal data will be hacked for criminal purposes or otherwise improperly accessed or disclosed. In this way, the risk of serious personal and financial harm including through identity fraud and identity theft increases;
- The consumer's exposure to potential disadvantage from unwanted consumer profiling, targeting and manipulation-based marketing is increased;[7] and
- There is an increased risk that the consumer's data will be combined with other data sets to re-identify anonymised sensitive data about the consumer, discriminate against the consumer, or otherwise use the data against the consumer's interests.

This is not to suggest that data collection is, on balance, generally harmful. We should take into account potential benefits from data collection and use. However, we should also take into account the potential detriments. It is, in fact, possible for "free" services to do more harm than good, if the increased detriment from degraded privacy is greater than the likely utility of the service provided.

## What does this mean for competition enforcement in digital platform markets?

It is important that antitrust regulators identify the existence and competitive effects of concealed data practices in a market, as well as the incentives to degrade consumer data privacy and objective detriments to consumers that result.

---

[6] See, eg, Federal Trade Commission, United States, 'Data Brokers: A Call for Transparency and Accountability' (Report, May 2014); Chris Jay Hoofnagle and Jan Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price' (2014) 61 *UCLA Law Review* 606, 633.

[7] See, eg, European Data Protection Supervisor, 'EDPS Opinion on Online Manipulation ad Personal Data' (Opinion 3/2018, 19 March 2018) 8-9; Ryan Calo, 'Digital Market Manipulation' (2014) 82 *George Washington Law Review* 995.

In practical terms, the presence of these factors in digital platform markets weighs in favour of measures which include:

- increased scrutiny of mergers and proposed mergers, including an explicit focus on existing data practices of the merging parties and the likely data effects of the transaction;
- consumer protection reform and enforcement which addresses imbalances in bargaining power and information asymmetries in respect of privacy terms offered by platforms; and
- increased scrutiny of conduct on the part of firms with market power where the firm's data practices are likely to be detrimental to consumer interests and potentially aid in the preservation of the firm's market power or the extension of that power into neighbouring markets.

We now make brief responses to some individual preliminary recommendations.

## Responses to preliminary recommendations

**Recommendation 1 – Data effects in merger analysis**

We do not believe this proposal amounts to a substantive change in the merger assessment law, which is already likely to permit consideration of data acquired and the acquisition of a potential competitor to the extent that they affect competition in the relevant market. However, it would provide predictability to merger parties if the importance of analysing data effects in the digital platform environment were to be included in the Merger Guidelines, including for the reasons outlined above.

**Recommendation 2 – Pre-notification of acquisitions**

We agree that dominant digital platforms have incentives to impede vigorous competition by acquiring significant rivals before their competitive significance becomes more broadly apparent. Requiring classes of businesses to provide advance notice of acquisitions may be reasonable within a certain regulatory framework. However, in our view, this is not appropriate while the merger test is that of 'substantial lessening of competition'. If the test were to be amended, either by reversal of the onus of proof or changing to a 'material lessening of competition' test, the notice in advance would be more reasonable.[8]

**Recommendation 3 – Choice of browser and search engine**

We support this recommendation. While it might be argued that Google and other search providers compete for the right to be the default general search engine for a particular browser by making competitive bids, rivals (and particularly new rivals) would be at a severe disadvantage in any attempt to match the bids of a company which enjoys a market share of around 90 percent in general search.

Under preliminary recommendation 3, it is still open to consumers to select the dominant search engine and the related browser. Given Google's arguments in favour of the superiority of its product, ensuring consumers have a choice of product is unlikely to impede Google's attempts to compete on the merits. The majority of consumers would then be likely to select Google as their search engine. However, the proposal could be very significant in permitting potential competitive challenges to Google's dominance, including by making the choice of search engine transparent and accessible for consumers.

**Recommendation 6 – Reform of media regulation**

We support this recommendation. In the interests of effective competition in the relevant media markets, there should be a level playing field in respect of the regulation of media, with regulation based on functions performed, rather than the nature or identity of the entity.

**Recommendation 8 – Privacy Act amendments**

At the outset, we note the ACCC's preliminary finding that there is significant confusion, uncertainty, and potentially obfuscation, about the meaning of the 'personal information' referred to in the privacy policies of digital platforms, which give a variety of meanings to this term (Report, pp 185-187).

[8] Consistent with the comments of Rod Sims in his annual CEDA address in 2019 at <https://www.accc.gov.au/speech/2019-compliance-and-enforcement-policy> accessed 8 March 2019.

We have had the benefit of reviewing the submissions of the Australian Privacy Foundation (APF) in response to the Report, particularly on the preliminary recommendations concerning the *Privacy Act* amendments. We support the submission by the APF that the definition of 'personal information' under the *Privacy Act* requires amendment to clarify that it includes an IP address, a URL or other information which can be used to identify an individual. These types of information are regularly used by digital platforms to identify other information which is 'about an individual'. Expanding the definition of 'personal information' under the *Privacy Act* in this way is also in line with the definition of 'personal data' under the GDPR, which expressly includes online identifiers and location data. It is essential that Australia has a clear definition of 'personal information' which takes account of the realities of the digital age.

***Recommendation 8(a) – Notification***

It is important to bear in mind that notifications of the collection of consumers' personal information are intended to provide clear, actionable information. Notifications of the collection of personal information should not be treated by digital platforms as a marketing opportunity. On the contrary, they should highlight, and lead with, the information that is most likely to concern consumers.

We support the submission of the APF that recommendation 8(a) should specify that the relevant notification accompanying collection of personal information should include 'the identity and contact details of the entity collecting data; the types of data collected and the purposes for which each type of data is collected; and whether the data will be disclosed to any third parties and, if so, which third parties and for what purposes'.

Some may consider that providing notification with this amount of specificity has the potential to 'overload' consumers with information and defeat the purpose of informing the consumer. However, by managing the notification interface, it is possible to provide consumers with brief and concise notification which nonetheless permits more concerned users to receive further information. For example, the notification could list the types of third parties to whom the consumer's information is disclosed and provide a hyperlink to a more detailed list of the actual third parties to whom the information is disclosed.

Providing the option of this further detail is particularly important in permitting expert intermediaries – such as consumer advocates and privacy advocates – to obtain sufficient information to inform less-expert consumers of the effect of the data practices in question.

***Recommendation 8(b) – Certification***

We have some reservations about a certification scheme to encourage compliance and consumer trust, given the relatively poor record of some certification schemes or privacy 'seals' in other jurisdictions. However, it is encouraging that the ACCC's proposal is for a *mandatory* certification scheme for some firms (that is, the participants will not be self-selecting customers of the certifier) and that compliance will be measured against the *Privacy Act* (which sets a higher standard than some other certification schemes).

***Recommendation 8(c) – Consent***

We support the recommendation to amend the definition of consent under the *Privacy Act* 'to require express, opt-in consent and incorporate requirements into the Australian Privacy Principles [APPs] that consent must be adequately informed (including about the consequences of providing consent), voluntarily given, current and specific …' The onus should be on the firm to prove that these higher standards of consent have been met.

It is also critical that the mechanism by which consumers provide their consent permits consumers to give 'unbundled' consent. That is, consumers should have the option of agreeing to the collection and use of their personal information for some purposes while refusing to consent to collection and use of their information for other purposes. Consent should not be an 'all or nothing' proposition, which allows firms to impose unnecessary and unwanted data uses on consumers as a condition of using the core service provided by the firm. Consumers are prevented from making informed choices in these circumstances, particularly where the firm engages in concealed data practices and/or where consumers have little real choice about whether to use the platform.

It should also be noted that the current wording of the APPs permits firms to interpret the meaning of collection necessity (APP 3.1-3.2) and use or disclosure for related, secondary purposes (APP 6.2(a)) to their own advantage, potentially taking a broad view of what collection is 'necessary' for its primary purpose or when a secondary purpose can be said to be 'related' to the primary purpose for which the data was collected. We support the submission of the APF that the wording of these APPs should be reviewed and tightened.

***Recommendation 8(d) – Erasure***

We support the recommendation that consumers should be enabled 'to require erasure of their personal information where they have withdrawn their consent and the personal information is no longer necessary to provide the consumer with a service'. We submit that

careful attention to the wording of this requirement will be required to ensure that firms do not retain information on the basis of spurious claims that they continue to provide the consumer with a 'service'.

Some may argue that consumers should not be allowed to prevent firms from continuing to use consumers' personal information where permission to use that personal information might be seen as the consideration provided by the consumer for a zero-priced service. However, it is not at all clear that consumers expect that their use of a particular online service will entitle the supplier to store and use the consumer's personal information for an indefinite period. Further, where the law has imposed restrictions on bargains with consumers in the interests of consumer protection (for example, by imposing consumer guarantees), suppliers have been able to adapt their business models to these fairer standards.

***Recommendation 8(e) – Increased penalties***

We support the recommendation that penalties for breaches of the *Privacy Act* should be increased to at least mirror the increased penalties for breaches of the Australian Consumer Law. The consequences of a firm's breach of the *Privacy Act* can be significantly more severe than the consequences of a breach of the Australian Consumer Law, given the ongoing risk and harm imposed on the individuals concerned once their personal information is wrongly used or exposed.

***Recommendation 8(f) – Individual right of action***

We support the recommendation that individuals should be given a direct right to bring actions for breach of their privacy under the *Privacy Act*. As under the Australian Consumer Law, individuals should have the option of litigating a breach of the *Privacy Act* directly, rather than depending on the decision-making processes of the OAIC.

This would give individuals greater agency in respect of the treatment of their personal information and potentially reduce the enforcement costs of the OAIC. More importantly, it would provide Australian courts with increased opportunities to interpret the *Privacy Act*, providing greater clarity and certainty for all those affected by its provisions.

***Recommendation 8(g) – OAIC resourcing***

We support this recommendation.

**Recommendation 9 – OAIC Code of Practice**

We support the recommendation that 'the OAIC engage with key digital platforms operating in Australia to develop an enforceable code of practice under Part IIIB of the Privacy Act' and that '[t]he ACCC should also be involved I the process for developing this code in its role as the competition and consumer regulator'.

The development of such a code would provide an opportunity for the regulators to propose boundaries on digital platforms' data practices which would limit the incidence of 'concealed data practices' and address the incentives to degrade consumer data privacy created by the particular dynamics of multi-sided digital platform markets (as described at the beginning of this submission).

**Recommendation 10 – Statutory action for serious invasion of privacy**

We support this recommendation as a long overdue reform in Australian privacy law, which would bring our law closer to the privacy laws of other major jurisdictions and provide a statutory cause of action which has been thoroughly considered, and justified, by the Australian Law Reform Commission.

**Recommendation 11 – Unfair Contract Terms Law**

We do not oppose the recommendation that 'unfair contract terms should be illegal (not just voidable) under the ACL, and that civil pecuniary penalties should apply to their use, to more effectively deter digital platforms from leveraging their bargaining power over consumers by using unfair contract terms in their terms of use or privacy policies'.

We have some reservations about the impact this reform might have in terms of the compliance burden imposed on the many firms, large and small, which use standard form contracts that fall under the Unfair Contract Terms Law in Part 2-3 of the Australian Consumer Law (UCTL). However, we recognise that the extent of the protection currently provided to consumers under the UCTL is doubtful in a large number of cases, particularly in the context of privacy terms.

At present, section 23(1) of the ACL makes unfair contract terms void if they are contained in a standard form consumer or small business contract. The consequence that an unfair term is void may assist consumers where the term in question imposes some

obligation on the consumer, that is, when it requires the consumer to *do* something. In such cases, the fact that the term is void means that the consumer has grounds for declining to fulfil that obligation.

However, the consequence that the unfair term is void may be less useful when that term provides a firm with *permission to do something*: in the case of privacy terms, the term may permit overbroad collection or use of the consumer's personal information secured under the original privacy terms, or under terms which have been unilaterally varied by the firm. In this case, the consumer would most likely need to bring proceedings to obtain a declaration that the term is unfair and seek an injunction to restrain the firm from relying on that term in future. More importantly, there is no realistic prospect of reversing the actions of the firm in unfairly collecting, using and disclosing the consumer's information up to that point. In these circumstances, the current remedies are likely to provide negligible recourse for a consumer affected by unfair privacy terms. We support the need for legislative reform to provide consumers with real recourse and to improve deterrence of unfair privacy terms.

**Dr Katharine Kemp and Dr Rob Nicholls**

**1 March 2019**