Submission to the Australian Competition and Consumer Commission Digital Platform Services Inquiry

Discussion Paper for Interim Report No. 5

April 2022

Table of Contents

Overview

1. The Department of Home Affairs (the Department) welcomes the opportunity to provide a submission regarding the Australian Competition and Consumer Commission (ACCC) *Digital Platform Services Inquiry Interim Report No.5 Discussion Paper* (the Discussion Paper).

2. The Department is particularly concerned about the law enforcement and national security challenges posed by digital platforms. These include the unprecedented global proliferation of child sexual abuse material, the use of the internet to promote terrorist and violent extremist content, malign interference by foreign actors in Australia's democracy and society, the spread of misinformation and disinformation, and increasing cyber and identity crime.

3. In relation to a range of online harms, the Australian government is at the forefront of global efforts to design regulatory frameworks that keep pace with innovation and meet community expectations for safety, accountability, and transparency.

4. The Department welcomes this Discussion Paper and the ACCC's observations. The characteristics of anti-competitive digital platform markets have important national security and law enforcement implications. Markets where a small number of large digital platforms dominate can result in large-scale data aggregation with inadequate safeguards, limited opportunities for new entrants to satisfy consumer demands for safety and security, private control over increasing segments of public life, and the creation of new channels to influence our democratic debate and institutions.

5. The observations of the ACCC in this Discussion Paper are an important step towards bringing the Australian framework for digital platforms in line with international partners and promoting a "race to the top" among digital platforms to design safe and secure systems for users.

Consumer Harms from Digital Platforms

6. The rapid rise of digital platforms has clearly brought immense positive change to Australian society. However, as these platforms scaled to global audiences the associated consumer harms have also increased in scope and severity.

7. The Department has found that digital platforms do not voluntarily do enough to build safety and security by design into their products and services sold to Australians.[1]

8. A range of online harms are actively facilitated by the technologies employed by digital platforms. This includes the use of algorithms to promote harmful content to increase user engagement, indiscriminate rollout of end-to-end encryption on messaging platforms, and a failure to implement adequate safety by design principles on platforms used by vulnerable groups.

9. The scale of this problem is immense and it is not confined to outlier digital platforms or the dark web. Statistics from the National Center for Missing and Exploited Children (NCMEC) – the United States organisation to which digital industry refer detected child sexual abuse material – show child sexual abuse material reports almost doubling in two years, from 17 million in 2019, to 21.7 million in 2020, then reaching nearly 30 million in 2021.

10. Each instance in which child sexual abuse material is shared, viewed, and accessed is an additional violation of a victim's fundamental rights and privacy. The majority of child sexual abuse material referrals come from the social media platforms which dominate the Australian market. In 2020, 20.3 million of the NCMEC reports were received from Facebook alone.

11. Social media has now also become the most profitable way for online scammers to reach victims. We note the ACCC's finding that this not only places particularly vulnerable groups of consumers, including children, at risk of being targeted by scammers, including via contact methods outside the digital platforms, but also enables the more effective targeting of scams generally. The Department agrees with

[1] Further detail is available from the *Department of Home Affairs Submission to the Parliamentary Inquiry into Social Media and Online Safety* (8 March 2022).

the ACCC's finding that digital platforms do not do enough to remove scams either proactively or in response to complaints.

12. The Department acknowledges the ACCC's observation that consumers are exposed to harm through malicious or exploitative apps distributed through app marketplaces. Some of these apps include embedded security risks, such as malware, which expose the personal information of consumers to criminal actors. The Department welcomes the previous ACCC finding that market leaders, including Apple and Google, should take further measures to prevent and remove apps that harm consumers. The Department further welcomes ongoing engagement with app marketplaces to enhance the transparency of information for consumers at the point of sale, including information related to app security.

13. The Department also notes that criminal tradecraft is continually evolving to exploit mainstream digital platforms for a range of crime types. The impact of COVID-19 has led perpetrators of child abuse to turn to livestreaming of child sexual exploitation and abuse from around the world, often using mainstream social media services. Analysis of payments data shows that Australian individuals engaging in child sexual abuse livestreaming tend to be aged in their 50s or 60s and the majority (55%) and have no criminal record.[2]

14. Scammers who might traditionally have relied on fraudulent sales or telephone scams are increasingly turning to child sexual abuse material as a source of criminal revenue. This disturbing crime involves financially motivated criminals targeting Australian children, due to their relatively high access to funds and use of social media, and impersonating children or peers to solicit self-generated child sexual abuse material. Criminals then use this material to extort children, demanding repeated and increasing payments under threat of sharing the child sexual abuse material with the child's friends and family, who the criminals are able to easily discover using social media services.

15. In 2021, the Australian Centre to Counter Child Exploitation (ACCCE) identified an increase in Member of the Public reports of children self-producing CSAM for financial incentives, with children as young as 10 years old being targeted with incentives such as in-game currency on popular online games. Children coerced to create self-generated sexual imagery may not view themselves as victims and can perceive their actions as voluntary. The Department notes that it is unacceptable for digital platforms to rely on children to self-report child sexual exploitation and abuse online. Digital platforms, particularly those which intentionally cultivate a large user-base of Australian children, must be proactive in ensuring that their services do not enable and promote the exploitation of vulnerable groups.

16. The Department notes that criminals often use social media services such as Instagram and Facebook to discover children and their social network, before requesting that children move to video chat services such as Skype or WhatsApp. This behaviour, known as "off-platforming" poses significant challenges to law enforcement due to limited platform record-keeping, storage of data offshore, limited coordination among digital platforms to address off-platforming, and the use of end-to-end encryption.

17. The proliferation of terrorist and violent extremist content on the internet is also enabled by digital platforms. Digital platforms and their algorithms can create echo chambers that isolate and radicalise individuals, and intensify ideologies due to limiting exposure to alternate viewpoints. This can be used to the advantage of terrorist organisations to recruit or radicalise vulnerable individuals. The rollout of end-to-end encryption without adequate safety mechanisms significantly limits the ability for law enforcement, the public, and digital platforms themselves to identify and intervene against terrorist and extremist content.

Consumer Preferences for Safety and Security from Digital Platforms

18. There is clearly consumer demand from Australians for digital platforms to provide safe and secure online services. 75% of Australians agree that technology companies have a responsibility for people's

[2] Rick Brown, Sarah Napier, and Russell Smith, "Australians who view live streaming of child sexual abuse: An analysis of financial transactions" (19/2/2020) *Trends & issues in crime and criminal justice* 589.

online safety. However, only 23% of Australians feel that industry is doing enough to build safety features into their services and products.[3]

19. Although children are among some of the most vulnerable groups online, there is demand from all age groups for improved safety and security online:

    19.1. 45% of children were treated in a hurtful or nasty way online in the past year and 26% had treated someone in a hurtful or nasty way online.[4]

    19.2. 18% of people from culturally and linguistically diverse (CALD) backgrounds, 30% of LGBTQI+ people, and 32% of Aboriginal and Torres Strait Islander peoples experienced online hate speech – which is double the national average of 14%.[5]

    19.3. Exposure to negative online content and sexual content is prevalent among 14-17-year-olds. 71% had seen sexual images in the past year, while 47% have received sexual messages from someone. Many parents of 14-17-year-olds are not aware that their children have viewed potentially harmful content such as violent images, suicide methods, and unhealthy eating.[6]

    19.4. 76% of Australians believe that platforms should be doing more to reduce the amount of false or misleading information people see online.[7]

20. Transparency around how digital platforms use and store data is currently lacking. Existing settings do not require digital platforms to tell users where there data is stored, and who can access it. Consent to broad terms and conditions is often a prerequisite of access to essential services, leaving users with little practical choice over how their data is captured and analysed.

21. The Department also encourages the ACCC to consider the impact of data scraping on privacy and national security. Advanced analytics and insights can be drawn from scraped datasets and users are often unaware that their personal data over long periods of time can be aggregated, stored, and analysed. The current measures to address data scraping are not commensurate with the risks.

Uncompetitive Markets Compromise on Safety and Security

22. The Department welcomes the findings of the Discussion Paper which would improve market competitiveness and allow digital platforms to compete in a "race to the top" to satisfy consumer demand for safer online services. It is clear that this demand exists and it has only become more evident that the rules which apply to behaviour offline must also apply online.

23. A well-functioning, competitive market would have already met these consumer preferences for online safety and security. In a market dominated by major platforms which often operate as default providers for search, social interaction, messaging, and engagement online, consumers are not empowered to select services that incorporate safety by design.

24. Digital platforms that are insulated from competitive pressures through anticompetitive conduct (such as through self-preferencing, predatory acquisitions, artificial barriers to entry, bargaining imbalances, and insufficient consumer protections) may be incentivised to degrade user safety where doing so maximises profits.

25. A lack of competition can be particularly harmful in the online safety and security context where the market operates on a zero monetary price model. Firms in this form of market are: (a) able to profitably

[3] eSafety Commissioner, "Building Australian adults' confidence and resilience online" (September 2020) 7.
[4] eSafety Commissioner, "Mind the Gap: Parental Awareness of Children's Exposure to Risks Online" (February 2022).
[5] eSafety Commissioner, "Adults' negative online experiences" (August 2020).
[6] eSafety Commissioner, "Mind the Gap: Parental Awareness of Children's Exposure to Risks Online" (February 2022).
[7] Australian Communications and Media Authority, "A report to government on the adequacy of digital platforms' disinformation and news quality measures" (June 2021) p 36.

degrade service quality; and (b) are more likely to become de facto providers of essential services. This is often expressed through digital platform services which enable online harms to be perpetrated against their users, for example via enabling the targeting of scams, allowing criminals to identify vulnerable children and their social circle, or algorithmically amplifying mis/disinformation to increase user engagement and advertisement revenue.

26. Although 85% of digital platform users do not want their personal data to be used or shared beyond the purposes for which a platform requires it,[8] there are few avenues for consumers to express this preference in an uncompetitive market.

27. The Department is also concerned that inadequate consumer protections allow digital platforms which compromise user safety and security to thrive, and in turn to acquire potential competitors who might seek to take a more responsible approach to user protection. Where a dominant firm with a history of disregarding user safety is permitted to acquire smaller competitors which may have focused on a safer user experience, these potential competitors are often consolidated into a single unsafe platform, enabling criminal activity online on a vast scale.

    27.1. For example, the ACCC has previously found that Meta has a significant competitive advantage in the supply of online private messaging services in Australia through Facebook Messenger and WhatsApp. Having consolidated its market position through acquisitions of competitors, Meta now plans to roll out end-to-end encryption by default across its messaging services. NCMEC expects that this product decision could result in the loss of 70% of referrals of child sexual abuse material to law enforcement.

28. In addition to online harms, anticompetitive markets can also exacerbate national security risks. Where monopoly providers are responsible for services to broad sections of the economy, without any of the requirements placed on essential infrastructure providers, there are supply chain risks due to a single point of failure. Diverse and competitive markets for essential services improve the resilience of the digital economy.

Incentivising Market-led Solutions

28. Digital platforms offer immense opportunity for democratic engagement, participation, and expression. However, security risks emerge where online discourse is no longer organic and is instead shaped by non-transparent algorithmic curation of content, foreign interference, and coordinated inauthentic messaging.

29. The ad-supported business model of digital platforms has led to sophisticated data aggregation and micro-targeting techniques which can be repurposed by hostile actors, including governments, to distribute harmful content to specific individuals or segments of the population.

30. The Department supports improved non-price transparency from digital platforms regarding the use of data and the operations of key algorithms for regulators, researchers, and the public. Greater transparency and interoperability in major digital platform services will ensure that the openness of our digital ecosystem becomes an advantage for the resilience of our digital economy.

31. The Department also supports the approach of the ACCC in considering measures to ensure that digital platforms that control large ecosystems of services do not unfairly exclude rivals by limiting interoperability. Approaches which improve interoperability should allow consumers, to the extent practical, to:

    31.1. Migrate to services which offer a preferred standard for safety and security;

    31.2. Promote access for third-party apps to core digital platform functions, device hardware, and operating system features; and

[8] Australian Competition and Consumer Commission, "Consumer Views and Behaviours on Digital Platforms" (November 2018).

31.3. Both export and import interoperable data related to use history, account information, platform reputation (e.g. accrued vendor ranking on marketplace platforms), settings, and associated data to prevent user lock-in.

32. Enabling third-party providers to append specific services to the offering of dominant platforms could improve consumer choice, transparency, and ensure that major portions of Australia's economy and information environment are not governed by the terms of service of a small number of providers. There are a range of "middleware" proposals which the ACCC could consider to improve competition in the market, including for algorithmic curation of content.

Evolving Digital Technologies

33. Australia has been world leading in its proactive regulatory approach to mitigating the risks of online harms. Acting in concert with international partners on issues of shared concern can promote a "race to the top" among digital platforms for user safety and security.

34. The Department agrees that international alignment across jurisdictions will promote consistency and ensure that Australians are able to access globally leading technologies. The Department also notes the importance of reducing the regulatory burden on businesses as a measure to ensure that new market entrants are not deterred by compliance costs which can only be borne by global incumbent platforms.

35. The Department supports the finding by the ACCC that there has been a persistent lack of effective redress for consumers in the face of escalating harmful content online. There is now a global push by civil society, businesses, users, and governments to build stronger foundations for our digital economies. As new technologies and platforms emerge, such as the metaverse, it is essential that the appropriate settings are in place to enable and encourage safe and secure innovation.