Meta response to Australian Government consultation on ACCC's regulatory reform recommendations

FEBRUARY 2023

Meta

Executive summary

Meta welcomes the opportunity to respond to the Australian Government's consultation on the regulatory proposals from the Australian Competition and Consumer Commission's (ACCC's) Digital Platforms Services Inquiry.

We commend the Australian Government for considering how to ensure consumers are protected when interacting with services online. Meta is strongly committed to encouraging safe and positive experiences for Australian consumers. The success of our services depends on our ability to deliver a great experience to Australian people, small businesses and advertisers.

We recognise the need to be part of cross-industry efforts to address online consumer harms. Unfortunately, Australians continue to be targeted by domestic and international bad actors. Most scams occur via phone, text message, or email[1], but bad actors also use online services. They create an adversarial environment and continuously evolve their tactics, meaning all parts of industry, government and civil society need to play their part to protect Australians.

Meta is constantly iterating on the best way to protect consumers, and we have made significant investments and improvements in recent years. Some highlights include:

- We have invested heavily in artificial intelligence to proactively detect content or behaviour on our services that may be harmful for consumers. For example, in the third quarter of 2022, we actioned 1.5 billion fake accounts from our services (99.6 per cent of which we detected proactively before a user reported it to us) and 1.4 billion pieces of spam content (98.5 per cent of which we detected proactively).
- We have continued to increase our protections against hacked accounts, including reducing the risk of bad actors abusing our support channels, improving methods of verifying consumers, creating new channels for users to get back into hacked accounts, and testing live chat support for users in countries like Australia.[2]
- We have partnered with Australian organisations to be responsive to any concerns experienced by Australian users, including partnerships with organisations like IDCare, Puppy Scam Awareness Australia, and consumer protection authorities.

[1] ACCC, *Targeting scams*, report https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202021.pdf . Phone: 50%; Text message: 23%; Email: 14%; Internet: 4%; Social media: 4%.
[2] N Gleicher and J Almendares, 'Designing account security across our apps', *Meta Newsroom*, 15 December 2022, https://about.fb.com/news/2022/12/designing-account-security-across-our-apps/.

Notwithstanding the significant proactive work that Meta does to protect consumers, we can see benefit in some of the consumer protection regulatory proposals from the ACCC. We have been longstanding supporters of the proposed ombudsman for digital platforms and internal dispute resolution requirements, since first proposed by the ACCC in the Digital Platforms Inquiry in 2019. If well-designed, these recommendations could benefit consumers by providing clear pathways for resolving concerns, and provide Australian policymakers with confidence in how we respond to consumers. If approved by the Government, these proposals could be implemented quickly, including potentially via industry co-regulation. Our submission provides constructive suggestions on how these proposals could be designed, and we would welcome the opportunity to engage with Treasury further.

However, one consumer protection recommendation is fundamentally ill-conceived: the proposed 'notice and action' obligation, which would make digital platforms liable for taking action in response to every communication from users. This proposal is near-impossible to practically implement and would perversely inhibit the policy outcomes it is intended to serve. Detecting scams can be difficult and user reports often lack the context or identifiers necessary to locate the alleged scammer or verify that fraud has occurred. If a 'notice and action' proposal were implemented, we anticipate the consequences could include: companies shifting resources away from proactive and more longer-term work to detect scams and towards a more reactive, 'whack-a-mole' approach; or limiting complaints channels to those methods which collect sufficient accurate information to take action (such as on-platform reporting).

There are other policy options which could improve responsiveness to consumer complaints much more effectively. We support the National Anti-Scams Centre, for which the Government has already allocated funding. The Government has already committed to a consumer code on scams that covers digital platforms, and we believe that industry could develop a set of obligations via an industry code quickly. Meta would be very willing to work constructively via this process, and other industry members may be too.

Other consumer recommendations would benefit from further consideration in how they could be put into practice. Verification of advertisers and financial services and products, for example, is a good concept but is practically challenging to implement, given it is not possible for a digital platform to determine with confidence whether a financial services entity holds (or indeed is required to hold) an appropriate licence for that activity. We make some constructive suggestions on the design of these recommendations in our submission.

In addition to the consumer protection proposals, the ACCC makes recommendations about major amendments to the Australian competition law framework. It recommends a fundamental shift away from the philosophy that has underpinned Australian competition law to date. The current cross-economy competition law framework is largely based on responding to the reality of anti-competitive conduct by carefully examining the actual impact that specific acts may have had ("ex-post") but these regulatory proposals are intended to attempt to forecast and speculate on possible conduct and prohibit companies from undertaking broad categories of behaviors without evidence that these acts actually harm consumers ("ex-ante"). Ex-ante regulation grants regulators significantly greater discretion and generates much greater uncertainty for companies. Importantly, they threaten to prohibit substantial swathes of conduct that may be pro-competitive or beneficial for consumers.

The rationale for establishing new and very broad ex-ante regulation - via a series of competition codes - is unsound.

Firstly, the ACCC claims that current laws are not sufficient to prevent anti-competitive conduct by digital platforms. We would not suggest digital markets are immune from anti-competitive conduct. Indeed, some of our competitors benefit significantly from their integration and control of the hardware and operating systems we rely on to reach users. Apple's and Google's control over both hardware and software in mobile ecosystems allows them to set the 'rules of the game' for competitors who seek to use their app stores, and they have both the ability and incentive to provide their own apps with a competitive advantage.

Even with our concerns about the conduct of some of our competitors, we still believe existing competition laws are sufficient to deal with concerns about anti-competitive conduct that could arise. Australia's existing competition laws are broad, flexible and modern.

The ACCC has claimed that enforcement of existing laws will be too slow for digital markets, which are more dynamic and move quickly. Courts play an important check and balance on the behaviour of regulators. The examples cited by the ACCC are not unique to digital platforms. And, in any case, the existing laws (in particular the new section 46 provision) are largely untested with respect to digital platforms, as the ACCC has generally not brought cases forward under existing law and has instead moved straight to regulatory reform.

Secondly, there is insufficient precision about the specific harms that the proposed codes are intended to address. The Digital Platforms Services Inquiry report speculates on possible harms but (with the exception of the app stores) does not provide examples or evidence that reflect the very broad proposed scope of ex-ante codes.

It is especially challenging for a company like Meta to comment, as the analysis of the markets in which we operate is not current. The ACCC is currently updating their view of social media services and advertising in the latest report under the Digital Platforms Services Inquiry. It is not possible to understand how these regulatory proposals might apply to our services, given the ACCC's analysis of these markets is still underway and is only being undertaken *after* proposing regulatory change.

We see significant dynamism in the digital markets in which we operate. There has been increased competition, new entry and rapid growth of Meta's competitors, since the Digital Platforms Inquiry began in 2017. TikTok has emerged as a major competitor (for example, in 2021, Australian users spent almost one day per month (23.4 hours) on TikTok compared to 17.6 hours on Facebook and 8.3 hours on Instagram)[3], along with continued strong competition from the likes of YouTube, Twitter, Snapchat, Twitch, Reddit, Discord, LinkedIn, Pinterest and new entrants like BeReal. In relation to advertising, we have seen the emergence of massive competitors like Apple. Apple is advantaged by its existing infrastructure in relation to apps and devices, and their growing ads business (as well as their iO14 changes purportedly aimed at "privacy") directly impacted Meta's global revenue by $10 billion in 2022 alone. Other developments have included the growth of Amazon (experiencing a three-fold increase in revenue in Australia), and new offerings from existing competitors like Google, Microsoft, Netflix and News Corp (among others).

While there may be sufficient evidence to implement ex-ante regulation for app stores, the regulatory reform report proposes competition codes for a much broader range of services and behaviours that do not have the same established evidence of harm. In fact, arguably, some of the proposed areas for codes (like interoperability, third party access to data, and transparency) are much broader than competition issues alone and raise major concerns relating to privacy and data protection.

Thirdly, the ACCC's report does not properly account for the risks associated with broad ex-ante competition codes. We are generally sceptical about the proposed approach to developing binding codes for 'designated' digital platforms. Mandatory codes that target

[3] Data.ai, *State of Mobile 2022,* report published 12 January 2022, p 50, https://www.data.ai/en/go/state-of-mobile-2022/.

one or two companies are a poor public policy tool. They risk distortion and inequity across markets. They run the risk of a regulator imposing regulatory requirements without regard for evidence, the potential costs or consequences of regulation, and without proper oversight.

If the Government proceeds with competition codes, we strongly believe robust checks and balances would need to be developed to ensure the responsible regulator(s) have proper regard for evidence, and the costs and risks of their actions.

We are concerned about the suggestion that competition codes are only necessary for digital platforms. The characteristics of markets identified in the Discussion Paper (such as use of data, potential self-preferencing, and lack of data-sharing between companies) are not unique to digital platforms. Regulating specific services or segments too narrowly will create market distortions between digital platforms and other competitors (such as print and broadcasting advertisers) and inhibit innovation and investment.

The Government is right to observe international developments in this space, but international developments are not of themselves sufficient cause to amend Australian law. Australia has kept its competition and consumer law framework current by making updates several times in recent years. Given we are yet to see the full impact of new international requirements, there is an opportunity for Australian policymakers here: Australia could learn from other jurisdictions and take ideas once they are proven to work, without any of the risk of unintended consequences to investment and innovation.

We recommend that the Australian Government at least wait until the conclusion of the Digital Platforms Services Inquiry in 2025 before proceeding with competition regulatory reform. This would provide further time to undertake further analysis and consultation, and for the codes to be targeted only at an identified series of behaviours. We recommend prioritising consumer reform before any competition recommendations.

Table of contents

Meta's existing work on consumer protection

It is in Meta's business interest to invest in ensuring that people have a positive and safe experience when interacting on our platforms. We take a comprehensive approach to protecting consumers from bad actors, through our **policies**, **enforcement** of those policies, **resources and tools** to raise awareness of scams among consumers, and **partnerships** with other organisations that can complement our efforts. More detail about each of these is provided below.

Policies

We have developed a set of policies, known as our Community Standards,[4] that outline what is and is not allowed on Meta's services. These policies are developed based on a range of values to help combat abuse. Safety is a core value of our Community Standards, alongside privacy, authenticity, voice, and dignity.[5] They relate to 'organic' content, or the material that people post from their accounts or Pages that is non-paid.

Aspects of our policies most relevant to protecting consumers and combatting scammers include:

- Our policy against **fake accounts** on Facebook. We require authenticity of our users, which we believe helps create a community where people are meaningfully accountable to each other, and to Facebook. For example, we prohibit impersonation of others, and the creation or use of an account that deliberately misrepresents identity in order to mislead or deceive others, or to evade enforcement.

- **Spam.** We work hard to limit the spread of spam on Facebook and Instagram because we do not want to allow content that is designed to deceive, or that attempts to mislead users, to increase viewership. For example, we prohibit the deceptive or misleading use of URLs, which could involve cloaking, deceptive redirect behaviour, deceptive landing page functionality, or typosquatting.

- **Cybersecurity.** We prohibit a range of behaviours to gather sensitive personal information or engage in unauthorised access of data by invasive or deceptive methods.

[4] See Meta, *Community Standards*, https://www.facebook.com/communitystandards
[5] Monika Bickert, *Updating the values that inform our community standards*, https://about.fb.com/news/2019/09/updating-the-values-that-inform-our-community-standards/

- **Inauthentic behaviour.** We do not allow people to engage in 'inauthentic behaviour', which we define as misrepresenting themselves on Facebook, using fake accounts, artificially boosting the popularity of content or engaging in behaviours designed to enable other violations under our Community Standards. While some inauthentic behaviour may be politically-motivated or influence operations, it may also be for financial purposes.

We adjust these policies regularly, in consultation with experts. We are in an adversarial situation with bad actors and find that they regularly adapt their tactics to evade our enforcement. We amend our policies to prohibit new forms of harmful behaviour as they emerge.

Advertisers must also comply with our Advertising Policies. Our Advertising Policies set even-stricter standards than our Community Standards. One of the key principles of our Advertising Policies is to protect people from fraud or scams.

Aspects of our Advertising Policies most relevant to protecting consumers and combatting scammers include:

- **Unrealistic outcomes.** Ads are not allowed to contain promises or suggestions of unrealistic outcomes that we have specifically identified with experts and relate to health, weight loss or economic opportunity.

- **Prohibited financial products.** Ads are not allowed to promote financial products and services that are frequently associated with misleading or deceptive promotional practices. Some of these products include payday loans, bail bonds, initial coin offerings, or contract for difference trading.

- **Spyware or malware.** We do not allow ads to contain spyware, malware or any software that results in an unexpected or deceptive experience.

We have additional, specific restrictions for certain kinds of businesses and products, including financial and insurance products and services, cryptocurrencies, online gambling and gaming (including social casinos).

Finally, we also have developed a Branded Content Policy that requires any content from creators or publishers that are promoting branded content to tag the featured third-party product, brand or business partner using the branded content tool. This helps to provide

transparency for consumers about when a creator is promoting a brand under a partnership.

Enforcement

We invest substantial resources in detecting and actioning content and accounts that can cause harm to consumers.

In recent years, we have invested significantly in artificial intelligence to detect harmful content and accounts, before a user needs to see it. This progress is evident through the transparency reports that we publish every quarter. For example, in Q3 2022, the last quarter with available data:

- We actioned 1.5 billion **fake accounts**, 99.6 per cent of which we detected proactively ourselves via artificial intelligence before a user reported it to us. This is in addition to the millions of fake accounts that we block at the point of creation every day.

- We actioned 1.4 billion pieces of **spam** content, 98.5 per cent of which we detected proactively ourselves via artificial intelligence.

- We have now taken action against more than 200 networks of coordinated **inauthentic behaviour** since we began our public reporting on that work in 2017. We know that inauthentic behaviour threats are rarely confined to one platform.

- In October 2022, we reported that we had identified more than 400 malicious android and iOS apps that were designed to steal Facebook login information and compromise people's accounts. These apps were listed on the Google Play Store and Apple's App Store and disguised as photo editors, games, VPN services, business apps and other utilities to trick people into downloading them. We reported these malicious apps to our peers at Apple and Google and they have been taken down from both app stores. We also alerted people who may have unknowingly self-compromised their accounts by downloading these apps and sharing their credentials, and are helping them to secure their accounts.[6]

In addition to our use of technologies to enforce our policies, we are also taking action against bad actors *under the law*, creating real world consequences for their actions on

[6] D Agranovich and R Victory, 'Protecting people from malicious compromise apps', *Meta Newsroom*, 7 October 2022, https://about.fb.com/news/2022/10/protecting-people-from-malicious-account-compromise-apps/.

our platforms. This means not just suspending and deleting accounts, Pages, and ads, but also taking legal action in certain instances against those responsible for violating our rules. We have led the industry in pursuing legal avenues across borders to protect users, no matter where they are in the world.

For example:

- in March 2022, we commenced legal proceedings against an individual that violated our Facebook Terms and Policies by providing fake reviews and feedback for businesses to artificially increase their Facebook Customer Feedback Score and evade Meta's detection and enforcement against misleading ads.[7]

- in February 2022, we filed a lawsuit with a financial services company against two Nigerian-based individuals engaged in international financial scams through online impersonation.[8]

- in December 2021, we filed legal action against a Vietnamese-based group which targeted the accounts of employees of marketing companies and tricked victims into self-compromising their accounts by installing malicious software that was deceptively promoted as Facebook-affiliated tools for managing ads.[9]

- in June 2021, we brought a lawsuit against a company and two individuals who ran deceptive ads on Facebook, which redirected users to a third-party e-commerce site and engage in a bait-and-switch scheme. We also took action against a group of individuals who misled victims into self-compromising their accounts by installing a mobile app from the Google Play Store deceptively called "Ad Manager for Facebook", which prompted users to share their Facebook login credentials.[10]

Many of the examples of our platform enforcement have relevance for Australia, either by combatting bad actors who may target Australians, or by pursuing bad actors based in Australia.

We strongly believe that creating real world consequences for scam advertisers and other bad actors - including through legal action - is important to protect our users and

[7] J Romero, 'Taking action against fake customer feedback and reviews', *Meta Newsroom*, 16 March 2022, https://about.fb.com/news/2022/03/taking-action-against-fake-customer-feedback-and-reviews/
[8] J Romero, 'Taking legal action against financial services scams', *Meta Newsroom*, 8 February 2022, https://about.fb.com/news/2022/02/taking-legal-action-against-financial-services-scams/ .
[9] J Romero, 'Combating e-commerce scams and account takeover attacks', *Meta Newsroom*, 29 June 2021, https://about.fb.com/news/2021/06/combating-e-commerce-scams-and-account-takeover-attacks/.
[10] J Romero, 'Combating e-commerce scams and account takeover attacks', *Meta Newsroom*, 29 June 2021, https://about.fb.com/news/2021/06/combating-e-commerce-scams-and-account-takeover-attacks/.

maintain the integrity of our services. However, creating these consequences – and disrupting economic incentives – also requires that Governments and regulators play a critical role in pursuing action against scammers. Meta would welcome further action by Governments and regulators to take action against scammers on online platforms and other communication services.

Resources and tools

We work hard to provide resources and tools for consumers, to raise their awareness about how they can take steps to protect themselves.

Some of the awareness-raising steps we take include:

- Regularly providing in-product reminders to prompt users to strengthen the security of their account by opting into two-factor authentication. These can be seen below in **Image 1** and **Image 2**. This feature guides users through setting up two factor authentication, checking login activity, confirming the accounts that share login information and updating account recovery.

Image 1: Facebook security prompt

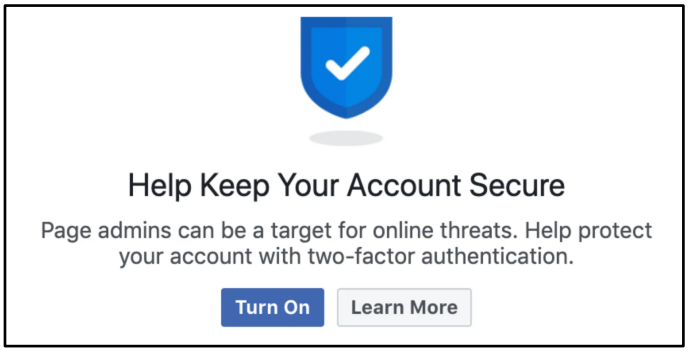
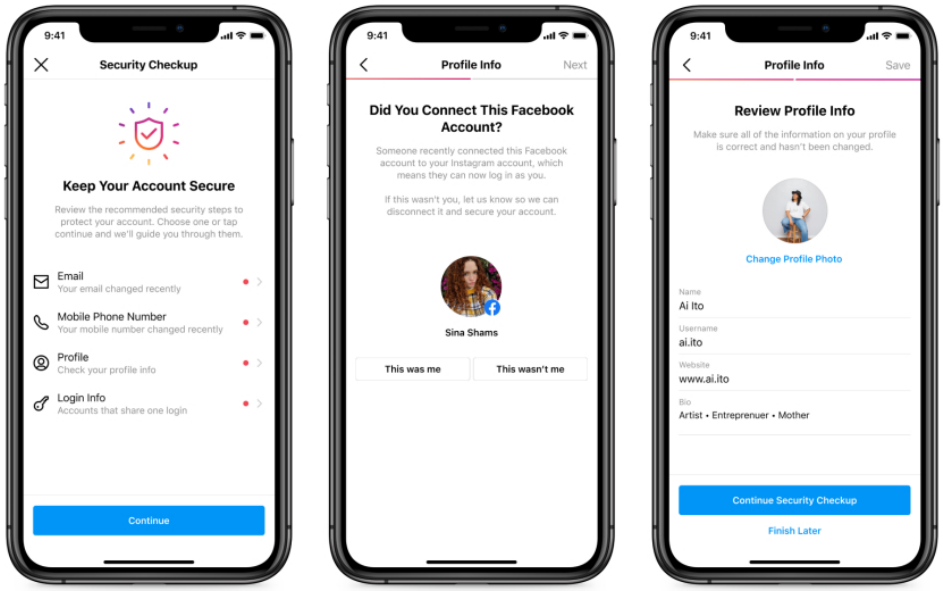


Image 2: Instagram security checkup



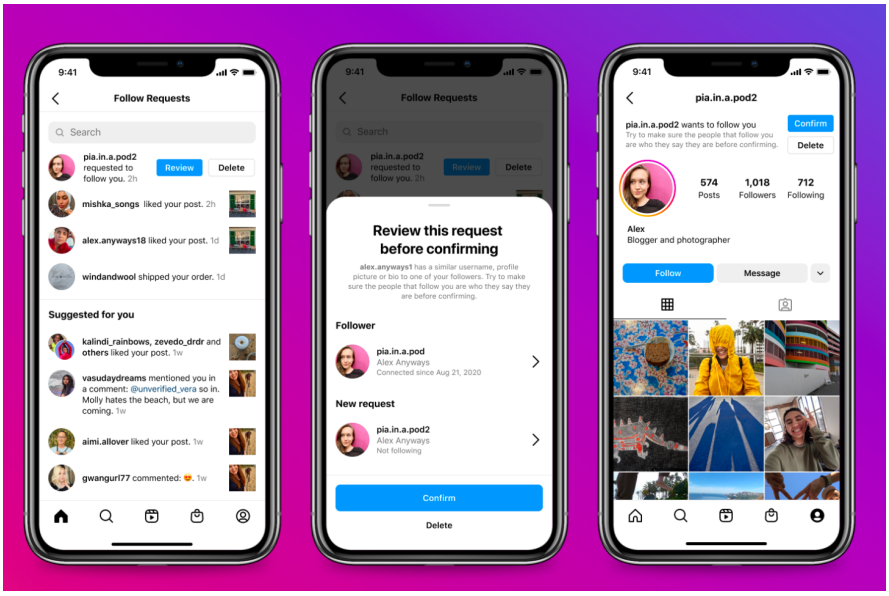
- We include tutorials in our education hub on how to turn on each security control, including providing tips on how to recognise spam and suspicious emails or messages.

- In 2021, we launched Australia Facebook Protect in Australia, a program designed for people that are likely to be highly targeted by malicious hackers. Facebook Protect helps these groups of people adopt stronger account security protections, like two-factor authentication, and monitors for potential hacking threats.

- Messenger impersonation safety notices. If an account messaging someone appears like it could be impersonation, we intervene with a safety notice, asking them if they would like to report the account to us.[11]

[11] Instagram, 'Continuing to keep Instagram safe and secure', *Instagram Blog*, 15 December 2022, https://about.instagram.com/blog/announcements/continuing-to-keep-instagram-safe-and-secure.

Image 3: Instagram safety notice



- In December 2022, we announced that we've built additional ways for people to get back into their accounts when they have been hacked.[12] For instance, in certain cases, people can use recently removed contact points to recover access. As a result, this year we've helped **eight times more people a day on average get back into their Facebook account** than last year when they don't have access to their listed contact points. We're also running global in-app prompts across Facebook reminding people to confirm their contact points and exploring alternative ways to confirm people's identity during the account recovery process on Instagram, including using their friend network.

  We've also launched dedicated portals to help users regain access to their accounts if they have been hacked: facebook.com/hacked and instagram.com/hacked. Re-gaining access to hacked accounts is a particular challenge because it's one area where the easier you make it for consumers, the easier it is for hackers to use as well.

- In Australia, we have run a series of public awareness campaigns. In July 2022, we ran a public awareness campaign with the Australian Small Business and Family Enterprise Ombudsman and IDCARE that reached more than **8 million Australians**. We replicated that campaign for Scam Awareness Week in November 2022, with specific tips on some of the most popular types of scams, including romance scams, investment scams, online shopping scams, phishing, scams

[12] N Gleicher and J Almendares, 'Designing account security across our apps', *Meta Newsroom*, 15 December 2022, https://about.fb.com/news/2022/12/designing-account-security-across-our-apps/.

around family members in need, and impersonation. We are planning to extend these very successful campaigns into 2023.

- While our scaled account recovery tools aim at supporting the majority of account access issues, we know that there are groups of people that could benefit from additional, human-driven support. In 2022, we carefully grew a small test of a **live chat support feature** on Facebook in nine countries (including Australia).

Partnerships

Our efforts to protect consumers on our platforms are extensive. However, no technology or process is perfect. For that reason, we partner with other organisations that can raise concerns with us on behalf of a consumer if they require additional support.

We have partnered with NGOs like IDCare and the Puppy Scam Awareness Australia to raise awareness and support people who have observed a potential scam.

We work with government agencies and regulators in a variety of ways. As mentioned above, we partnered with the Australian Small Business and Family Enterprise Ombudsman to reach 8 million people with materials to raise awareness about scams. We work with state and territory consumer protection bodies. We take a 'no closed door' approach and consider any referrals or concerns raised with us by any government agency.

We have also built systems to assist with intaking referrals from the ACCC. We hope the National Anti-Scam Centre, an election commitment of the government, may provide an opportunity to examine how the ACCC and other federal government agencies could have improved collaboration with industry.

We have further constructive suggestions about ways to improve collaboration between government agencies and industry that we would be happy to provide.

Consumer protection recommendations

Notwithstanding the significant proactive work that Meta does to protect consumers, we can see benefit from some of the consumer protection regulatory proposals from the ACCC.

In considering potential new consumer measures applying to digital platforms, we recommend that Treasury account for the large number of consumer protection proposals currently under consideration by governments. As noted in the discussion paper, the Government is already pursuing economy-wide consumer measures (relating to unfair trading practices and unfair contract terms laws) and new regulatory codes for platforms relating to scams. Many of the proposals in the discussion paper would duplicate these efforts.

We provide further comments on the following specific proposals:

- An independent ombudsman scheme for digital platforms
- A legislative 'notice and action' requirement
- Obligations around verification processes for advertisers and business users.

Digital platforms ombudsman

The ACCC has reiterated its recommendations from the 2019 Digital Platforms Inquiry to establish a digital platforms ombudsman and internal dispute resolution standards.

We have been longstanding supporters of the proposed ombudsman for digital platforms and internal dispute resolution requirements, since first proposed by the ACCC in the Digital Platforms Inquiry. If well-designed, these recommendations could benefit consumers by providing clear pathways for resolving concerns, and provide Australian policymakers with confidence in how we respond to consumers.

If approved by the Government, these proposals could be implemented quickly, including potentially via industry co-regulation.

There are some important design considerations for any digital platforms-specific ombuds scheme. We provide some constructive suggestions on the following aspects:

- *Scope of complaints*. The nature of digital platform complaints differs from those received by a telecommunications company or a bank.

  As well as transactional complaints around a customer's own account and financial exchanges with the platform, we also may receive complaints about content (for example, when a customer may be unhappy that their post violates our policies against hate speech or bullying). Content complaints are

fundamentally different in nature to transactional complaints: they raise questions of free expression, safety and harm, and political expression. They are also subject to other laws and regulatory processes. These complaints are entirely unsuitable to be considered by an ombudsman, and we strongly recommend they should be out of scope for any ombuds scheme.

Similarly, consumers may have also concerns about an interaction that they have with *other users* on the platform. These are called 'social disputes', such as where there may be a dispute about an exchange of second-hand goods. Digital platforms are rarely able to assist in these instances; even if the initial introduction or part of the engagement occurs on our services, social disputes almost always involve some off-platform context or interaction where a platform does not have visibility. There would also be concerns raised about asking large companies to arbitrate between two disputing individuals.

And, finally, because of the ease with which consumers can switch between services, bad actors can often ask consumers to hop around between different services. This makes detection very challenging, as a single digital platform does not have all the information or context themselves that is necessary to determine if a scam has occurred.

There has been thorough research undertaken by a number of academics at the University of Technology Sydney which assists in categorising the different types of interactions between users, platforms, and user to user.[13]

To account for these practical difficulties, we recommend that the scope of an ombuds scheme should be limited to interactions *between a consumer and a platform* and generally relating to the *financial or transactional* elements of that interaction.

- *Format for complaints.* Digital platforms have been leaders in innovative approaches to customer service which have since been copied across other industries. It is digital companies who pioneered approaches like self-service options, live chat, and clear, simple, consumer-friendly reporting, and they have done so when their services are free to consumers to use. These techniques are much better for consumers than old approaches to customer service that relied on

[13] H Raiche, D Wilding and A Stuhmucke, *Digital platform complaint handling: options for an external dispute resolution scheme*, https://www.uts.edu.au/sites/default/files/2022-08/CMT%20DPCH%20Report%20-%20electronic%20version.pdf

call centres and are often bureaucratic and slow. We anticipate digital platforms will continue to innovate in how they engage with consumers.

For that reason, we recommend that an ombudsman should not have powers to prescribe the format in which complaints must be received, in order to avoid chilling innovation in how digital platforms engage with consumers.

- *Scope of platforms.* To avoid distortions in markets, an ombudsman should be empowered to deal with complaints from all participants who engage in an industry. For example, if digital advertising is considered within scope, *all* digital advertisers should be captured.

- *Interaction with other complaint channels.* As we have outlined earlier, Meta engages with a large number of federal, state and territory regulators - and civil society actors - to ensure a 'no closed door' approach to consumer concerns. Part of the reason we can see benefit in a digital platforms ombudsman is because the large number of regulators and government agencies can leave consumers confused and unclear about pathways available to them. For that reason, the benefits of a digital platforms ombudsman will only be realised if it simplifies processes for consumers. An ombudsman should work with other regulators to ensure streamlined pathways for both consumers and platforms, potentially via a central clearinghouse.

  There may be opportunities to build on existing cross-industry complaints channels, like the one that the industry association DIGI has established under the voluntary industry code on misinformation and disinformation.

- *Independently reviewed for effectiveness*. Once an ombudsman is established, they may have incentives to entrench or expand their scope. The effectiveness of the ombudsman should be reviewed independently, at some point in the 2-3 years after establishment.

Notice and action obligation

The ACCC has proposed a "notice and action" obligation, which would make digital platforms liable for taking action in response to every communication from users. This proposal is fundamentally ill-conceived, near-impossible to practically implement and would perversely inhibit the policy outcomes it is intended to serve.

At its heart, it over-estimates the quality and usefulness of user reports as a signal of scams or fraud.

Detecting scams is tremendously difficult. Bad actors are highly sophisticated and take complex steps to evade enforcement and detection.

The overwhelming majority of fake accounts, spam or harmful content that we remove from our platform is detected proactively by us using artificial intelligence. These techniques are not just more suitable for the global scale at which our services operate, but also better for consumers, given they do not need to experience the scam in the first place.

At times, user reports can play a helpful role in supplementing our proactive detection. They can send us a signal of behaviour or content that people do not want to see on our services. However, there are some major limitations in relying primarily on user reports for scam detection:

- There can be a significant amount of 'noise' in user reports. The accuracy of user reports can be highly variable, depending on the type of report. Alleged scams and fraud can be particularly challenging.
- User reports often lack the context or identifiers necessary to locate the alleged scammer or verify that fraud has occurred. This can be because the user and scammer switch across different platforms to engage, or because there is some context (potentially offline) that is not visible to the platform.
- Adversarial bad actors may abuse reporting systems by submitting abusive, fraudulent or overreaching reports. This problem could be compounded if they know that platforms may have legal liability attached to responding to those channels.

Consequently, a 'notice and action' obligation would cause great concern for digital platforms because it establishes potential liability for a scam via the notice, but does not provide sufficient information for the digital platform to detect or identify the behaviour at issue. Platforms would be placed in the challenging position of deciding how to respond and would either need to:

- Invest enormous resources to investigate and thoroughly run down every possible user report they receive, via every channel. The regulatory cost impact would be very significant and it would be challenging for platforms to meet this resourcing

obligation without re-directing resources away from other work (such as proactive detection) that is actually more long term.

- Limit the channels via which platforms accept user reports. Currently, under our 'no closed door' approach, we accept referrals from trusted partners and regulators, even if they are not high-quality. For example, reports we receive from some regulators do not collect information relevant to Facebook (such as specific URLs) because the form has not been appropriately designed. If a 'notice and action' proposal were to proceed, we would only be able to accept referrals from channels that collect sufficient specific information for us to take action.

Neither of those outcomes serve the interests of Australian consumers.

There are other policy options which could improve the ability of digital platforms to be responsive to consumer complaints much more effectively. One of the reasons we believe a digital platforms ombudsman could be effective is because it provides consumers with a clear channel to resolve concerns and also a single point of contact that would develop deep knowledge about digital platforms' processes to detect harmful content or behaviour. An ombuds scheme could assist in this regard.

Alternatively, if the Government is determined to regulate digital platforms' responsiveness to complaints, the Online Safety Act provides a much more effective model. However, it relies on the notice to be provided by an expert regulator that has invested the resources to vet and investigate the veracity of a complaint first. This ensures that (1) if there is information across different platforms or services, it can be aggregated to provide full context; and (2) consumers have a simpler experience that means they do not need to report across multiple platforms or sites.

Verification process obligations

The discussion paper specifically identifies three other potential new obligations that would relate specifically to the processes digital platforms take in relation to verifying advertisers and business users. These are:

- To verify certain business users
- To add additional verification of advertisers of financial services and products
- To improve review of verification disclosures.

In principle, verification of advertisers is a beneficial measure to ensure the integrity of advertising. Meta takes steps to verify some users, especially for certain kinds of products, such as cryptocurrencies, online gambling or political advertising. We also require certain businesses to be verified, and have taken a proportionate approach by specifying the categories of businesses that need to meet this requirement.[14]

However, there are a range of detailed design considerations that would need to be considered before compelling digital platforms to take further steps to verify business users.

- For financial products, it is not always clear whether a financial licence is required. Verification of advertisers of financial services and products, for example, is a good concept but is practically challenging to implement. There is no comprehensive public register of which financial services providers are licensed and which are not. While some licence holders are publicly searchable, in some cases, financial services providers are not required to be licensed because they may be able to avail themselves of an exemption or the licence may apply to aspects of their services and not others.

- Any obligations should be strictly limited to paid advertisements, that is, advertising content that digital platforms are promoting in exchange for payment. It is not possible for these obligations to apply to 'organic', non-paid content without applying to *all* organic users, whether they are individuals, businesses, community groups or other creators. The risks of requiring large-scale verification of the identity of all users of digital platforms have been well-examined in the context of the previous Government's proposed Anti-Trolling Bill, which did not proceed.

- It is important to note that requiring verification processes to be stricter or broader will not necessarily mitigate against scams. For example, we see examples where verified business accounts then become high-value targets for scammers to hack because users think it is verified and trusted. There is no 'silver bullet' to combatting scammers: it requires a comprehensive and constantly-evolving set of measures. Overly-broad or prescriptive requirements can increase the regulatory burden, without necessarily improving the efficacy of scam detection work.

[14] Meta Business Help Center, 'About Business Verification', *Meta Business Help Center*, https://www.facebook.com/business/help/1095661473946872?id=180505742745347.

Competition recommendations

In addition to the consumer protection proposals, the ACCC makes recommendations about amendments to the Australian competition law framework.

It recommends a fundamental shift away from the philosophy that has underpinned Australian competition law to date. The current cross-economy competitive law framework is largely based on responding to the reality of anti-competitive conduct ("ex-post") but these regulatory proposals are intended to attempt to forecast and speculate on possible conduct and prohibit companies from undertaking behaviours which could be anti-competitive in future ("ex-ante"). Ex-ante regulation grants regulators significant greater discretion and generate much greater uncertainty for companies.

We believe the rationale for establishing new, broad ex-ante regulation - via a series of competition codes - is unsound. While we acknowledge the risks of anti-competitive conduct with relation to app stores identified by the ACCC, for all other proposed areas to be covered by competition codes, the rationale is based on speculation of possible - not observed - risks.

We also provide some general comments on the consequences of shifting to an ex-ante based regime that relies on a series of narrow codes. And we provide some commentary on the matters that the ACCC recommends to be covered by codes.

Rationale underpinning the ACCC's recommendations

We have a number of concerns with the underpinning rationale that the ACCC has relied on to recommend new and very broad competition codes.

Firstly, the ACCC claims that current laws are not sufficient to prevent anti-competitive conduct by digital platforms.

We would not suggest digital markets are immune from anti-competitive conduct. Some of our competitors benefit significantly from their integration and control of the hardware and operating systems we rely on to reach users. Apple's and Google's control over both hardware and software in mobile ecosystems allows them to set the 'rules of the game' for competitors who seek to use their app stores, and they have both the ability and incentive to provide their own apps with a competitive advantage.

However, even with our concerns about the conduct of some of our competitors, we still believe existing competition laws are sufficient to deal with concerns about anti-competitive conduct that could arise. Australia's existing competition laws are broad, flexible and modern.

The ACCC has claimed that enforcement of existing laws will be too slow for digital markets, which are more dynamic and move quickly. They cite international enforcement actions against digital platforms and Australian enforcement actions against other large / sophisticated firms, as the ACCC has not brought any competition proceedings against any digital platform in Australia.

While we acknowledge competition proceedings can occasionally take time, it's important to recognise that these are matters that require complex analysis and can have significant consequences for businesses and consumers. Courts also play a vital check and balance on the behaviour of regulators. While regulators may prefer to move much faster and with greater discretion, it is not necessarily in the broader public interest.

In any case, the existing laws (in particular the new section 46 provision) are largely untested with respect to digital platforms as the ACCC has generally not brought cases forward under existing law and has instead moved straight to regulatory reform.

There is no evidence that an ex ante regulatory regime will address these complex issues faster. Declaration regimes may also end up in lengthy court litigation in order to determine matters such as whether a party ought to have been declared, the proper application of criteria, and the exercise of discretion (for example, declared infrastructure under Part IIIA of the CCA). In this case, the designation criteria being recommended to designate a digital platform could be subject to the same process that the ACCC sees as slow and high-cost.

Secondly, there is insufficient precision about the specific harms that the proposed codes are intended to address. The Digital Platforms Services Inquiry report speculates on possible harms but (with the exception of the app stores) does not provide examples or evidence that reflect the very broad proposed scope of ex-ante codes.

It is especially challenging for a company like Meta to comment, as the analysis of the markets in which we operate is not current. ACCC is currently updating their view of social media services and advertising in the latest report under the Digital Platforms Services Inquiry. It is not possible to understand how these regulatory proposals might

apply to our services, given the ACCC's analysis of these markets is still underway and is only being undertaken *after* making regulatory proposals.

We see significant dynamism in the digital markets in which we operate. There has been increased competition, new entry and rapid growth of Meta's competitors, since the Digital Platforms Inquiry began in 2017.

Current evidence would strongly contradict the view that Meta has substantial market power in "social media": TikTok has emerged as a major competitor (for example, in 2021, Australian users spent almost one day per month (23.4 hours) on TikTok compared to 17.6 hours on Facebook and 8.3 hours on Instagram).[15] TikTok did not even exist in Australia at the time of the 2019 Digital Platforms Inquiry, indicating the level of dynamic competition in digital markets is high.

In addition to the emergence of a large player, there has also been continued strong competition from YouTube, Snapchat, Twitch, Reddit, Discord, LinkedIn, Pinterest and new entrants like BeReal.

In relation to advertising, we have seen the emergence of massive competitors like Apple. Apple is advantaged by its existing infrastructure in relation to apps and devices, and their increasing ads business (as well as their iO14 changes) directly impacted Meta's global revenue by $10 billion in 2022 alone. Amazon has also seen rapid growth as a direct competitor to Meta. In 2021, Amazon's advertising business generated $31.2 billion in revenue globally, with 32% year-over-year growth,[16] including a threefold revenue increase in Australia in 2021 alone.[17] There have also been new offerings launched from existing competitors like Google, Microsoft, Netflix and News Corp.

We have also continued to adapt and evolve their offerings in response to technological developments and changes in consumer demand. Indeed, we renamed our company Meta to reflect our focus to bring the metaverse to life and to help people connect, find communities, and grow businesses. Advancements have shifted the focus towards generative artificial intelligence. And consumers' preferences are fundamentally shifting towards short-form video and creator content. Rapidly-changing technology and

[15] Data.ai, *State of Mobile 2022*, p 50, https://www.data.ai/en/go/state-of-mobile-2022/ .
[16] Amazon, 'Amazon.com Announces Fourth Quarter Results', *Amazon*, 3 February 2022, https://ir.aboutamazon.com/news-release/news-release-details/2022/Amazon.com-Announces-Fourth-Quarter-Results/#:~:text=Operating%20income%20decreased%20to%20%243.5,share%2C%20in%20fourth%20quarter%202020.
[17] S Buckingham, 'Amazon triples Australian ad revenues, media execs predict it will triple again in 2022 as juggernaut starts to roll', *Mi3*, 22 February 2022, https://www.mi-3.com.au/22-02-2022/amazon-tripled-its-ad-business-2021-track-more-100m-revenue-2022.

consumer preferences erode any competitive advantages that might otherwise have been available to services with large user bases.

While there may be sufficient evidence to implement ex-ante regulation against app stores, the regulatory reform report proposes competition codes for a much broader range of areas that do not have the same evidence base. In fact, arguably, some of the proposed services and behaviours for codes (like interoperability, third party access to data and transparency) are much broader than competition issues alone and raise major concerns relating to privacy and data protection.

Thirdly, the ACCC's report does not properly account for the risks associated with broad ex-ante competition codes. We are generally sceptical about the proposed approach to developing binding codes for 'designated' digital platforms. Mandatory codes that target one or two companies are a poor public policy tool. They risk distortion and inequity across markets. They run the risk of a regulator imposing regulatory requirements without regard for evidence, the potential costs or consequences of regulation, and without proper oversight.

The analysis does not pay sufficient regard to significant benefits that digital platform services have brought to Australian consumers, including lowering barriers to entry, lowering costs of expansion and facilitating new and efficient ways for Australian businesses to reach interested customers worldwide. For example, a recent report by Deloitte found that 82% of Australian small businesses reported using free, ad-supported Facebook apps to help them start their business, and 71% of Australian small businesses that use personalised advertising reported that it is important for the success of their business.[18] This means that badly-designed regulation could have significant consequences for innovation and investment.

We are concerned about the suggestion that competition codes are only necessary for digital platforms. The characteristics of markets identified in the Discussion Paper (such as use of data, self-preferencing, and lack of data-sharing between companies) are not unique to digital platforms. Regulating specific services or segments too narrowly will create market distortions between digital platforms and other competitors (such as print and broadcasting advertisers) and inhibit innovation and investment.

[18] Deloitte, *Dynamic Markets Unlocking small business innovation and growth through the rise of the personalized economy,* https://www.facebook.com/business/news/new-insights-on-personalized-ads-and-social-medias-impact-on-small-businesses; and
Meta, *Dynamic Markets Report: Australia,* :
https://australia.fb.com/wp-content/uploads/sites/69/2021/10/nji-fb-ausresearch-report-r26.pdf

We recommend that the Australian Government at least wait until the conclusion of the Digital Platforms Services Inquiry in 2025 before proceeding with competition regulatory reform. This would provide further time to undertake further analysis and consultation, and for the codes to be targeted only at an identified series of behaviours. We recommend prioritising consumer protection recommendations (internal dispute resolution standards and a digital platforms ombudsman) before any competition recommendations.

Codes as a public policy tool

For that reason, we are generally sceptical about the proposed approach to developing binding codes for 'designated' digital platforms - even though Meta may stand to benefit if these codes target the anti-competitive behaviour that we have experienced. Mandatory, narrowly-scoped codes are a poor public policy tool. They risk distortion and inequity across markets. They run the risk of a regulator like the ACCC imposing regulatory requirements without regard for evidence, the potential costs or consequences of regulation, and without proper oversight.

We are concerned about the suggestion that competition codes are only necessary for digital platforms. The characteristics of markets identified in the Discussion Paper (such as use of data, self-preferencing, and lack of data-sharing between companies) are not unique to digital platforms. Defining markets too narrowly will create market distortions between digital platforms and other competitors (such as print and broadcasting advertisers) and inhibit innovation and investment.

We are concerned about assigning such broad matters to a regulator with full discretion and fewer checks and balances than they experience for the existing ex-post regimes.

If the Government proceeds with competition codes, we strongly believe robust checks and balances would need to be developed to ensure the responsible regulator(s) have proper regard for evidence and the costs and risks of their actions, and ensure robust due process rights for impacted parties against which new obligations may be enforced.

We would very much welcome the opportunity to work with Treasury on possible checks and balances. These should include:

- development of clear and objective criteria for inclusion of particular services.
- requirements that are based on an actual evidence base of harm, not simply speculation that harms could occur. This could be tied to a specific requirement

that a competitive assessment of specific service markets with evidence of harm has been undertaken by the ACCC prior to designation and inclusion of new services.

- requiring via legislative obligations that any designation (and inclusion of new services) is informed by current analysis that specifically identifies harms to consumer welfare resulting from observed conduct. This should also include a cost-benefit analysis or Regulatory Impact Statement to understand the cost of new requirements, without an ability to evade these requirements via a exemption
- a level of independence between the decision maker on designation and the regulator or body who is preparing market analysis and responsible for enforcement of any obligations
- compulsory consultation with all impacted stakeholders as part of the process (from designation to creation of codes), with a reasonable time period for consultation (for example, a minimum of 40 days)
- ensuring there are opportunities for companies to appeal their designation or inclusion in codes on appropriate standards for review. Judicial oversight is an essential component of Australia's competition law framework, and this should extend to both judicial and merits review of designation decisions and enforcement of any obligations.
- dedicated examination of regulator performance, to ensure the very broad discretion is used fairly. This could be done via dedicated components of the Regulator Performance Framework, via regular reviews of regulator performance by the Productivity Commission, and by a statutory review of the designation regime within two years of commencement.

Recommendations

Given the significant concerns associated with the ACCC's proposals, we recommend that the Australian Government wait until the conclusion of the Digital Platforms Services Inquiry in 2025 before proceeding with competition regulatory reform. This would provide further time for the ACCC to undertake further analysis, and for the codes to be targeted only at an identified series of behaviours. We recommend prioritising consumer protection recommendations (internal dispute resolution standards and a digital platforms ombudsman) before any competition recommendations, given they are more likely to benefit Australian consumers and do not need legislation to be established.

Comments on international alignment

International alignment is a worthy policy goal. It is one possible way to reduce the costs associated with Australia's regulatory regime, and can better enable cross-border trade with major trading partners.

However, international regulatory developments impacting digital markets - including the European Union's Digital Markets Act (DMA) and Digital Services Act (DSA) - are subject to many misunderstandings in Australia. Some have argued that the passage of this legislation alone is sufficient justification for Australia, without considering the downsides for the Australian economy.

Many renowned academics and experts have expressed concerns about the direction represented by ex-ante regulation in Europe.[19] A growing body of research and commentary recognises that digital ecosystems and digital markets are not sufficiently understood. For example, research is identifying problematic restrictions around data or self-preferencing in the DMA.[20] While there is much interest in the European Union's approach, other major markets are taking different approaches and there is no international consensus.

There can be unintended consequences in regulating markets and products before being able to properly understand the public policy problem, and the best solutions. There can be benefits for countries like Australia in waiting to understand the consequences of this regulation, before copying it. The Australian economy differs in many ways from our trading partners like the EU, the UK, the US and Japan. With GDP growth expected to slow to 1.6 per cent this year[21], Australia should not miss opportunities to attract inbound investment and innovation which improves productivity and living standards.

---

[19] See for example, 'Can the EU Regulate Platforms Without Stifling Innovation?' (March 2021), Harvard Business Review article by Carmelo Cennamo and D. Daniel Sokol; 'Digital Platforms and Antitrust' (22 May 2020), Geoffrey Parker, Georgios Petropoulos and Marshall Van Alstyne, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3608397; and 'Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act' (1 December 2021), European Law Review article by Pinar Akman. Available https://ssrn.com/abstract=3978625.

[20] See for example, 'EU Closes in on Regulating Big Tech with Digital Markets Act' (13 January 2022), Insights@Questroom blog post by Marshall Van Alstyne. Available: https://insights.bu.edu/techtarget-eu-closes-in-on-regulating-big-tech-with-digital-markets-act; 'Can the EU Regulate Platforms Without Stifling Innovation?' (March 2021), Harvard Business Review article by Carmelo Cennamo and D. Daniel Sokol. Available: https://hbr.org/2021/03/can-the-eu-regulate-platforms-without-stifling-innovation; and 'Digital Platforms and Antitrust' (22 May 2020), Geoffrey Parker, Georgios Petropoulos and Marshall Van Alstyne. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3608397.

[21] IMF, *IMF Executive Board Concludes 2022 Article IV Consultation with Australia*, https://www.imf.org/en/News/Articles/2023/01/26/pr2316-imf-executive-board-concludes-2022-article-iv-consultation-with-australia