



**CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE**

CSCRC SUBMISSION:

Response to the ACCC's Digital Platform Services Inquiry, *Discussion Paper for Interim Report No.5: Updating competition and consumer law digital platform services*

Dear Sir/Madam,

Submission – Response to the ACCC's Digital Platform Services Inquiry, *Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services*

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Australian Competition and Consumer Commission's (ACCC) Digital Platform Services Inquiry, *Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services* (the Discussion Paper).

While digital platform services play a vital role in supporting Australian businesses and consumers, some platforms have monopolised certain markets. This has made it difficult for new competitors to enter the market and has reduced the variety of providers available to consumers, which in turn perpetuates an environment of reduced competition. Furthermore, in order to use these services, which are now necessary for many business and lifestyle functions, consumers must abide by often complex and confusing privacy policies and terms of service. This has direct impacts on the security of their data and how it is used.

Therefore, the ACCC's review of competition and consumer law as it applies to digital platform services is both timely and necessary. It is not in the interests of Australian businesses and consumers to operate in an online environment where a small number of 'gatekeeper' platforms are able to dominate the market with unfair advantage. Furthermore, cyber security has a key role to play, especially as it comes to the protection and use of personal data, how this data is used, and the proliferation of harms that are unintentionally facilitated by powerful digital platforms, like scams and fraudulent activity.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem.

We look forward to answering any queries about this submission and welcome the opportunity to participate in any future consultation regarding this very important topic.

Yours Sincerely,



Rachael Falk
CEO, Cyber Security Cooperative Research Centre
ceo@cybersecuritycrc.org.au

Question 1

What competition and consumer harms, as well as key benefits, arise from digital platform services in Australia?

Digital platform services have changed the way Australians live and do business for the good. They underpin the digital economy, heighten the effectiveness and efficiency of organisations, and are essential for the automated and ubiquitous delivery of services Australian organisations and consumers rely upon. Likewise, digital platform services play a key role in connecting Australians via social media, which in this respect plays a significant social good.

However, as highlighted in the Discussion Paper, digital platform services in Australia also present significant competition and consumer harms, which must be addressed. The Discussion Paper provides in-depth and wide-ranging analysis of these harms, which the CSCRC wholly agrees with.¹ Taking a cyber security lens, the CSCRC would like to highlight the excessive use of online tracking, the use of dark patterns, complex and confusing privacy policies and terms of service, and the proliferation of online scams and harmful apps as particularly important harms to consider.²

Excessive use of online tracking directly impacts on the privacy and data security of consumers and, as noted in the Discussion Paper, increases the risk of data breaches, identity fraud and targeting by scammers.³ The *Australian Community Attitudes to Privacy Survey 2020*, found Australians want to be protected against harmful online practices, with 84 per cent stating that personal information should not be used in ways that cause harm, loss or distress.⁴ The survey also found Australians were generally uncomfortable with the data practices of digital platform services.⁵

The use of dark patterns exploits cognitive biases, prompting consumers to purchase goods and services that they do not want or to reveal personal information they would usually not disclose.⁶ The CSCRC is particularly concerned by the use of dark patterns that exploits the behaviour of consumers as it comes to the selection of privacy controls and settings, manipulating them to select more intrusive options.

The length, complexity and ambiguity of online privacy policies are challenging for consumers and can result in data harms. As a result, and as noted in the Discussion Paper and in the *ACCC's Digital Platforms Inquiry – Final Report*, consumers are generally unaware

¹ [DPSI September 2022 Report - Discussion Paper \(acc.gov.au\)](#), PP 37-56

² *Ibid* 1, PP 43-49

³ *Ibid* 1, P44

⁴ [Australian Community Attitudes to Privacy Survey 2020 \(oaic.gov.au\)](#), P5

⁵ *Ibid* 4, P7

⁶ [Shining a light on dark patterns \(silverchair.com\)](#) P43

of how much of their data is collected, and how it is collected, used and shared by digital platforms.⁷

And finally, as noted in the Discussion Paper, the expansion of digital platforms has fuelled an explosion of online scams and harmful apps.⁸ These scams continue to grow in sophistication and scale and have resulted in significant financial losses for Australians and the disclosure of personal identifying information. The CSCRC submits there is an onus on gatekeeper digital platforms to more effectively police scams on their platforms, as well as introduction of redress options for those impacted.

Question 2

Do you consider that the CCA and ACL are sufficient to address competition and consumer harms arising from digital platform services in Australia, or do you consider regulatory reform is required?

While the CCA and ACL continue to play a vital role in addressing competition and consumer harms arising from digital platform services in Australia, enhancements are required to ensure they remain fit-for-purpose in the rapidly and continuously evolving digital platform environment. Therefore, the CSCRC supports the ACCC's assertion that new rules to specifically address consumer harms caused by digital platforms may be required.⁹ In relation to CCA, this could include new sector-specific rules for digital platforms where general consumer law is deemed inadequate, and in relation to ACL, this could include prohibitions on certain types of conduct not currently captured by existing laws.

Question 3

Should law reform be staged to address specific harms sequentially as they are identified and assessed, or should a broader framework be adopted to address multiple potential harms across different digital platform services?

While there are advantages and disadvantages to both staged and more broad approaches to law reform, the CSCRC submits that a 'middle ground' approach may be most beneficial. That is, the most significant and urgent harms be identified and addressed together in a staged way, with those deemed 'less' urgent addressed in further stages. Such an approach would strike an appropriate balance between introducing tailored approaches to address specific harms, as well as addressing broader systemic issues in a more measured manner.

The CSCRC supports the ACCC's suggestion that a tiered approach to reform could be taken, reflecting different business models or service offerings of digital platforms, with thresholds

⁷ [Digital platforms inquiry - final report.pdf \(acc.gov.au\)](#), P23

⁸ Ibid 1, P47

⁹ Ibid 1, P62

or sub-categories governing the applicability of such legislative provisions.¹⁰ A vital element of reforming consumer law as it applies to digital platform services is that of dynamism. That is, reforms must be adequately flexible stand the test of time in a rapidly evolving space.

Question 5

To what extent should a new framework in Australia align with those in overseas jurisdictions to promote regulatory alignment for global digital platforms and their users (both business users and consumers)? What are the key elements that should be aligned?

Given the transnational and borderless nature of the internet and the digital platforms that operate upon it, it is important that a new Australian framework is aligned and interoperable with those other jurisdictions. This will not only support international consistency as it comes to global governance of digital platforms but will also help reduce the regulatory burden on digital platforms themselves.

Regulatory burden and duplication are often cited by digital platforms in opposition to legislative change, due to added layers of cost and increased compliance requirements. By harmonising international regimes to the greatest extent possible, the ability of digital platforms to comply across jurisdictions would ultimately be enhanced and the burden of increased cost reduced.

Question 9

9. Data limitation measures would limit data use in the supply of digital platform services in Australia:

- a) What are the benefits and risks of introducing such measures?**
- b) Which digital platform services, out of those identified in question 6, would benefit (in terms of increased competition or reduced consumer harm) from the introduction of data limitation measures and in what circumstances?**
- c) Which types of data should be subject to a data limitation measure?**

Data limitation measures would separate data across the breadth of a digital platform's entire business, ringfencing different units. This would help stop the use of data from one part of a business being used to create an unfair market advantage in another. As noted in the discussion paper, such a measure may be deemed appropriate for 'gatekeeper' digital platform services, like Apple and Google, which are able to use their vast repositories of data across different parts of the business for gains across the whole business.¹¹ While data limitation measures may decrease the efficiency of operations, there may be a broader

¹⁰ Ibid 1, P74

¹¹ Ibid 1, P93

benefit in creating a fairer marketplace, in which new digital platforms could compete with gatekeepers.

The CSCRC contends that where a platform is deemed to be a gatekeeper, be it across any digital service, data limitation measures should be enacted. This is especially important for platforms that have multiple business interests across various services, like Google, Apple and Facebook.

In terms of data limitation measures, controls should be put in place for consumers' personal identifying information, like health, financial and location data. Furthermore, information regarding online searches and purchases should be ringfenced to prevent targeted marketing and the use of dark patterns.

Question 11

What additional measures are necessary or desirable to adequately protect consumers against:

a) the use of dark patterns online

b) scams, harmful content, or malicious and exploitative apps?

The CSCRC supports the ACCC's recommendation that the ACL be amended to prohibit certain unfair trading practices, which could deter the use of dark patterns through the potential application of ACCC enforcement action.¹² In relation to deterring the use of dark patterns, the CSCRC also supports the application of regulatory measures that would improve consumer autonomy, such as the introduction of specific design requirements for large digital platforms that do not take advantage of consumers' behavioural biases.¹³

In relation to protecting consumers against online scams, harmful apps and fake reviews, the CSCRC is supportive of steps to place further fair-trading obligations on digital platforms. Specifically, the CSCRC supports the ACCC's continued advocacy for an economy-wide prohibition on certain unfair trading practices, as well as preventative measures such as regular sweeps of websites or apps to identify breaches of consumer law.¹⁴

Question 12

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

Consumer protections should apply to all digital services platforms operating in Australia, regardless of their size. However, given the prominent market role gatekeeper services play across various markets, different thresholds could be established in determining penalties.

¹² Ibid 1, P97

¹³ Ibid 1, P97

¹⁴ Ibid 1, P95

For example, thresholds could be set according to annual global turnover or number of domestic users/ subscribers.

As previously stated, the CSCRC also supports the ACCC's suggestion that a tiered approach to reform could be taken, reflecting different business models or service offerings of digital platforms, with thresholds or sub-categories governing the applicability of such legislative provisions.¹⁵

Question 13

Should digital platforms that operate app marketplaces be subject to additional obligations regarding the monitoring of their app marketplaces for malicious or exploitative apps? If so, what types of additional obligations?

The CSCRC is supportive of moves to enact additional measures to protect consumers from harmful apps on some digital platforms. Such obligations could include more effective monitoring, blocking and removal of harmful apps; notification and potential redress for impacted consumers; timely reporting of malicious or harmful apps to the ACCC by captured platforms; and the ACCC's existing recommendation for economy-wide prohibition on particular unfair trading practices.¹⁶

Question 16

In what circumstances, and for which digital platform services or businesses, is there a case for increased transparency including in respect of price, the operation of key algorithms or policies, and key terms of service?

There is an urgent need for increased transparency by digital platform service providers. As noted in a recent Lawfare article, "transparency reporting by the wider tech sector has been mostly voluntary. Companies such as Apple, Facebook and Twitter have been left to determine how and when they undertake transparency reports, leading to ad hoc and unstandardized disclosures".¹⁷ From a cyber security perspective, the most important areas where greater transparency is required are the operation of algorithms, privacy policies and terms of service.

There is a case for independent regulatory oversight of algorithms used by digital platforms to help protect consumers against practices like the use of dark patterns and targeted advertising. The Brookings Institute has highlighted that access to algorithms is an essential factor to improved transparency, with a recent article suggesting that "vetted researchers and regulators should have access to enough information about the algorithms used in

¹⁵ Ibid 1, P74

¹⁶ Ibid 1, P95

¹⁷ [Time for Transparency From Digital Platforms, But What Does That Really Mean? - Lawfare \(lawfareblog.com\)](https://www.lawfareblog.com/time-for-transparency-from-digital-platforms-but-what-does-that-really-mean/)

content moderation, prioritization, advertising, and recommendation, and enough data about how these algorithms affect platform content to allow an independent assessment".¹⁸ From a competition perspective, the vetting of algorithms would also help level the playing field. As is stands, gatekeeper platforms have a significant data advantage, with data collection and profiling practices vital to revenue generation. This data is used to train algorithms which in turn may increase revenue, deterring platforms from implementing stronger user privacy controls.¹⁹

As previously mentioned, the length, complexity and ambiguity of online privacy policies and are challenging for consumers. As a result, and as noted in the Discussion Paper and in the ACCC's Digital Platforms Inquiry – Final Report, consumers are generally unaware of how much of their data is collected, and how it is collected, used and shared by digital platforms.²⁰ Furthermore, confusing behavioural biases introduced by digital platforms may make it difficult for consumers to understand terms and conditions and privacy policies.²¹ Key examples include information overload, whereby consumers are provided with too much information to process and opt in to potentially intrusive conditions and privacy policies, and the default effect, whereby one choice is presented as a default option, which could encourage consumers to choose that option.²²

There is a fundamental bargaining power imbalance between media businesses and Google and Facebook that results in media businesses accepting terms of service that are less favourable.²³

¹⁸ [How online platform transparency can improve content moderation and algorithmic performance \(brookings.edu\)](https://www.brookings.edu/research/how-online-platform-transparency-can-improve-content-moderation-and-algorithmic-performance/)

¹⁹ [Regulating Platform Algorithms: Approaches for EU and U.S. Policymakers \(newamerica.org\)](https://www.newamerica.org/technology/policy/regulating-platform-algorithms-approaches-for-eu-and-u-s-policy-makers/)

²⁰ Ibid 7, P23

²¹ Ibid 7, PP 423-424

²² Ibid 7, PP 423-424

²³ Ibid 7, P206