Digital Platforms: Australian Treasury consultation on ACCC's regulatory reform recommendations

Spotify's comments

A. Introduction

Spotify welcomes the Australian Treasury's consultation on behalf of the Australian Government on the ACCC's regulatory reform recommendations (the "**Consultation**") and the opportunity to submit its views on the future of digital regulation in Australia.

Spotify's response to the Consultation focuses on mobile app stores and outlines Spotify's views on how digital regulation can help create a competitive and innovative, fair playing field for developers, to the benefit of consumers.

As Spotify has a substantial Australian customer base, but operates globally, Spotify's response seeks to address the Treasury's request for views on international alignment of digital regulation, having regard to that experience in dealing with digital gatekeepers on a global basis. We trust our response may assist the Treasury in striking the right balance in regulation that promotes a vibrant digital economy in Australia, as well as assisting gatekeepers and businesses that interact with them, having clear and enforceable "rules of the road".

This response is structured as follows: First, Spotify explains why, in its view, *ex ante* digital regulation is needed to complement the existing legislative instruments, in particular *ex post* antitrust enforcement (**Section B**) and makes suggestions on where the new regulatory regime should focus (**Section C**). **Section D** dispels common myths about the impact of digital regulation on innovation and user privacy and security that gatekeepers are seeking to perpetuate. Finally, **Section E** highlights priority considerations for the implementation of *ex ante* regulation to optimise its effectiveness for the benefit of Australians.

B. *Ex ante* regulation is needed in the digital sector

Spotify agrees with the ACCC's recommendation that Australia would benefit from a new regulatory framework to improve the competitive conditions in the digital economy, in particular to open mobile app distribution to competition and make app markets more contestable.

Mobile devices are the predominant (and increasingly exclusive) gateway to the internet for consumers and businesses alike. In the past 15 years, the mobile space has become increasingly dominated by what can best be described as two parallel monopolies operated by Apple and Google. These companies now act as gatekeepers to the mobile internet and have control over the relationship between businesses and their customers. Nothing happens on mobile devices that is not in the interest of these two gatekeepers.

Much like in the '90s and early '00s, when Microsoft was the main digital gatekeeper, the digital economy stands at a critical juncture that will determine the future of the Internet. Ensuring a level playing field on mobile is essential to creating the right conditions for the next wave of digital innovation to emerge, to the benefit of consumers. It suffices to recall that Apple and Google

themselves owe their success to a large extent to the antitrust actions that broke Microsoft's gatekeeper power only two decades ago.

Today, antitrust enforcement globally has proven insufficient to single-handedly address and deter the swathe of abuses by digital gatekeepers. Antitrust enforcement and fines have, in many cases, become a cost of doing business and every step is taken to delay enforcement and maintain market power. The time is ripe, therefore, for antitrust enforcement to be *complemented* by *ex ante* regulation similar to that which applies in other parts of the economy (e.g., energy, telecommunications). Governments globally are reaching consensus on the need for digital regulation, as indicated by the record speed at which legislation was passed in the European Union (the Digital Markets Act ("**DMA**"))[1] and is being considered in the US *inter alia* with the proposed American Innovation and Choice Online Act and Open App Markets Act ("**OAMA**"). These legislative instruments explicitly seek to regulate app stores as one of the core gatekeeping services in today's digital economy.

This sentiment is shared also in Australia, as shown by the ACCC's Fifth Report to Treasury focusing on regulatory reform published on 11 November 2022 **("Report**").

Ex ante regulation should be mandatory and robust if it is going to create real change on the market. Global regulators' efforts to force gatekeepers to comply even with mandatory antitrust remedies is resisted at every turn, as Apple's conduct demonstrates (see **Sections C and E** below). Gatekeepers often delay compliance or, at worst, circumvent it through abusive conduct "by another name" that generates the same harmful outcomes. In this respect, we note that while certain parties have been suggesting that voluntary industry codes would suffice, when dealing with gatekeepers, the Treasury's own experience has been that a mandatory code such as the Media Bargaining Code has been necessary.

Ex ante regulation can take many shapes and forms. This is demonstrated by the different approaches taken in the EU, where the DMA provides a list of *per se* unlawful behaviours agnostic as to the gatekeeper's business model, and the UK, where - according to the UK Government's and the Competition and Markets Authority's ("**CMA**") statements - the new "pro-competition regime for digital markets" will focus on codes of conduct tailored to each gatekeeper (or, firm of Strategic Market Significance). In our view, it is of limited practical significance whether an *ex ante* regime takes a so-called rules-based approach (like the DMA) or a principles-based approach, like the upcoming UK regime. These two different approaches to *ex ante* regulation ultimately seek to achieve the same outcome through different methods. Factors which are more important in this respect include: (i) the regime being mandatory in nature; (ii) capturing and sanctioning the key abusive behaviours in which gatekeepers engage; and (iii) prompt and robust enforcement.

Australia should not miss the opportunity to enact legislation promptly, while other sophisticated jurisdictions globally are doing the same, thereby not only assisting in shaping the global dialogue and principles on the Internet of tomorrow, but also to ensure that Australia remains competitive in the global marketplace for attracting innovative businesses. The legislation will be to the benefit of today and tomorrow's ***Australian*** businesses and consumers.

[1] The text of the DMA is available here https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925&from=EN.

C. Regulating gatekeeping app stores

In Spotify's experience, there should be four legislative priorities for the regulation of app stores, which are borne out of past and present antitrust cases: (i) a straightforward ban on anti-steering provisions contained in developers' distribution agreements with app stores; (ii) a straightforward ban on "tying" *i.e.*, making the distribution of apps on app stores conditional upon developers' accepting unrelated obligations towards the app store owner; (iii) limiting the risk of gatekeepers circumventing the *ex ante* regime, depriving it of its effectiveness while paying lip-service to its provisions and (iv) breaking the distribution monopoly the gatekeepers currently hold for mobile applications. In Spotify's view, similar provisions should be prioritised in a future Australian *ex ante* regulatory regime.

(i) A ban on anti-steering provisions

Certain gatekeeper app stores (e.g., Apple) require apps that sell 'digital goods' (e.g., music streaming subscriptions) in a mobile app (in-app) exclusively to use the app store owner's in-app purchase system[2] and pay a corresponding "tax", which typically starts at 30% of the value of each in-app transaction. To complement this obligation and guarantee their in-app "tax", gatekeeper app stores impose so-called "anti-steering provisions" *i.e.*, they prohibit developers from informing users of alternative (and often cheaper) purchasing mechanisms and offers found outside the app. As part of this, apps must also not link out to any external purchasing methods.

Gatekeepers' own apps (e.g., Apple Music), are free of these restrictions, but third-party developers like Spotify are either forced to increase prices to cover the "tax", absorb the "tax", or disable in-app purchases altogether, shutting off the ability to acquire subscribers via their mobile apps, and depriving users of information about valuable offers outside the app.

As a result:

- **Consumers are harmed:** the lack of transparency leads to them either paying a higher price for in-app digital goods (as they are less aware of offers outside the app) or not purchasing at all.
- **Developers are harmed:** they cannot compete with gatekeeper's apps on in-app price and are deprived of their ability to communicate with their customers about offers outside and thus acquire significantly fewer paying customers.

Importantly, these anti-steering rules did not always exist. Apple released the first iPhone without third-party apps, making it unsuccessful. The iPhone only became successful when Steve Jobs allowed developers to come in and create a rich ecosystem of services, which Apple famously marketed with the slogan "There's an App for That". Once the Apple ecosystem gained critical mass, Apple started imposing abusive terms on developers, including the anti-steering rules, employing a classic "bait and switch" once it had the market power to do so. While Apple purports to be a "closed ecosystem" that should be allowed to remain as such, it has in fact opened its App Store to competition and is demanding the right to reap the entirety of the benefits arising mainly from third-parties' contribution to that ecosystem.

[2] For Apple, that is In-App Purchase ("**IAP**") and for Google, Google Play Billing ("**GPB**").

Anti-steering rules are under serious antitrust scrutiny because they tend to lead to higher prices and less choice for consumers. The European Commission ("**EC**") is investigating the lawfulness of Apple's App Store practices and, in April 2021, provisionally found that Apple's anti-steering rules violate EU law as they provide an unmerited competitive advantage to Apple Music.

In addition, the DMA explicitly bans anti-steering rules such as Apple's "[t]*o prevent further reinforcing* [businesses'] *dependence on* [...] *gatekeepers, and in order to promote multi-homing…*"[3] by requiring gatekeepers to:

> "*...allow business users, free of charge, to communicate and promote offers, including under different conditions, to end users acquired via its core platform service or through other channels, and to conclude contracts with those end users, regardless of whether, for that purpose, they use the core platform services of the gatekeeper.*"[4]

This provision is effective for various reasons:

- it is a straightforward ban on anti-steering, making its implementation easier and does not contain exemptions that would allow gatekeepers to manipulate and circumvent the provision (*e.g.*, using user security as an excuse); and
- it seeks to prevent circumvention by explicitly requiring gatekeepers to allow developers to advertise out-of-app purchasing options *free of charge* and - even more importantly - to conclude contracts with users outside of the gatekeeper's platform (e.g., through external links placed in the app) also *free of charge*.

Similarly, the OAMA in the US takes a direct approach to banning anti-steering provisions:

> "*Sec. 3(b) Interference With Legitimate Business Communications.—A covered company shall not impose restrictions on communications of developers with the users of an app of the developer through the app or direct outreach to a user concerning legitimate business offers, such as pricing terms and product or service offerings.Nothing in this subsection shall prohibit a covered company from providing a user the option to offer consent prior to the collection and sharing of the data of the user by an app.*"

(ii) A ban on tying

Gatekeeping app stores have been imposing unrelated obligations as a condition to allowing developers to distribute apps on their platforms, including primarily the obligation exclusively to use the app store owner's in-app purchasing mechanism to sell digital goods. Most sophisticated antitrust regimes globally prohibit "tying" of unrelated obligations to a dominant service (in this case, a dominant app store), as this enables leveraging market power between markets instead of competing on the merits.

The DMA explicitly prohibits tying practices such as those described above:

> "*The gatekeeper shall not require end users to use, or business users to use, to offer, or to interoperate with, an identification service, a web browser engine or a* ***payment service****, or* ***technical services that support the provision of payment services, such as payment***

[3] Preamble 40, DMA.

[4] Article 5(4) DMA.

> ***systems for in-app purchases****, of that gatekeeper in the context of services provided by the business users using that gatekeeper's core platform services.*"[5] (**emphasis added**)

What makes this provision particularly effective is the direct reference to payment services and in-app purchase mechanisms, which removes the need for a debate on the scope of the prohibition.

The OAMA in Section 3(a)(1) provides that a covered company shall not:

> *"require developers to use or enable an in-app payment system owned or controlled by the covered company or any of its business partners as a condition of the distribution of an app on an app store or accessible on an operating system;"*

(iii) Pre-emptively limiting avenues of circumvention

The risk of circumvention is perhaps the single most important threat to the effectiveness of digital regulation.

The DMA seeks to pre-empt this by devoting an entire article to anti-circumvention. We copy below the most important excerpts from Article 13 with **added emphasis** (Article 13 is also annexed in its entirety):

> *Article 13*
>
> *Anti-circumvention*
>
> *1. An undertaking providing core platform services* ***shall not segment, divide, subdivide, fragment or split*** *those services through contractual, commercial, technical or any other means* ***in order to circumvent the quantitative thresholds*** *laid down in Article 3(2). [...]*
>
> *2. [...]*
>
> *3. The gatekeeper shall ensure that the obligations of Articles 5, 6 and 7 are* ***fully and effectively complied with****.*
>
> *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.*
>
> *5. [...]*
>
> *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.*
>
> *7. [...]*

[5] Article 5(7) DMA.

8. [...]

The complex technical nature of digital services tends to create opportunities for circumvention in practice. In Spotify's view, while a general provision prohibiting circumvention is important, such a provision should be complemented by specific instructions from the regulator to individual gatekeepers warning them against adopting specific behaviour that would likely constitute circumvention.

The OAMA also seeks to prevent such circumvention in Sec. 3(a)(3), which states that a gatekeeper shall not: *"take punitive action or otherwise impose less favorable terms and conditions against a developer for using or offering different pricing terms or conditions of sale through another in-app payment system or on another app store."*

(iv) Opening mobile app distribution to competition

Making any regulatory regime successful in increasing fairness and contestability in app distribution has to include paving the way for mobile app developers to be able to reach end users without needing a mobile gatekeeper. Both the DMA and the OAMA address this by enabling alternative means of distribution, including direct downloading of an app from a developer's website, and ensuring that third-party app stores are able to exist on gatekeepers' operating systems and devices. These provisions are combined with provisions creating obligations on gatekeepers to enable users to select alternative distribution methods as default and to remove impediments to switching between them.

More specifically, the DMA provides that gatekeepers must:

"…allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that gatekeeper. The gatekeeper shall, where applicable, not prevent the downloaded third-party software applications or software application stores from prompting end users to decide whether they want to set that downloaded software application or software application store as their default. The gatekeeper shall technically enable end users who decide to set that downloaded software application or software application store as their default to carry out that change easily."[6]

Similarly, under the OAMA, covered platforms are obliged *inter alia* to allow end users to:

> *"(1) choose third-party apps or app stores as defaults for categories appropriate to the app or app store;*
>
> *(2) install third-party apps or app stores through means other than its app store.*
>
> *(3) hide or delete apps or app stores provided or preinstalled by the app store owner or any of its business partners."*

D. Dispelling myths commonly perpetuated by gatekeepers

6 Article 6(4) DMA.

As part of their defence against regulation, gatekeepers have been applying scaremongering tactics, centred around perceived risks to: (i) innovation and (ii) user privacy and security stemming from regulations. This section explains why these concerns do not withstand scrutiny.

Myth #1: Digital regulation will lower the level of innovation

Gatekeepers have been claiming that by regulating (and therefore restricting) their conduct, their freedom and ability to innovate will be curtailed and the overall level of digital innovation will drop as a result.

In Spotify's view, the opposite is true: digital regulation will increase the level of innovation as it will provide certainty for developers that their investment and innovation will be protected by rules of the road. For example:

- First, this has been the case historically. Steps taken to limit Microsoft's power as an Internet gatekeeper in the '90s and '00s gave rise to innovators like Apple and Google, while not impeding Microsoft's ability to innovate.

- Second, digital regulation will allow innovation from a diverse base of businesses instead of concentrating it on a few digital giants. Currently, any innovation in the mobile space is limited by the business interests of the two gatekeepers. Digital regulation should aim to create a level playing field for all businesses, that will enable innovation to flourish where it would otherwise be stifled by abusive practices. Such practices often raise rivals' costs (e.g., by refusing interoperability with key inputs or making it more expensive) or restrict rivals' growth to favour the gatekeeper's own products. Strengthening competition will create more sources of innovation, increasing the overall level of innovation in Australia, including by empowering home-grown Australian businesses.

- Third, a drop in the overall degree of innovation has not been observed in other regulated sectors, such as telecoms. Digital regulation would not be depriving gatekeepers of the ability or the incentive to innovate but forcing them to compete on their merits.

- Finally, gatekeepers' often present digital regulation as potentially limiting their incentives to innovate by allowing third-parties to free-ride on their investments (e.g., by forcing gatekeepers to provide effective interoperability or improved access to data). Often, what gatekeepers present as free-riding, legislators globally see as allowing third-parties to reap some of the benefits arising from ecosystems they have helped establish and grow.

Myth #2: Digital regulation will open ecosystems causing security and privacy risks for consumers

Gatekeepers are alleging that opening digital markets will jeopardise user privacy and security online, as ecosystems will no longer be wholly controlled by them.

Once again, the opposite is true: regulation will improve privacy and security standards protection compared to what is currently the case.

- First, gatekeepers' app stores have only been moderately successful in protecting security and privacy. For example, in March 2021, security company Avast published a list of scam apps on Apple's App Store. After 15 months, more than 60% are still available on the App Store, bringing in 7.2 million unique downloads, giving Apple net revenues of

approximately $8.6 million in a single month. Moreover, amongst other criticisms of the App Store's effectiveness in preventing harmful scams, in his deposition in the *Epic v Apple* US litigation, a senior Apple engineer likened the defences of the App Store against malicious actors to "*bringing a butter knife to a gunfight*".[7]

- Moreover, opening digital markets to competition will mean that security and privacy will no longer be controlled by gatekeepers, but will rather become parameters of competition between the gatekeepers and their rivals. This will enable better privacy and security solutions to emerge, that will be focused on the needs and desires of consumers instead of on perpetuating gatekeepers' control (e.g., truly curated app stores with solid review processes).

E. Making regulation effective

Enacting new legislation in Australia might perhaps be the easier step - the real challenge will be ensuring that regulation operates effectively and brings about the positive outcomes it set out to achieve for competition and consumers. In Spotify's experience, the following factors would be critical in increasing the likelihood of effective compliance:

- **Not replicating the features of traditional antitrust enforcement that result in less-than-optimal effectiveness**

    - Antitrust investigations are not subject to time limits, and it can take several years for effective remedies to be imposed. Imposing statutory deadlines for key steps in the implementation of digital regulation (e.g., designating regulated "gatekeeper" companies) would lead to a faster pace of implementation.

    - The most important difference between *ex ante* regulation and *ex post* antitrust enforcement is that *ex ante* regulation imposes obligations and prohibitions based on the legislator's assessment of what behaviours are *a priori* desirable or undesirable. Gatekeepers' ability to raise defences based on market efficiencies purportedly created by their abusive conduct should be limited. Allowing "gatekeepers" to argue that they should not comply with their regulatory obligations because their current (abusive) behaviour creates efficiencies for consumers would result in a never-ending "battle of the economists" between the gatekeepers and the regulator, and likely litigation, leading to a stalemate on the compliance front. The benefit of *ex ante* regulation is that any efficiencies associated with gatekeepers' conduct have already been taken into account by the legislator and incorporated into the law.

- **Adequate resources for the sectoral regulator.** Gatekeepers will devote considerable resources to preserving their market power and privileges. While regulators cannot replicate the size of gatekeepers' resources, they should be armed with sufficient personnel (in terms of numbers but also of technical skills) to handle the volume and technical requirements of the task at hand. In this context, regulators should consider increasing their number of technical experts (e.g., data or computer scientists).

[7] See *inter alia* https://www.ft.com/content/914ce719-f538-4bd9-9fdf-42220d857d5e.

- **When in doubt, compliance first.** One of the key delaying tactics the gatekeepers are expected to implement is litigation. Thus, appeals should carry no automatic suspensory effect, as that could hold the entire regulation hostage to gatekeepers' vexatious litigation tactics.

- **Market testing.** Implementing *ex ante* regulation will require continuous regulatory dialogue between the regulator and the regulated firms, especially given the technical complexity in designing digital remedies (as antitrust cases have amply demonstrated). At the same time, compliance measures proposed by gatekeepers should be heavily market tested, by bringing into the process the types of third parties (e.g., customers, rivals) whom the regulatory provisions are meant to protect. This would also be a protective mechanism against the risk of regulatory capture or the perception thereof.

- **Material (not just monetary) penalties for non-compliance.** While monetary penalties are an important deterrent, digital giants often treat them as an unavoidable but inconsequential "cost of doing business". Thus, not only must monetary penalties be considerable[8] but they should be accompanied by non-monetary penalties that would be serious enough to serve as real deterrents, such as, for instance, a temporary moratorium on M&A activity (which the DMA provides for in cases of recidivism), structural remedies (forced break-ups or divestments), or personal consequences for corporate executives.

***

28 February 2023

[8] For instance, the DMA caps penalties at 10% of annual global turnover, which becomes 20% in the event of recidivism.

Annex - Article 13 of the DMA

Article 13

Anti-circumvention

1. An undertaking providing core platform services shall not segment, divide, subdivide, fragment or split those services through contractual, commercial, technical or any other means in order to circumvent the quantitative thresholds laid down in Article 3(2). No such practice of an undertaking shall prevent the Commission from designating it as a gatekeeper pursuant to Article 3(4).

2. The Commission may, when it suspects that an undertaking providing core platform services is engaged in a practice laid down in paragraph 1, require from that undertaking any information that it deems necessary to determine whether that undertaking has engaged in such a practice.

3. The gatekeeper shall ensure that the obligations of Articles 5, 6 and 7 are fully and effectively complied with.

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.

5. Where consent for collecting, processing, cross-using and sharing of personal data is required to ensure compliance with this Regulation, a gatekeeper shall take the necessary steps either to enable business users to directly obtain the required consent to their processing, where that consent is required under Regulation (EU) 2016/679 or Directive 2002/58/EC, or to comply with Union data protection and privacy rules and principles in other ways, including by providing business users with duly anonymised data where appropriate. The gatekeeper shall not make the obtaining of that consent by the business user more burdensome than for its own services.

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.

7. Where the gatekeeper circumvents or attempts to circumvent any of the obligations in Article 5, 6, or 7 in a manner described in paragraphs 4, 5 and 6 of this Article, the Commission may open proceedings pursuant to Article 20 and adopt an implementing act referred to in Article 8(2) in order to specify the measures that the gatekeeper is to implement.

8. Paragraph 6 of this Article is without prejudice to the powers of the Commission under Articles 29, 30 and 31.