Open
Web Advocacy

OWA - Australia Treasury - A New Digital Competition Regime Response

VERSION 1.0

Open Web Advocacy
contactus@open-web-advocacy.org

1. Table of Contents

2. Introduction

We would like to commend the Treasury for its thorough and well-considered proposal. It is clear, insightful, and exactly what Australia needs to restore fair and effective competition in digital ecosystems. It is obvious that the Treasury is diligently following the work of their counterparts in the UK and the EU.

We particularly appreciate the Treasury's focus on addressing the following anti-competitive behaviours:

- Anti-competitive self-preferencing
- Anti-competitive tying
- Impediments to consumer switching
- Restrictions on interoperability that limit effective competition
- Unfair treatment of business users
- Lack of transparency

We are excited about the opportunity this creates to enable fair competition between browsers and between web apps and native apps.

At present, mobile app stores face little to no genuine competition. The web, which should be a viable alternative, is actively restricted from competing on equal terms. This is in stark contrast to desktop computing, where approximately 70% of user activity takes place within a browser, largely due to the absence of a gatekeeper tax and browsers having access to the necessary APIs on desktop, which they are denied on mobile.

Gatekeepers wield vast power due to the security model that these devices are built on. Traditionally, on operating systems such as Windows, macOS and Linux, users can install any application they want, with no interaction from the operating system gatekeeper, either by the business or the end user. Users can then grant these programs the ability to do anything they desire.

Locking down what applications can do, such as restricting which APIs they can access behind user permissions, is not by itself anti-competitive and can bring legitimate security advantages. However, the manner in which it has been implemented on mobile devices is both self-serving and in its current form, significantly damages competition.

Web Apps have a number of properties that allow them to solve this critical problem. They are run in the security of the browser's sandbox, which even Apple admits is "orders of magnitude more stringent than the sandbox for native iOS apps.". They are truly interoperable between operating systems. They don't require developers to sign contracts with any of the OS gatekeepers. They are capable of incredible things and 90% of the apps on your phone could be written as one today.

> *"While Apple currently makes an estimated $64 billion a year from its App Store and tells The Verge it has computer automation, proprietary review tools, huge volumes of internal data, and a dedicated "Discovery Fraud team" of humans at its disposal, a single person on a laptop in his living room is finding egregious scams that Apple continues to host, and I was able to use his basic technique to do the same thing.* ***As Apple faces down hearings in Congress and lawsuits in court, its argument that it needs to maintain total control over the iPhone app ecosystem to keep users safe doesn't mesh with the obvious examples of grift that anyone can easily find.****"*
>
> Sean Hollister - The Verge (April 2021)
> *(emphasis added)*

In certain cases, in particular browsers, gatekeepers will need to delegate the task of protecting the user and the OS to competent third-parties. Thus, the primary security measure for browsers is vetting which browser vendors get the relevant access and revoking it if the browser vendor is significantly incompetent or malicious.

> *"In the end, Apple deploys privacy and security justifications as an elastic shield that can stretch or contract to serve Apple's financial and business interests."*
>
> DOJ Complaint against Apple

Australia is joining the EU, UK, and Japan in rebuilding fair competition in digital markets, allowing browsers to compete on a level playing field and enabling web apps to fairly compete with rival native applications. This presents a pivotal opportunity for Australia to reshape the mobile software landscape and reestablish the web as a strong, open, and truly interoperable alternative, and deliver opportunities for Australian businesses for decades to come. Moreover, via these changes, Australian consumers will benefit from cheaper, higher-quality, more interoperable, more secure, and more private software.

3. Answers to Questions

3.1. The Proposed Framework and Legislative Approach

3.1.1. Q1: Major Challenges

> *"1. Are there any major implementation challenges associated with the proposed framework?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

There are two primary issues that must be considered, namely the burden on smaller companies and non-compliance.

3.1.1.1. Burden on Smaller Companies

The legislation must avoid placing a heavy burden on smaller and medium businesses. This can be done by only applying it to the largest of tech companies, whose scale and entrenched market power justify increased costs to comply with the regime. Companies who are not considered "gatekeepers" or having "strategic market status" should have no obligations to comply under this regime.

We're glad to see that the Treasury has taken this into account and built it into the framework.

3.1.1.2. Non-Compliance

Large, well-funded tech giants with significant legal and lobbying power may resist compliance and actively challenge the regulations.

The regulator will face complex, highly technical, and nuanced issues, making it easier for gatekeepers to present misleading yet seemingly reasonable arguments to avoid compliance.

We have documented what we believe to be extensive non-compliance by Apple in relation to browsers and web apps.

To effectively enforce the regime, the department will require a large number of technically proficient staff. Funding for this could come from fees or levies imposed on gatekeepers. Additionally, the department should seek input and technical expertise from external stakeholders.

Gatekeepers are likely to engage in aggressive lobbying efforts to weaken or block the regulation, potentially leveraging threats to reduce investment in Australia.

> *"'Apple has been able to intimidate and use a lot of money' to kill legislation"*
> Arizona Rep. Regina Cobb

Moreover, they may implement strategies that appear to comply on the surface while undermining the intent of the obligations. These tactics could be highly sophisticated or as straightforward as deliberately slowing down processes at each stage.

To address this, the legislation should include a mechanism similar to the Digital Markets Act's (DMA) specification process, allowing the ACCC to investigate and clarify how a particular gatekeeper must comply.

The Commission is currently conducting two such specification proceedings (one into third-party devices and one into interop requests) and the Treasury should study these to evaluate where such a power might fit into their regime.

Any enforcement process should allow the ACCC to revisit and refine measures if they prove ineffective. This is also part of the DMA.

> *"In respect of proceedings pursuant to paragraph 2, the Commission may,* ***upon request or on its own initiative, decide to reopen them where****:*
>
> *(a) there has been a material change in any of the facts on which the decision was based; or*
>
> *(b) the decision was based on incomplete, incorrect or misleading information; or*
>
> *(c)* ***the measures as specified in the decision are not effective****."*
> Digital Markets Act

The Treasury should incorporate a version of these two critical passages related to circumvention into the Act:

> *"13(4) The gatekeeper shall not engage in any behaviour that undermines effective compliance with the obligations of Articles 5, 6 and 7 regardless of whether that behaviour is of a contractual, commercial or technical nature, or of any other nature, or consists in the use of behavioural techniques or interface design."*

Digital Markets Act

> *"13(6) The gatekeeper shall not degrade the conditions or quality of any of the core platform services provided to business users or end users who avail themselves of the rights or choices laid down in Articles 5, 6 and 7, or make the exercise of those rights or choices unduly difficult, including by offering choices to the end-user in a non-neutral manner, or by subverting end users' or business users' autonomy, decision-making, or free choice via the structure, design, function or manner of operation of a user interface or a part thereof"*

Digital Markets Act

Finally, in cases of proven systematic non-compliance, the legislation must include powerful additional enforcement powers. The DMA includes such a provision, and the Treasury should consider incorporating a similar mechanism into their legislation.

> *"The Commission should investigate and assess whether additional behavioural, or, where appropriate, structural remedies are justified, in order to ensure that the gatekeeper cannot frustrate the objectives of this Regulation by systematic non-compliance with one or several of the obligations laid down in this Regulation. This is the case where the Commission has issued against a gatekeeper at least* ***three non-compliance decisions within the period of 8 years****, which can concern different core platform services and different obligations laid down in this Regulation, and if* ***the gatekeeper has maintained, extended or further strengthened its impact in the internal market****, the economic dependency of its business users and end users on the gatekeeper's core platform services or the entrenchment of its position. A gatekeeper should be deemed to have maintained, extended or strengthened its gatekeeper position where, despite the enforcement actions taken by the Commission, that gatekeeper still holds or has further consolidated or entrenched its importance as a gateway for business users to reach end users.*
>
> ***The Commission should in such cases have the power to impose any remedy, whether behavioural or structural, having due regard to the principle of proportionality****."*

Digital Markets Act

Ensuring that, in the event of non-compliance, tailored behavioral or structural remedies can be imposed will deter gatekeepers from attempting to circumvent the legislation. Moreover, if they do attempt to evade their obligations, the ACCC must have the authority to swiftly and effectively intervene, ensuring that any breaches are addressed. The ACCC

requires robust enforcement powers, an unequivocal "big hammer", that compels compliance and makes long-term defiance an unviable option.

3.1.2. Q2: Appropriate Scope?

> *"2. Is the proposed scope of digital platform services targeted appropriately? Are there any digital platform services that should be added or removed?"*
> *A new digital competition regime - The Australian Government the Treasury*

The scope and list of digital platform services eligible for regulation under this legislation appear well-considered and reasonable.

Virtual assistants should encompass both voice assistants and AI assistants integrated into operating systems. It is essential that third parties can compete with gatekeepers in the provision of virtual assistants on a level playing field, without the gatekeepers having an unfair advantage

It is crucial to consider how user flows to third-party apps within operating systems can be influenced or manipulated across various OS interfaces. The focus on anti-competitive self-preferencing, impediments to consumer switching and restrictions on interoperability that limit effective competition is correct here.

Interoperability should be a core focus, ensuring seamless communication between devices, peripherals, and applications that function across multiple platforms. A strong focus on interoperability will drive competition and lower costs for both businesses and consumers.

3.1.3. Q3: Initial Targets for Designation

"3. Do you agree with the proposal that app marketplaces, ad tech services and social media services should be prioritised as the first services to be investigated for designation under the framework?"

A new digital competition regime - The Australian Government the Treasury

Competition in mobile app markets is fundamentally flawed, hindering fair and open innovation.

On iOS, Apple restricts browsers from using their own engines, effectively eliminating meaningful competition and reinforcing its control over the browsing experience. On Android, Google leverages agreements such as MADA to suppress rival browsers, maintaining its dominance and limiting consumer choice.

Likewise, the web and web-based applications are unable to compete effectively with app stores under the current conditions. Mobile operating systems impose restrictions on web app functionality, give preferential treatment to native apps, and restrict browser competition, creating an uneven playing field that entrenches the dominance of app stores.

If the web were allowed to compete on equal terms, it could emerge as a powerful, open, and interoperable alternative within the mobile ecosystem. A truly competitive web environment would drive innovation, expand consumer choice, and reduce reliance on closed app store ecosystems controlled by a few dominant players. This would bring significant benefits to both Australian companies and consumers, allowing for cheaper, higher quality, more private and more secure software delivered by the web. Gatekeepers would not have an opportunity in this distribution system to block rivals nor charge a 30% fee.

Given these long standing competition problems, we believe the primary initial focus should be on operating systems and app distribution to ensure fair competition and greater opportunities for innovation.

For operating systems, the focus should include:

- **Access to essential OS software and hardware features**, subject only to security measures that are strictly necessary, proportionate, and justified to protect the integrity of the operating system.

- **Fair competition for browsers**, including the ability to install and manage web apps using their own engines without undue restrictions.

- **Equal ease of application installation**, ensuring that all apps, regardless of third-party origin, can be installed with comparable ease and lack of friction.

- **Non-preferential treatment**, prohibiting gatekeepers from giving undue advantages to their own apps or services over those of competitors.

- **Interoperability**, enabling third party services and apps to work with the OS seamlessly and to the same level of integration as the gatekeepers own apps.

  This should include:
  - Browsers not being limited in their ability to contest the operating system by providing access to hardware/software features to websites and web apps, including features the gatekeeper does not provide.

  - Interoperability for close-range wireless file transfer services (such as AirDrop, Nearby Share) and other competitors to enable universal file sharing between devices.

  - The ability for third-party providers to contest operating system backup services such as Apple's iCloud and Google One Backup as well as data syncing, and application data storage.

  - The ability for hardware manufacturers to build physical devices that can interface with the operating system.

For app distribution, the focus should include:

- **Direct distribution**, allowing developers to distribute apps without being forced through a gatekeeper's store, either via third-party app stores or directly from their own websites. This can be subject to strictly necessary, proportionate and justified security measures.

- **Seamless app distribution switching**, enabling users to choose and switch app distribution sources freely. Specifically there should be an operating system prompt to enable a user to switch the distribution source to either another app store or the developers website directly, without having to uninstall and reinstall the app.

- **Web app installation**, ensuring web apps can be installed just as easily as native apps. Specifically we believe that Safari should be obligated to implement a feature called install prompts.

- **Elimination of friction and scare tactics**, preventing unnecessary warnings or barriers that discourage alternative distribution methods.

- **Equal access to payment and subscription management**, ensuring developers can use their preferred payment systems without disadvantage regardless of the source or type of their application. This must provide equivalent ease, integration, and biometric authentication as Apple Pay or Google Pay.

3.2. Designation

3.2.1. Q4: Benefits and Risks from other International Approaches

> *"4. What are the benefits and risks of the various designation approaches taken or proposed internationally?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

Both the UK's Digital Markets, Competition and Consumers (DMCC) Act and the EU's Digital Markets Act (DMA) should be carefully studied. Since the DMA has been in effect for a longer period, it offers more concrete lessons for the Australian Treasury.

The primary risks include non-compliance, the potential exclusion of certain digital platforms from regulation due to the designation process rules and the risk of imposing undue compliance burdens on smaller companies if designation thresholds are set too low.

A critical decision for the Australian government is whether services such as Edge, watchOS, VisionOS, macOS, and iMessage (which are not covered by the DMA) should be covered under the legislation.

For large gatekeepers, all derivative operating systems should be treated as a single entity, particularly when they bind accounts and share an app store. Even if some of these sub-platforms have lower market shares individually, excluding them could lead to regulatory fragmentation.

For example, allowing fair browser competition on iOS and macOS, but not on other Apple devices like wearables, would create inconsistencies in what is available. This would

enable gatekeepers to increase friction and strengthen user lock-in rather than genuinely opening up competition.

An under-resourced enforcement team, lacking an adequate number of legal experts, economists, and high-level technical specialists, should also be considered a key implementation risk for the legislation.

3.2.1.1. Gaps in the Designation Process

Another issue is how services that are important for consumers but not necessarily critical for businesses are designated. A key example is iMessage, which was not designated under the DMA for this reason.

This could be addressed by modifying the designation criteria so that either consumer usage or business usage thresholds are sufficient to trigger automatic designation, rather than requiring both. This OR approach, rather than the current AND requirement used by the DMA, would prevent key services from slipping through regulatory gaps.

In all cases, the ACCC should retain the flexibility to apply a proportional and common-sense approach when determining which services should fall under the regime.

3.2.2. Q5: Quantitative Thresholds and Qualitative Factor

> *"5. Would the proposed quantitative thresholds and qualitative factors appropriately target entities that are significant to Australian consumers, businesses and the economy? What other quantitative thresholds or qualitative factors should be considered to ensure they are adaptable to a variety of circumstances? How could any risks of over and under capture be mitigated?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

This legislation must ensure that compliance obligations are placed only on the largest companies that wield significant market power within relevant digital markets.

As stated in the Australian Treasury's proposal:

> *"Under the proposed framework, quantitative thresholds would act as the primary criteria to ensure the regime only targets large digital platforms with critical positions in the Australian economy."*
>
> *A new digital competition regime - The Australian Government the Treasury*

To avoid unintentionally subjecting widely used but non-profit projects (such as Linux) to regulation, the framework should include a quantitative revenue threshold at the parent

company level. This would ensure that only highly profitable and market-dominant entities are covered.

Once a parent company meets the revenue threshold, a platform should qualify if it is used by either a sufficiently large number of Australian consumers or a sufficiently large number of Australian businesses, not necessarily both. This approach ensures that platforms with significant market influence are included, even if their primary user base is concentrated in one sector. Requiring both consumer and business thresholds to be met, as seen in the DMA, is a flaw that should be avoided.

A good reason for setting the revenue threshold at the **global parent company level** rather than just individual arms is that large multinational tech companies could structure their operations in a way that minimizes their reported revenue in individual organizational units. Setting it at the global parent company level prevents the gatekeepers from **artificially segmenting their financial reporting** to avoid regulation, even if they have substantial market influence.

Additionally, in some cases, interconnected digital properties within a company should be grouped together for regulatory purposes. For instance, iOS, iPadOS, watchOS, and VisionOS should be treated as a single entity to prevent fragmentation and lock-in. This is particularly true in this case as these all share Apple's app store and identity system.

We believe that framework should be set up in a manner that guarantees the following digital properties are included:

Operating Systems

- **iOS** (including iPadOS, watchOS, visionOS, tvOS)

  With a **market share exceeding 60%**, Apple's tightly integrated ecosystem disadvantages apps that cannot be distributed across its platforms. **Restrictions on third-party app installation, limited web app support, and barriers to interoperability** further hinder competition.

- **Windows**
  As the dominant PC operating system, ensuring fair competition in software and services is crucial.

- **MacOS**
  With **31% of Australian laptop owners using MacBooks**, including a significant

share of **high-income consumers and business decision-makers**, Apple's tightly integrated ecosystem limits competition.

- **Android** (including Android TV, Wear OS)
  With a **significant market share**, Google's control over **licensing, app distribution, and default services** creates barriers for competition and limits consumer choice.

Browsers

- **Chrome**
  Dominant browser (especially on desktop) & default browser on most Android devices

- **Safari**
  The default and dominant browser on iOS (90%+ market share), with restrictions on third-party browser engines and limitations on web app functionality, preventing fair competition and alternative browser development.

- **Edge**
  The default browser on Windows, with deep integration into the OS and ongoing anti-competitive practices, including aggressive nudging and restrictions that steer users away from alternatives. Microsoft's preferential treatment of Edge in system features further distorts competition.

App Marketplaces

- **Google Play**
  The dominant app store on Android.

- **Apple AppStore**
  The only app store on iOS (in Australia).

The DMA failed to designate various Android and iOS subvariants (except for iPadOS) and Microsoft Edge. The Australian act should be structured to ensure that these interconnected components of major tech ecosystems are properly covered.

3.2.3. Q6: Adjusted Quantitative Thresholds

> *"6. For quantitative thresholds, the proposed regime would draw on the threshold levels used by international regimes, adjusted to reflect the size of the Australian economy and population. Is this approach appropriate?"*
> *A new digital competition regime - The Australian Government the Treasury*

This approach seems reasonable and is a good starting point for a design.

3.2.4. Q7: Automatic Quantitative Thresholds

> *"7. Are there any circumstances where quantitative thresholds may be sufficient by themselves to inform a designation decision and if so, what circumstances would they be?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

We believe that as with the DMA, the quantitative metrics should be chosen such that if they are met there is **a presumption that the service should be designated**. The ACCC should have the ability to choose not to designate a service if they believe it is not sufficiently significant to both Australian consumers and Australian businesses.

For services that are below these metrics, the ACCC should still have the power to designate it but they would need to be satisfied that the service was sufficiently significant to either Australian consumers or Australian businesses.

The DMA includes a well-structured provision allowing services that do not meet quantitative thresholds to still be designated under specific conditions. We recommend that the Australian Treasury consider incorporating a similar mechanism to prevent key services from escaping oversight:

> *"1. **An undertaking shall be designated as a gatekeeper if**:*
>
> *(a) it has a significant impact on the internal market;*
>
> *(b) it provides a core platform service which is an important gateway for business users to reach end users; and*
>
> *(c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.*
>
> [...]
>
> *8. The Commission shall designate as a gatekeeper, in accordance with the procedure laid down in Article 17, any undertaking providing core platform services that meets each of the requirements of paragraph 1 of this Article, but **does not satisfy each of the thresholds in paragraph 2 of this Article**.*

For that purpose, the Commission shall take into account some or all of the following elements, insofar as they are relevant for the undertaking providing core platform services under consideration:

(a) the size, including turnover and market capitalisation, operations and position of that undertaking;

(b) the number of business users using the core platform service to reach end users and the number of end users;

(c) network effects and data driven advantages, in particular in relation to that undertaking's access to, and collection of, personal data and non-personal data or analytics capabilities;

(d) any scale and scope effects from which the undertaking benefits, including with regard to data, and, where relevant, to its activities outside the Union;

(e) business user or end user lock-in, including switching costs and behavioural bias reducing the ability of business users and end users to switch or multi-home;

(f) a conglomerate corporate structure or vertical integration of that undertaking, for instance enabling that undertaking to cross subsidise, to combine data from different sources or to leverage its position; or

(g) other structural business or service characteristics."

3.2.5. Q8: Basis of Initiating Investigations

"8. The proposed framework provides the relevant minister the ability to direct the ACCC to conduct designation investigations and the ACCC to also self-initiate designation investigations. On what basis should the ACCC be able to self-initiate investigations?"

A new digital competition regime - The Australian Government the Treasury

We believe there are strong justifications for allowing the ACCC to self-initiate designation investigations under the proposed digital competition regime.

Digital markets evolve rapidly, and delayed intervention can lead to lasting harm. If the ACCC must wait for ministerial direction before launching an investigation, anti-competitive practices may persist unchecked, damaging competition and stifling

innovation. Self-initiated investigations allow the ACCC to act proactively rather than reactively, ensuring timely enforcement.

Requiring ministerial approval for every investigation also introduces the risk of political interference. Large digital platforms wield significant lobbying power, and a ministerial-only initiation process could result in delays or even prevent necessary investigations altogether. An independent ACCC ensures that enforcement decisions are based on economic evidence, not political considerations.

Other jurisdictions with similar digital competition frameworks, such as the EU (under the DMA) and the UK (under the DMCC Act), grant their regulators the ability to self-initiate investigations. This approach ensures that regulatory bodies can effectively enforce compliance without external constraints that may weaken their ability to act.

Without self-initiated investigations, the ACCC's ability to administer and enforce this regime effectively and in a timely manner would be significantly compromised.

3.2.6. Q9: Non-Confidential Summary of Designation Investigation Findings

> *"9. Should the ACCC be required to publish a non-confidential summary of its designation investigation findings?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

It is crucial that the ACCC publishes a non-confidential summary of its designation investigation findings to ensure trust, transparency, and stakeholder engagement in the regulatory process.

Public confidence in the ACCC's decisions depends on transparency. If designation investigations occur behind closed doors without accessible findings, there is a risk of distrust, skepticism, and accusations of bias or undue influence. Publishing a non-confidential summary allows businesses, policymakers, the public, and organizations such as OWA to understand the ACCC's reasoning, the evidence considered, and the rationale behind any decision. It also ensures that powerful digital platforms cannot use secrecy or confidential lobbying to undermine investigations without public scrutiny.

Transparency is not just about trust, it also improves the quality of decision-making. Third parties, such as competitors, industry experts, consumer advocacy groups, and academics, may have additional evidence, insights, or concerns that the ACCC has not yet considered. If findings remain unpublished, important stakeholders may be unaware of investigations that could impact them, limiting their ability to contribute valuable

information. A public process ensures that the ACCC does not rely solely on information provided by gatekeepers themselves, which may be self-serving.

Both the EU's Digital Markets Act (DMA) and the UK's Digital Markets, Competition and Consumers Act (DMCC) incorporate public consultation and stakeholder engagement as part of their regulatory processes. They publish findings, invite public comment, and hold industry conferences to gather input from a wide range of perspectives. Australia should follow this global best practice to ensure its digital competition regime is equally robust, fair, and evidence-based.

For the integrity and effectiveness of the designation process, the ACCC must publish non-confidential summaries of its findings, ideally at multiple steps throughout its process. The timeline and status of an investigation must be clear to the public at all times.

Both the UK's designation process and the EU's various investigations are good examples of this done well.

3.2.7. Q10: Designation Period of 5 Years

> *"10. The digital competition regime proposes designation to last for up to 5 years. Is this time period appropriate?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

The proposed five-year designation period appears reasonable. However, there should be a clear, easy and straightforward process for extending the designation if the original conditions still apply. In effect, the designation should remain in place indefinitely for as long as the service retains its critical position in the Australian digital economy.

3.3. Obligations and Exemptions

3.3.1. Q11: Cost, Benefits and Risks of Proposed Framework

> *"11. What are the costs, benefits and risks of the proposed framework comprising both broad and service-specific obligations? How can any costs or risks be mitigated? How should broad and service-specific obligations interact?"*
> *A new digital competition regime - The Australian Government the Treasury*

The proposed framework of combining broad and service-specific obligations appears to be a reasonable and well-balanced approach. The broad rules are well-structured and necessary, and we fully support them. In particular, this framework improves upon the DMA, which lacks a clear self-preferencing rule that is independent of anti-circumvention measures.

> *"For example, broad obligations would target:*
> - *Anti-competitive self-preferencing*
> - *Anti-competitive tying*
> - *Impediments to consumer switching*
> - *Restrictions on interoperability that limit effective competition*
> - *Unfair treatment of business users*
> - *Lack of transparency"*
>
> *A new digital competition regime - The Australian Government the Treasury*

However, broad obligations alone are not sufficient. Different digital services operate in distinct ways, and the obligations placed on them should reflect those differences. For example, the regulatory requirements for an operating system would necessarily be different from those for a search engine. Service-specific obligations are a good way to address the unique ways in which different platforms can exert market power and limit competition.

Given that gatekeepers are likely to develop new tactics to avoid compliance and that it is hard for the ACCC to anticipate what these strategies may be, it is also critical that the legislation includes mechanisms similar to the DMA's specification proceedings and systematic non-compliance powers. This ensures that regulators can refine and enforce obligations as needed, on a gatekeeper by gatekeeper basis, rather than being constrained by predefined rules that may become ineffective or be circumvented.

3.3.2. Q12: Additional Types of Anti-Competitive Conduct

> *"12. Are there any additional types of anti-competitive conduct common across different digital platform services the government should consider when drafting broad obligations?"*
> *A new digital competition regime - The Australian Government the Treasury*

The list outlined in the previous question effectively covers the key broad obligations. However, there are numerous service-specific obligations that are equally important and should be included to ensure comprehensive regulation across different digital platform services that we covered in question 14.

3.3.3. Q13: Additional Anti-Competitive Conduct for App Marketplaces, Ad Tech Services, Social Media Services

> *"13. For app marketplaces, ad tech services and social media services, are there any additional types of anti-competitive conduct in the supplies of these services the government should consider when drafting service-specific obligations?"*
> *A new digital competition regime - The Australian Government the Treasury*

For app marketplaces we believe a number of additional obligation are necessary:

- Designated app marketplaces should **not be able to prohibit browsers from using their own browser engines.**

- Designated app marketplaces should only be able to apply rules to browsers on strictly necessary, proportionate and justified security grounds.

- Designated app marketplaces should not be able to inhibit the degree to which browsers and the web apps they power can compete with that app marketplace as well as the broader operating system and its native ecosystem. This includes preventing any restrictions that limit the functionality, performance, or integration capabilities of web apps in ways that disadvantage them relative to native apps.

- Designated app marketplaces should not prevent businesses from and should enable businesses to distribute web apps directly via the app marketplace. Conditions designed to force developers to ship native apps should be removed.

- Designated app marketplaces should not prevent browsers from bringing their own browser extensions architecture that is distributed directly by the browser rather than via that app marketplace.

- Designated app marketplaces must allow "**app distribution switching**", to allow both users and developers to easily switch between app stores or direct from the developer.

3.3.4. Q14: Additional Obligations

> *"14. Are there particular obligations or design features in similar regimes in international jurisdictions the government should consider including or not including in a regime in Australia?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

There are a number of obligations that we believe the Treasury and the ACCC must facilitate via this legislation. It is critical that there is a clear unavoidable path to implementation.

3.3.4.1. Software and Hardware API Access

The act should include an equivalent to the DMA's Article 6(7) which obligates designated operating systems to share all software and hardware APIs with third-parties free of charge, subject to strictly necessary, proportionate and duly justified security measures to protect the integrity of the operating system.

This is a critical component of opening up fair competition on operating systems where gatekeepers currently restrict critical functionality to themselves and their own apps.

3.3.4.2. Browser Engines

The act should mandate that operating systems and app stores are not allowed to prohibit browsers using any browser engine that they choose. This is already law in the EU and Japan, is part of the UK SMS proceeding into Apple and was discussed in the ACCC's fifth report into digital platforms.

> *"Mandatory use of WebKit impedes fair and equitable competition between Safari and third-party browsers [...]*
>
> *Platform operators that provide OS of a certain size or larger shall be prohibited from requiring app developers to use OS providers' own browser engines"*
>
> Japan's HDMC

> *"In particular, **each browser is built on a web browser engine**, which is responsible for key browser functionality such as speed, reliability and web compatibility. **When gatekeepers operate and impose web browser engines, they are in a position to***

> ***determine the functionality and standards that will apply not only to their own web browsers, but also to competing web browsers and, in turn, to web software applications.*** *Gatekeepers should therefore not use their position to require their dependent business users to use any of the services provided together with, or in support of, core platform services by the gatekeeper itself as part of the provision of services or products by those business users."*
>
> Digital Markets Act

> *"The code of conduct for mobile OS services could require Designated Digital Platforms to allow third-party browser engines to be used on their mobile OS. This could allow third-party providers of browsers and web apps to compete on their merits."*
>
> ACCC - Digital Platform Services Inquiry 2020-25

3.3.4.3. Web Apps

It is critical to web app competition that browsers have the ability to install web apps, and be able to manage web apps they have installed, using their own browser engine.

> *"A number of the above requirements would need to be complemented by ensuring Apple: (i) permits browser apps to use alternative browser engines; and (ii) enables browser vendors using alternative browser engines to install and manage progressive web apps."*
>
> UK's SMS Investigations into Apple's and Google's mobile ecosystems

This enables browsers to compete in the functionality, performance, security and privacy in the provision of web apps. For this to be truly effective browsers must have sufficient access to all software and hardware APIs they might reasonably require to allow web apps to compete fairly and effectively with their native counterparts.

3.3.4.4. Install Prompts for Safari

In order for Web Apps to fairly contest the iOS App Store, they need to be as visible as native apps. Apple has progressively added features to iOS Safari to push users towards native apps on their app store, however refuses to add the equivalent feature for Web Apps: Install Prompts, despite incredible pressure from developers over many years.

Install Prompts are the essential missing feature for Web Apps, without which Web Apps will not be able to compete with native apps.

Currently the installation of Web Apps in Safari is completely hidden away under an awkward multi-step process which the user must access through the "share" menu. The

install process for Web Apps are so obscured in Safari that the majority of users are unaware of their existence.

In order for Web Apps to be able to fairly contest Apple's native app ecosystem, and to enable businesses to take over the extensive advantages Web Apps have to offer (including Security/Interoperability/Cost) **Apple must be compelled to provide an effective implementation of Install Prompts from within Safari.** Apple will not provide this without regulatory intervention.

As such, we believe the following remedy is appropriate, justified and proportionate to allow Web Apps to compete with the OS's apps, app store, services and apps delivered via their app store. We ask that the Treasury consider including it:

> *"A requirement for Apple to implement Install Prompts for iOS Safari."*

We cover this in more detail in section "3.3.1. Install Prompts" in our previous submission "OWA - Mobile Browsers and Cloud Gaming - Response to Working Papers 1-6".

3.3.4.5. Feature Parity between Web Apps and Native Apps

Apple has repeatedly claimed that Web Apps are the alternative distribution method for apps in their mobile ecosystem.

> *"QUESTION: Apple is the sole decision maker as to whether an app is made available to app users though the Apple Store, isn't that correct?*
> *REPLY: If it's a Native App, yes sir, if it's a Web App no."*
>
> *Tim Cook - Speaking to US* Congress

> *"Web browsers are used not only as a distribution portal, but also as platforms themselves, hosting "progressive web applications" (PWAs) that eliminate the need to download a developer's app through the App Store (or other means) at all."*
>
> Apple's Lawyers - Court Filing in Australia

> *"For everything else there is always the open Internet. If the App Store model and guidelines are not best for your app or business idea that's okay, we provide Safari for a great web experience too."*
>
> Apple App Store Guidelines

Even if the various regulators compel Apple to allow third party browsers using their own engine to power Web Apps, only Apple can really build and maintain the integration into the many surfaces that apps on iOS inhabit.

These surfaces include (but are not limited to):

- The Web App icons, text, badging on the homescreen
- The settings/permissions page of each Web App
- Notifications from the Web App
- Menus to uninstall or move the Web App
- Various search menus
- Various defaults (i.e. default email client, default map)

Only Apple (the developers of iOS) have control over each of these surfaces. We are concerned that if Apple became nervous as to the potential for Web Apps to undermine its app store that Apple might take steps to lessen Web Apps appeal via these surfaces. That is, while allowing competition in browser engines powering Web Apps solves most issues, i.e. functionality that takes place within the Web App, it is important that Apple is not allowed to make Web Apps second tier citizens via their control and design of the integration into these surfaces.

The aim here is to allow browsers to facilitate Web Apps being true substitutes and competitors to native apps distributed via Apple's app store. This should not be undermined by Apple.

The CMA in their mobile ecosystems study noted that Apple has an incentive to prevent Web Apps from competing and as far back as 2011 Apple executives were concerned about the threat the Web presents to their app store.

> *"Food for thought:* ***Do we think our 30/70% split will last forever?*** *While I am a staunch supporter of the 30/70% split and keeping it simple and consistent across our stores, I don't think 30/70 will last unchanged forever.* ***I think someday we will see a challenge*** *from another platform or* ***a web based solution*** *to want to adjust our model"*
>
> Internal Apple Emails
> (emphasis added)

With all of these facts in mind, we believe it is reasonable and proportional to have a obligation that:

> *"Where feature parity between Web Apps and native apps is possible, Apple must technically enable it and it should not be artificially prevented either by OS rules or OS design. Apple must not self-preference their own apps, apps sold via their app store or their own services over Web Apps."*

3.3.4.6. Obligate Google to Share WebAPK Minting

To our knowledge WebAPK minting is the only functionality on Android devices that are not available to other browser vendors (excluding Samsung). This prevents these third-party browser vendors from competing in the provision of Web App functionality, performance, stability, security and privacy.

WebAPKs remaining exclusive to Chrome is anti-competitive, restricts browser competition and damages the viability of Web Apps because:

1. Other browsers can not compete to provide better functionality for Web Apps

2. Provides an unfair advantage to Chrome on Android through increased engagement from Web Apps.

3. Damages adoption of Web Apps by making them not work properly in other browsers.

Google publicly stated 7 years ago that they were working on sharing this functionality with other browsers but there has been no progress. We believe that they should be forced to share this functionality with other browsers. Google should be able to set strictly necessary, proportionate and justified security conditions attached to obtaining access to this API.

It is essential that Google allows competing browsers to properly install Web Apps. The simple, timely solution to this is for Google to make the existing Play Services API available to third-party browsers, allowing them to use the same WebAPK minting service that Chrome enjoys access to.

Google is already obligated under the Digital Markets Act to make this functionality available to third-party browsers making proportionality arguments stronger.

As such we believe the Treasury and the ACCC should consider ensuring that this obligation can be facilitated by the legislation:

> *"A requirement for Google to share WebAPK Minting with third-party browsers on Android subject to strictly necessary, proportionate, and justified security measures. This sharing should enable browsers on Android to install Web Apps and manage the Web Apps they have installed using their own browser engine."*

3.3.4.7. Prevent Google from using MADA for Chrome Placement and Default

Google uses its licensing of the Google Play store, other google properties and a series of complex revenue sharing agreements to push Chrome on Android.

The UK's CMA is also considering prohibiting this behavior.

> *"A requirement that prevents Google from making payments to OEMs and its licensing of its first-party apps and proprietary APIs conditional upon the prominent display and specific default-settings for Google Chrome on Android devices."*
>
> SMS Investigations into Apple's and Google's mobile ecosystems - Invitation to Comment

We fully support the remedy.

We support remedies that would prohibit Google from bundling Chrome's placement and default status with Google Play, whether directly, through fees, revenue-sharing agreements, or other such means.

We believe that any countervailing benefits from the revenue the OEM's receive are insufficient to offset the harm caused by the suppression of browser competition on Android.

Additionally, we would advocate for banning Google from leveraging its other properties on Android, such as Gmail, as mentioned in the browsers and cloud gaming provisional decision report, to prompt users to switch their default browser to Chrome.

Browsers should compete based on their merits, not on the ability of their vendors to exploit other properties (be it operating systems, operating system in-app browsers, apps, search engines, or app stores) to pressure, manipulate, or coerce OEMs or consumers into adopting their browser.

The Treasury should consider prohibiting this behavior and ensure the legislation has the ability to impose such obligations.

3.3.4.8. Prevent Google from Paying Apple Search Engine Revenue from Chrome on iOS

The Apple-Google agreement to share search engine revenue from Chrome on iOS significantly weakens Google's incentive to compete for browser market share on iOS, bordering on a tacit non-compete arrangement.

The UK's CMA is currently considering prohibiting this behavior:

> *"A requirement for Apple not to enter into agreements with Google where it receives search advertising revenues connected to the use of Chrome on iOS."*
> UK's SMS Investigations into Apple's and Google's mobile ecosystems

We believe that the Treasury should consider prohibiting such behavior in the obligations.

3.3.4.9. App Distribution Switching

Gatekeepers have built their app stores as walled ecosystems, making it nearly impossible for users and developers to leave. To repair over a decade of anti-competitive behavior, we must remove the excessive switching costs and friction that prevent real alternatives. Users have a vast body of apps that are by system design and friction locked into those app stores. App distribution switching is a key method by which this control can be broken.

App distribution switching is the ability for apps to prompt users to change their software distribution source. A clear system prompt would then appear, ensuring that the change occurs only with the user's explicit consent. The new distribution source could be either another app store or the developer directly.

Currently, the only way to switch distribution source is to delete and reinstall the app, a process that is time-consuming and risky due to potential data loss. This practice helps lock users into Google Play and Apple's app store. Friction can be a powerful barrier to competition. By making it difficult for users to switch, gatekeepers can maintain their dominant market position in the distribution of apps even after regulation compels them to allow it due to the vast body of native apps that users have already installed from the gatekeeper's app store.

An example prompt could be: *"'Firefox' would like to switch its distribution source from 'Apple App Store' to 'Mozilla Inc'. Changing this will mean all updates and app review will be performed by 'Mozilla Inc'. Would you like to switch distribution source: YES | NO"*

Gatekeepers, through anti-competitive behavior such as excluding alternative marketplaces and restricting direct downloads, have amassed a vast install base of applications within their ecosystems. As a result, the overwhelming majority of users are locked into these app stores, making it nearly impossible for developers to migrate their existing user base to alternative distribution channels where they could offer better deals, improved functionality, or more consumer-friendly policies. This entrenched dominance creates a severe structural barrier to competition, even when regulations theoretically allow for alternative app distribution.

Without a viable **exit strategy**, developers remain dependent on gatekeeper-controlled ecosystems, unable to transition their users without excessive friction, including forcing them to manually uninstall and reinstall apps, often at the cost of losing data or settings. This friction is not just an inconvenience, it reinforces the gatekeepers' control, ensuring that users and developers have no practical path to alternatives.

To ensure genuine competition in app distribution, **users must be able to seamlessly switch an app's distribution source without needing to delete and reinstall it**. The ability to switch will ensure that users can access better pricing, policies, and features outside of gatekeeper-controlled environments. Without such a safeguard, the regulatory intent of opening up app distribution will remain ineffective, as entrenched market power will continue to prevent meaningful competition from taking root.

We believe that the Treasury should carefully consider this as an obligation for operating systems/app marketplaces.

We write about this more extensively in our Apple DMA Review document

3.3.4.10. AirDrop and Airdrop Alternatives

Currently AirDrop is not interoperable with non-Apple devices, nor is it possible for a third-party to introduce AirDrop like functionality onto iOS.

> *"Apple shall provide effective interoperability with the features for close-range wireless file transfer services.*
>
> *The features for close-range wireless file transfer services allow Apple to offer feature-rich close-range wireless file transfer services, including AirDrop. Close-range wireless file transfers services, such as AirDrop, allow iOS devices to transfer files, such as photos or documents, between nearby devices. Furthermore, close-range wireless file transfer services encompass the ability to pair nearby devices and have access to several communication protocols to transfer files (e.g., P2P Wi-Fi, infrastructure Wi-Fi).*
>
> *Apple shall implement an interoperability solution that provides third parties with access to the same features for close-range wireless file transfer services described in the preceding paragraph as available to Apple, in a way that is equally effective as the solution available to Apple."*
>
> DMA - Public Consultation - Apple - Features for Connected Physical Devices

We are interested in AirDrop alternatives because file sharing is essential for modern apps to function effectively. Many apps rely on seamless data exchange between devices for

collaboration and convenience, but closed systems like AirDrop restrict this capability to a single ecosystem. Open, interoperable file sharing would allow both apps and web apps to work across devices and platforms, enabling users to share files freely and enhancing productivity without being locked into one brand.

The Treasury should consider adding an obligation for operating systems that both AirDrop-like sharing features should be interoperable with other operating systems and that it should be possible for third-parties to introduce replacements to the feature.

Other protocols should be allowed to compete across all platforms to provide improved file-sharing. AirDrop, frequently fails to function reliably, even though it only works on Apple devices. Despite being a core feature marketed for seamless file sharing, persistent connectivity issues, inconsistent performance, and unexplained failures remain common complaints among users. Such an intervention will not only lead to reduce switching costs between the mobile ecosystems but will also provide alternatives for Apple's users for a more reliable and interopable file sharing service.

3.3.4.11. Mobile Backup and iCloud/Google One Alternatives

Currently, there is no competition in the provision of backup services for Android or iOS. Services like iCloud and Google One face no real competitors because gatekeepers do not permit third parties to offer alternative backup solutions.

While providing such services entails significant security and privacy responsibilities, these risks can be effectively managed through appropriate, strictly necessary, and proportionate security measures, primarily focused on identifying and vetting companies offering these services.

The Treasury should ensure that its obligations on operating systems and app marketplaces include a requirement to allow all gatekeeper apps and services to be fairly and effectively contested.

Specifically, there should be an obligation to allow third-party providers to compete in operating system backup services, including Apple's iCloud, Google One Backup, data syncing, and application data storage, ensuring a more competitive and open ecosystem.

A significant number of features are integrated into iCloud (Backup, Files, Photos, Passwords, Find My, Family Sharing, App & Data Syncing), and third-party companies should have the ability to compete on equal footing with gatekeepers, whether by offering individual features or a comprehensive bundle within a single app.

3.3.5. Q15: Benefits and Risks of Exemptions in DMA and DMCC

> *"15. What are the benefits and risks of various international approaches to exemptions (such as the EU's Digital Markets Act and the UK's Digital Markets, Competition and Consumers Act)?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

In some cases, the ACCC may require a mechanism to grant narrow exemptions to specific obligations. The legislation should be designed so that the bar for granting these exemptions is set high, ensuring they are only granted when strictly necessary. However, it should also provide the ACCC with the flexibility to temporarily pause, modify or replace an individual obligation if it is determined that enforcing it as written would cause significant harm to Australian consumers or businesses. When granting an exemption, the ACCC should be required to publish a non-confidential document outlining its rationale to maintain transparency and accountability.

Every effort should be made to keep exemptions as narrow as possible, including the option to partially adjust obligations rather than fully rescinding them.

It is worth noting that the exemption under the DMA is extremely limited:

> *"An exemption pursuant to paragraph 1 may only be granted on grounds of public health or public security."*
>
> Digital Markets Act

Whereas the DMCC contains the 'countervailing benefits' clause:

> *"29 - Countervailing benefits exemption*
>
> *(1) The CMA must close a conduct investigation under section 28 where representations made by the undertaking to which the investigation relates lead the CMA to consider that the countervailing benefits exemption applies.*
>
> *(2) The countervailing benefits exemption applies where—*
>
> *(a) the conduct to which the investigation relates gives rise to benefits to users or potential users of the digital activity in respect of which the conduct requirement in question applies,*
>
> *(b) those benefits outweigh any actual or likely detrimental impact on competition resulting from a breach of the conduct requirement,*

> *(c) those benefits could not be realised without the conduct,*
>
> *(d) the conduct is proportionate to the realisation of those benefits, and*
>
> *(e) the conduct does not eliminate or prevent effective competition.*
>
> *(3)Where the CMA closes a conduct investigation as a result of subsection (1), the undertaking to which the decision relates is to be treated as if the CMA had found that the conduct did not constitute a breach of the conduct requirement."*
>
> DMCC - Section 29

We would advocate for a middle ground between those leaning towards the DMCC's model but with an important distinction: that rather than outright removing the obligation, we would instead prefer that it grant the ACCC the power to offer bespoke modified obligations in its place that lessen any harms of the conduct, while broadly retaining its benefits.

This would allow the ACCC to **strike a careful balance without forcing it to either drop an obligation entirely or to inflict significant harm** on Australian businesses and consumers.

Such an exemption should be reviewed on an annual basis, the DMA has a reasonable clause to this effect:

> *"Where an exemption is granted pursuant to paragraph 1, the Commission shall review its exemption decision if the ground for the exemption no longer exists or at least every year. Following such a review, the Commission shall either wholly or partially lift the exemption"*
>
> Digital Markets Act

The legislation must be crafted with the presumption that exceptions will be granted only in rare circumstances and, when they are, they will be limited in scope. Exemptions must not become a loophole for well-resourced gatekeepers to systematically bypass their obligations through legal maneuvering.

3.3.6. Q16: Exemption Mechanism - Countervailing Benefits

> *"16. For the grounds for exemption, would a broad 'countervailing benefits' exemptions mechanism with a high threshold be appropriate? What measures should there be to reduce the risk of vexatious applications?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

The question of a broad 'countervailing benefits' exemption mechanism with a high threshold has largely been addressed in the response to the previous question.

To mitigate the risk of vexatious applications, the burden of proof must rest entirely on the gatekeeper seeking the exemption. The gatekeeper must demonstrate that:

1. The claimed benefits to users exist and are significant.
2. These benefits could not be achieved without the specific conduct in question.
3. The conduct is proportionate to the benefits provided.
4. The conduct does not eliminate or prevent effective competition.

Additionally, any modifications to an obligation as an alternative to a full exemption should remain entirely under the ACCC's control. This ensures that exemptions do not weaken the overall regulatory framework while still granted the ACCC flexibility to avoid harming consumers in unexpected and exceptional circumstances.

3.3.7. Q17: Obligations with No Exemption

> *"17. Are there any potential obligations for which exemptions should not be available?"*
> *A new digital competition regime - The Australian Government the Treasury*

At this stage, we do not have a definitive position on which obligations, if any, that it should not be possible to have an exemption for.

3.4. Enforcement and Compliance

3.4.1. Q18: Safeguards for Information Gathering Powers

> *"18. What safeguards are required to ensure any information gathering powers for the proposed regime are used appropriately?"*
> *A new digital competition regime - The Australian Government the Treasury*

The DMA contains this provision:

> *"Where authorisation referred to in paragraph 9 of this Article is applied for, the* ***national judicial authority shall verify that the Commission decision is authentic and that the coercive measures envisaged are neither arbitrary nor excessive having regard to the subject matter of the inspection****. In its control of the*

> *proportionality of the coercive measures, the national judicial authority may ask the Commission, directly or through the national competent authority of the Member State, enforcing the rules referred to in Article 1(6), for detailed explanations in particular on the grounds the Commission has for suspecting infringement of this Regulation, as well as on the seriousness of the suspected infringement and on the nature of the involvement of the undertaking concerned."*
>
> Digital Markets Act

An equivalent that aligns with Australia's legal system seems reasonable. Additionally, information-gathering rules should include clauses on proportionality and being limited to the purpose of the investigation.

That said, both the DMA and DMCC appear to contain exceptionally strong investigatory powers. The treasury should consider providing the ACCC with equivalent powers.

3.4.2. Q19: Record Keeping Requirements

> *"19. The proposed framework could include record keeping requirements for designated digital platforms to record and keep certain information in a standardised format. How could these requirements be scoped to limit regulatory burden? Would there be any public benefit of publishing some of these records?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

Gatekeepers (companies designated under the Act) should be required to produce an annual report detailing their compliance with the Act. If they align their compliance approach with an overseas regime such as the DMA or DMCC, this report could focus on outlining the differences between that compliance and their approach in Australia.

A non-confidential version of this report should be published to ensure transparency for stakeholders, advocacy groups, and the public. This version should mirror the confidential report, with only sensitive information redacted, and should be substantial & comprehensive rather than a mere press release. The annual report should be expansive enough to allow any party to independently assess the gatekeepers compliance.

This transparency is essential for all parties to understand how the gatekeeper is meeting its obligations. Additionally, whenever a gatekeeper significantly updates its compliance strategy, it should publish an amendment to the previous year's report.

3.4.3. Q20: Limited Record Keeping Obligations for Undesignated Entities

> *"20. The regime could include limited record keeping obligations for entities that meet specified global revenue thresholds but are not yet designated. How could this requirement be scoped to limit regulatory burden and impacted entities? Are there any risks of this approach and how could these be mitigated?"*
> *A new digital competition regime - The Australian Government the Treasury*

It may be reasonable to require the collection of limited data necessary for the quantitative metrics used to designate an entity.

3.4.4. Q21: Resources and Guidance to Allow Stakeholders to Assist

> *"21. What guidance or resources would be needed by stakeholders to clarify and assist compliance with the obligations?"*
> *A new digital competition regime - The Australian Government the Treasury*

The most valuable resource for stakeholders is clear, publicly available information on ongoing cases, along with regular opportunities for comment. Both the UK's CMA and the EU Commission set strong examples in this regard, and we hope the ACCC can adopt a similar approach under the new Act.

For instance, the UK's Browsers and Cloud Gaming MIR, its SMS investigation into Apple and Google, and the EU's two specification investigations serve as useful benchmarks.

The published materials should include all summary documents, non-confidential responses, and a clear timeline outlining the previous and next steps in each case.

3.4.5. Q22: Penalties for New Regime

> *"22. Are increased monetary penalties and/or new specific non-monetary penalties required in the new digital competition regime? If so, why?"*
> *A new digital competition regime - The Australian Government the Treasury*

In the report it states that the current maximum penalty is the greater of AUD $50 million, 3 times the benefit obtained or 30% of the adjusted turnover during the breach period.

> *"Following the passing of the Treasury Laws Amendment (More Competition, Better Prices) Act 2022 (Cth), maximum financial penalties for businesses for a breach of a provision under the CCA is the greatest of AUD50 million, three times the value of the benefit obtained, or 30 per cent of adjusted turnover during the breach period.*

> *Treasury considers that these maximum penalty amounts are appropriate for the proposed digital competition regime."*
>
> *A new digital competition regime - The Australian Government the Treasury*

To ensure meaningful deterrence, the Treasury must guarantee that fines, especially for repeated violations, can reach a level that no company, including those valued in the trillions, would simply absorb as a cost of doing business.

Furthermore, there should be provisions for significant daily fines for continued non-compliance. Both the EU and UK have deemed such measures necessary for their regimes to be effective. The Treasury should assess whether introducing similar enforcement powers would be appropriate for Australia.

3.4.6. Q23: Structural Remedies for New Regime

> *"23. Should the new digital competition regime provide for structural remedies similar to those available in overseas regimes? Alternatively, should the regime include a mechanism for the ACCC to require that, where a platform has implemented a structural remedy overseas under an equivalent international regime, the platform roll out that same remedy in Australia?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

As discussed in this section, we believe the ACCC should be granted additional powers to address cases of systematic non-compliance.

3.4.7. Q24: Recognising Platforms Compliance with Similar International Regimes

> *"24. Is the proposed compliance proposals regime an efficient and workable way of recognising platforms' compliance with similar international regimes as compliance in Australia?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

Gatekeepers should have the ability to notify the ACCC if they intend to implement a compliance plan equivalent to one already adopted under an overseas regime (e.g., DMA, DMCC). They must also disclose any differences between their compliance approach in Australia and other regions.

If the proposed compliance plan fully meets all obligations under Australia's digital competition regime, both broad and specific, the ACCC should accept it. However, the

ACCC must retain full authority to prescribe and enforce obligations that exceed those set by its EU or UK counterparts.

Gatekeepers should also avoid introducing unnecessary fragmentation that disrupts alignment between equivalent compliance plans across regions. For instance, they should not require browser vendors to develop separate versions of their apps for the EU, UK, Australia, and other jurisdictions when a unified approach could achieve compliance across multiple regions.

3.5. Other Implementation Considerations

3.5.1. Q25: Should a Merit Review be Available for Certain Administrative Decisions?

> *"25. Should merits review be available for certain administrative decisions under this regime (such as exemption decisions)? What would be the associated risks, and can these risks be mitigated?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

We do not have a definitive position on this issue at this time.

3.5.2. Q26: Recovering Costs

> *"26. Would it be appropriate for government to recover the costs of administering the regime from industry?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

Yes, but only from designated firms under the regime. Ensuring that the ACCC is well-resourced is crucial, particularly given the vast legal budgets of gatekeepers and the aggressive legal strategies some of these companies have historically employed.

Bruce Sewell, Apple's former General Counsel, has openly discussed Apple's approach to legal risk:

> *"work out how to get closer to a particular risk but be prepared to manage it if it does go nuclear, ... steer the ship as close as you can to that line because that's where the competitive advantage occurs. ... Apple had to pay a large fine, Tim [Cook]'s reaction was that's the right choice, don't let that scare you, I don't want you to stop pushing the envelope."*
>
> Bruce Sewell - Apple's Former General Counsel

This demonstrates why regulators must have the necessary resources to effectively oversee compliance.

In the EU, concerns have already emerged regarding insufficient staffing for DMA enforcement. While the European Commission initially estimated 80 staff members would be sufficient, it has since acknowledged the need for at least 150. A levy to increase enforcement capacity has been considered.

> *"The EC has said it will need at least 150 staff members to enforce the DMA, almost twice the number it estimated when the rules were first proposed. The EC's DMA team is anticipated to have around 20 staff members this year, growing to around 80 by 2025. DMA enforcement will be shared between the EU's competition and digital departments."*
>
> Wilson Sonsini - DMA

Given this, The Treasury should ensure that the ACCC has adequate funding, potentially through a levy on designated firms, to properly enforce the regime.

3.5.3. Q27: Fit-for Purpose in Fast Moving Digital Platform Markets

> *"27. Are any additional measures required to ensure that the framework remains fit-for purpose to address harms in fast moving and dynamic digital platform markets?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

The Treasury should consider incorporating mechanisms that allow the ACCC to adapt the regime as needed, ensuring it remains effective in regulating fast-moving digital markets.

These mechanisms could include:

- **Specification Proceedings** – Enabling more precise definitions of how a particular gatekeeper should comply.
- **Adding or Modifying Obligations** – Tailoring requirements for specific platform types as necessary.
- **Expanding Coverage** – Adding new platform types to be designated under the regime.
- **Stronger Enforcement Measures** – Granting the ability to impose additional remedies or obligations in cases of systematic non-compliance.

All of these measures should be subject to requirements related to proportionality and remaining aligned with the intent of the Act.

3.5.4. Q28: A Customised Approach for Australia?

> *"28. Noting the benefits of Australia adopting the approach taken in international jurisdictions, where might a customised approach for Australia be warranted and why?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

While adopting good work from other regimes, such as the DMA and DMCC, offers clear benefits, the ACCC should have the flexibility **to close regulatory loopholes** and **improve** upon existing frameworks where needed.

In some cases, Australia's market dynamics and regulatory needs may differ, requiring bespoke measures to ensure effective competition. The ACCC must have the authority to tailor regulations to address unique conditions specific to Australia and, if necessary, to have bespoke requirements for our market.

Australia should not be afraid to be both a leader on some individual competition areas while copying what works from other regulators.

3.5.5. Q29: Should Australia be a Fast Follower

> *"29. Is the proposed approach for Australia to be a 'fast follower' of international regimes appropriate?"*
>
> *A new digital competition regime - The Australian Government the Treasury*

The 'fast follower' approach is a practical and beneficial strategy for Australia. It allows consumers and businesses to benefit from the successes of the DMA and DMCC, ensuring that Australia can implement proven regulatory measures.

Adopting requirements that have already been tested in EU and UK markets also simplifies enforcement, as compliance plans and precedents will already be established following international investigations.

Cooperation with other regulators is essential and lessens the ability of gatekeepers to play games across jurisdictions.

That said, the ACCC should have both the authority and intent to improve on what these regimes have achieved. If either the DMA or DMCC fails to adequately address specific competition issues, the ACCC must have the ability to implement its own solutions. The

ACCC is an influential regulator worldwide and any unique improvements will be closely watched globally.

4. Toward A Brighter Future

OWA believes that the Web's unmatched track record of safely providing frictionless access to information and services has demonstrated that it can enable a more vibrant digital ecosystem. The web's open, interoperable, standards-based nature creates an inclusive environment that fosters competition, delivering the benefits of technology to users more effectively and reliably than any closed ecosystem.

OWA's goal is to ensure that browser competition is carried out under fair terms, that user choice in browsers matters, and that web applications are provided equal access and rights necessary to safely contest the market for digital services.

The Treasury has a critical opportunity to fix key issues that have undermined both browser and Web App competition for over a decade to the benefit of both Australian consumers and Australian businesses. This will improve interoperability, contestability, and fairness leading to lower priced and higher quality apps, not only for Australia but for the entire world.

OWA believes competition, not walled gardens, leads to the brightest future for consumers, businesses, and the digital ecosystem.

5. Open Web Advocacy

Open Web Advocacy is a not-for-profit organization made up of a loose group of software engineers from all over the world, who work for many different companies and have come together to fight for the future of the open web by providing regulators, legislators and policy makers the intricate technical details that they need to understand the major anti-competitive issues in our industry and potential ways to solve them.

It should be noted that all the authors and reviewers of this document are software engineers and not economists, lawyers or regulatory experts. The aim is to explain the current situation, outline the specific problems, how this affects consumers and suggest potential regulatory remedies.

This is a grassroots effort by software engineers as individuals and not on behalf of their employers or any of the browser vendors.

We are available to regulators, legislators and policy makers for presentations/Q&A and we can provide expert technical analysis on topics in this area.

For those who would like to help or join us in fighting for a free and open future for the web, please contact us at:

Email	contactus@open-web-advocacy.org
Web / Web	https://open-web-advocacy.org
Mastodon	@owa@mastodon.social
Twitter / X	@OpenWebAdvocacy
LinkedIn	https://www.linkedin.com/company/open-web-advocacy