Testimony of ACT | The App Association on Competition in Digital Ecosystems of Mobile Devices

February 12, 2025

ACT | The App Association writes to provide input in response to the Public Hearing on Competition in Digital Ecosystems of Mobile Devices (iOS and Android) before the Administrative Counsel for Economic Defense (CADE).

The App Association's comments are organized as follows:

I. Statement of Interest and Background

ACT | The App Association represents thousands of small business application developers and connected device companies, located both within Brazil and around the globe. These companies drive a global app economy worth more than BRL 25.8 trillion globally[1] and are responsible for approximately 428,000 jobs across Brazil.[2] App Association members leverage the connectivity of smart devices to create innovative solutions that introduce new efficiencies across consumer and enterprise use cases and rely on a predictable and fair approach to platform regulation to grow their businesses and create new jobs; therefore, inquiries into online intermediation platforms are directly relevant to us, and we urge for the careful consideration of our views by Brazil and other policymakers and enforcers.

Generally, the App Association encourages Brazil to avoid developing industry- or sector-specific guidance or enforcement. There would be substantial risks and unintended consequences associated with disparate treatment among industries if policymakers were to carve out exemptions or specifically target certain sectors of the economy. A flexible, industry-agnostic approach to competition policy and enforcement is far superior in addressing unique and challenging use cases, promotes a harmonized and predictable legal and business environment, and will be more able to keep pace with changes to the marketplace brought on by technological advancements that cannot be anticipated. The app economy, and the concept of a "digital platform" and "digital market," is constantly changing as new services and products are introduced to the public. Differences in terminology between how phrases are used in commerce and how phrases are used in static industry-specific guidance will inevitably diverge, leading to an inconsistent application of antitrust law.

[1] https://actonline.org/global-appcon22-competition-and-privacy/.

[2] https://www.progressivepolicy.org/wp-content/uploads/2023/10/Brazilian-App-Economy-Portguese.pdf.

Below, the App Association provides views on digital platforms and competition, as well as reactions and feedback on specific issues raised by various competition authorities, noting that:

- Data overwhelmingly indicates that today's Brazilian mobile app economy is competitive and vibrant, enabling small business developers to innovate and create Brazilian jobs. The global app economy is valued at more than BRL 25.8 trillion globally[3] and are responsible for approximately 428,000 jobs across Brazil.[4] Global app store revenue continues to grow steadily due to strong competition across the market.
- Brazil should acknowledge the benefits of variety in digital software distribution platforms on which small developers rely. Otherwise, Brazil risks biasing its policy decisions made in the policy development process.
- Small businesses within the app ecosystem rely on a flexible, industry-agnostic approach to competition policy and enforcement. A predictable legal and business environment allows for innovators to better navigate changes to the marketplace brought on by technological advancements that cannot be anticipated.
- Brazil should, in light of the evolution of the software development industry and the clear objective indications of competition and innovation in the mobile app ecosystem, conclude that the digital platform ecosystem is healthy and competitive, and that calls for governmental intervention into this ecosystem, or changes to existing laws and regulations that would upend this vibrant ecosystem, will not be pursued.

The App Association shares Brazil's goals of advancing competition and innovation in the digital economy across consumer and enterprise sectors. On behalf of the small business developer community, we offer general perspectives and recommendations below and respond to various Inquiry findings and proposed remedies posed by Brazil. The App Association welcomes the opportunity to assist Brazil in its efforts moving forward.

[3] https://actonline.org/global-appcon22-competition-and-privacy/.

[4] https://www.progressivepolicy.org/wp-content/uploads/2023/10/Brazilian-App-Economy-Portguese.pdf.

II. General Views and Recommendations of ACT | The App Association on Competition in the Mobile App Ecosystem

a. How Developers Distributed Software Before Platforms

Much has changed for consumers and developers since the early days of software applications. In the early 1990s, consumers were tasked with the challenge of locating and then travelling to a brick-and-mortar store that happened to sell software. Once internet connectivity became a standard feature in most private residences, consumers began to download applications from the comfort of their homes without having to step foot in a physical store. Despite the changes brought by internet connectivity, the golden age of personal computer (PC) software pales in comparison to the size and scale of the mobile app revolution during which software developers evolved into app developers. During this transition to online distribution, consumers were often unable to trust software downloaded from the internet because the vetting function of platforms had not yet been introduced.

Before the ubiquity of mobile platforms, the software ecosystem ran on PCs, and software companies had to cobble together a distribution plan, including the creation of consumer trust from the ground up. This forced early app companies, often with teams of one to two developers, to wear many hats to develop, market, and benefit from the sale of their products. App companies were not only required to write code for their products, but they were also responsible for:

1. Managing their public websites;
2. Hiring third parties to handle financial transactions;
3. Employing legal teams to protect their intellectual property; and
4. Contracting with distributors to promote and secure consumer trust in their product.

The skillsets required to manage the overhead of online software distribution were often not core competencies of small development companies, and the additional steps cost app developers valuable time and money, with little tangible benefit.

In the internet economy, immediate consumer trust is almost impossible without a substantial online reputation, and not attaining it spells death for any app company. However, what does “trust” mean? In this context, trust refers to an established relationship between the app company and consumer where the consumer demonstrates confidence to install the app and disclose otherwise personal information to an app company. Prior to platforms, software developers often had to hand over their products to companies with a significant reputation to break through the trust barrier.

Developers in a pre-app store world experienced difficult and oppressive distributor requirements. When dealing with retail distributors, these small businesses were required to guarantee a competitive price, pay 3-6 percent of sales as a marketing fee in addition to BRL 470,000 for product launch marketing, shipping to deliver their products to distributors, and buying back unsold products. Once contracts were negotiated, software developers were often required to spend additional money so that in-store catalogues would feature their product or retail stores would place their product on an endcap display, all before consumers even saw the products.

However, with the advent of the smartphone and app stores, the experience of these innovative small businesses became a relic of the past. The smartphone, in its brief history, revolutionized the economy at large and established a symbiotic relationship between software platforms and developers. The fact that developers have a choice in which platform to use to reach their consumers and clients underscores that platforms compete not only as app marketplaces but as developer services providers. Even when developers distribute an app through an internet browser, and not through a platform's app store, the developer still benefits from the trust consumers have that the web browser running on their phone is safe to use.

b. The Impact of Platforms on Software Distribution: What Makes an Ecosystem Work?

The app ecosystem has grown exponentially alongside the rise of the smartphone. These companies drive a global app economy valued at more than BRL 25.8 trillion globally[5] and are responsible for approximately 428,000 jobs across Brazil.[6] However, the app economy's trajectory is due to a variety of factors. The single most important factor in the app ecosystem's dynamic growth and unrivalled success is the presence of curated platforms, or app stores. Trusted app stores serve as a vital foundation for the growing uses of apps across industries and enterprises. Three key attributes led to the revolution in software distribution:

1. The provision of a bundle of services that reduces overhead costs;
2. Instantaneous and cost-effective consumer trust mechanisms; and
3. Cost-effective access to a global market.

Today, every successful platform for mobile, desktop, gaming, and even cloud computing must provide these features or risk failing in the marketplace. And increased competition amongst platforms has provided an unprecedented avenue for entrepreneurship.

[5] https://actonline.org/global-appcon22-competition-and-privacy/.

[6] https://www.progressivepolicy.org/wp-content/uploads/2023/10/Brazilian-App-Economy-Portguese.pdf.

c. The Mobile App Economy Shows Strong Signs of Competitiveness, Growth, and Job Creation

Smartphones are the single most rapidly adopted technology in human history, outpacing innovations like the printing press and the steam engine. In just 15 years, and with the union of app stores (or platforms), mobile, and cloud, apps changed the phones, devices, and services we use every day. The entry of platforms created novel opportunities for consumers and developers. But while platforms provide some of the infrastructure, developers and companies bring smart devices to life. Without apps, a smartphone is just a phone.

The mobile app economy exhibits strong signs of competitiveness, growth, and job creation:

- The global app economy is valued at more than BRL 25.8 trillion globally.
- The Brazilian software developer workforce is estimated to total approximately 570,000 and growing.[7]
- The 6.3 billion global smartphone owners downloaded 230 billion apps in 2021.
    - Top app downloads (non-gaming):[8]
        - 12.13 billion business-related downloads
        - 5.87 billion finance downloads
        - 4.87 billion productivity-related downloads
        - 2.48 billion health and fitness-related downloads
        - 950 million education downloads

d. The Applicability of Competition Law to Software Platforms: Two-Sided Market Analysis

i. *Software Platforms and Market Definitions*

An appropriately scoped market definition should precede determinations of market power and whether a market feature has an adverse effect on competition, including with regard to the impact on small businesses. While Brazil's market definition should consider antitrust foundations such as the existence of substitutes, such an analysis must be fact-specific and traditional antitrust analysis is not easily applied to platforms that often are multi-sided markets.

Multi-sided platforms differ from traditional markets in important ways because the platform creator's practices and pricing on one side of the market affect the other side. For example, investments that increase participation or quality on one side of the market create the value that is sought by the other side. The value of the services that a two-sided platform provides increases as the number of participants on both sides of the platform increases. A platform firm must, therefore, be concerned not only with its

[7] https://nextbillionusers.google/research/africa-developer-community-2021/#.

[8] https://sensortower.com/.

own quality and advertising, but also that of the vendors who operate over its network.[9]

Traditionally, antitrust analyses on two-sided markets (e.g., newspapers) have focused on only one side of the market because of the limited impact of network effects. Where platforms experience more indirect network effects with linked demands and pricing—such as in the case of software app distribution platforms—including both sides in the relevant antitrust market is appropriate. Mobile platform markets likely require consideration of at least three distinct markets (possibly four if one considers wireless carriers) to perform one transaction. But even where multi-sided platforms have demonstrable competition on both sides of a transaction, using traditional constructs such as the "small but significant non-transitory increase in price test" (SSNIP) on one side of the transaction would lead to the misapplication of antitrust law. Brazil is encouraged to provide flexibility for case-by-case market definitions, and to appropriately apply antitrust law to multi-sided digital platforms. Both legacy and novel economic and legal approaches can and should address the complexities of multi-sided platforms.

In its efforts so far with respect to the bill, Brazil has recognized a number of prominent digital platforms in existence today; however, the App Association requests that this discussion be supplemented by further discussing the broad range and diversity of digital platforms that serve countless consumer and enterprise use cases and explore the ways in which they compete with one another for developers and customers. While Brazil has chosen to focus on only two platforms--Apple and Google-- in a list of "app stores," for developers the market is much wider, with different choices being most desirable based on the use case and potential customer base. Certainly, the Apple and Google app stores offer immense value that developers realize through lower overhead and compliance costs, built-in customer trust, increased speed to market, and wider distribution and market access, as discussed elsewhere in this comment. These platforms provide a centralized framework for app developers to engage and secure visibility to app users worldwide, but App Association members routinely leverage many further options for developers. A game developer can choose platforms like Epic or Steam, and enterprise developers can look to hundreds of proprietary, custom platforms or could create their own. Moreover, for developers looking to reach a general audience, using the web is an alternative, especially for companies that are looking for different kinds of distribution or search services than those available on platforms. Additionally, software developers could choose to advertise on Facebook, distribute their products through Amazon, or leverage further platforms. It is worth noting, however, that there are some important distinctions between software platforms—like the App Store or Google Play which provide a marketplace for software apps—and social media platforms or "aggregators" that connect people with information and are fueled by data. Aggregators like Facebook and X (formerly Twitter), for example, connect people with information and other people (and generate valuable data in the process), while the Google Play store

[9] Mark Rysman, *The Economics of Two-Sided Markets*, 23 J. Econ. Persp. 125, 136 (2009).

and Apple's App Store provide a marketplace for consumers and app developers to transact directly. These differences illustrate the diversity in the market for distribution methods, as developers may prefer one model over another, and we urge Brazil to acknowledge the broad competition between software distribution platforms and capture how that competition has improved platform features and reduced prices.

Although developers can choose from multiple platforms, there is no such thing as a perfect software distribution platform. Some, but not all, app developers pay a fee to platforms for developer services, and they expect those services to meet their needs. Just as online companies must clearly communicate their data practices to consumers, so must platforms clearly define the requirements and details of their terms of service to developers. For example, when platforms change their developer guidelines, they must communicate clearly and ensure developers understand what the changes mean for them and their customer relationships. The App Association continuously fights for improvements in these areas on behalf of its small business developer community.

ii. *Software Distribution Platforms, Market Power, and Monopoly Power*

Once a market has been appropriately defined, we urge for Brazil's antitrust analysis to turn to a determination of market power and monopoly power to inform whether a market feature has an adverse effect on competition. Market power and monopoly power are related concepts but are not the same. Market power is the seller's ability to raise prices above those that would be charged in a competitive market, while monopoly power occurs when a firm has the power to control prices and exclude competition. Policymakers and enforcers should distinguish the two concepts as a matter of degree, monopoly power being higher. However, a firm's mere possession of either market power or monopoly power should not be enough to find competitive harm; Brazil should demonstrate that the firm unfairly values its products resulting in harm to consumers and competitors. Demonstration of such abuse is critical to properly determining whether antitrust remedies are appropriate, and if so, to what degree. The App Association urges for Brazil's analysis to be updated to clearly define and explore both market power and monopoly power.

Platforms play an important role across a variety of economic sectors, bundling sets of services together for sellers and connecting those sellers with specific categories of buyers. Brazilian antitrust policy should reflect that market power assessments should be more holistic and rely on factors beyond market share alone, and that new digital platforms illustrate that the application of traditional antitrust fact patterns to complex software platforms is ill-advised. Over-reliance on basic market share (e.g., the relative size of a user base) breakdowns wrongly equates *share* with *power*, ignoring unique attributes of multi-sided platforms such as the ability to benefit from multiple services on the same platform, a low barrier to substitution, and ease of market entry by new competitors. Such characteristics minimize the lock-in effect on users. Further, a proper antitrust analysis should also demonstrate that the monopoly power at issue

is not short-lived. Such a determination will, again, be highly fact-dependent and should be comprehensive, based on rigorous and objective economic analysis. We also strongly caution Brazil and others to avoid relying on unproven allegations made by outlier opportunist companies seeking to upend the harmonious app ecosystem simply for their own company's benefit, including in current ongoing litigation.

iii. *The Software Side of the Market*

Turning to the different sides of the software platform market, the most visible side for the general public is the one characterized by software sellers (app developers) selling to software consumers (businesses and individual consumers). Brazil's evidence base and the App Association's experiences reflect strong and dynamic competition on the software side of the market.

With respect to self-preferencing by platforms, blanket characterizations of self-preferencing should be avoided because, considering the unique nature of software distribution platforms, self-preferencing can be a pro-competitive example of vertical integration. We strongly urge Brazil to conclude that where vertical integration or self-preferencing can lead to greater efficiency, better quality, or lower costs for consumers, there are minimal antitrust issues when users can easily switch to another platform. Considering that smartphones are music players, cameras, and multimodal communications devices, a narrowly focused view of one of these features without recognizing the integration of the same into the devices is incompatible with the way consumers experience them. Moreover, authorities should expect competition to discipline examples where self-preferencing is bad for consumers because those consumers can leave the platform due to demonstrably low switching costs. Just like other categories of market activity, an antitrust inquiry into self-preferencing is generally only appropriate where the company at issue has market power and where it is using that market power to harm competition and consumers.

iv. *The Developer Services Side of the Market*

Similarly, we encourage Brazil to conclude that its evidence base and the App Association's experience align with the conclusion that the developer services side of the market exhibits strong competition. Brazil should be especially wary of rash calls for the overapplication of antitrust law to digital platform activity on this side of the market. Some are seeking to leverage this trend to use the antitrust laws to punish their competitors based on gross overstatements of the problems they identify. For example, advocates for antitrust intervention point to the cost of the services software platforms provide to developers as evidence that policymakers should expand antitrust law. To show that paying for developer services is unfair, they compare the cost of software distribution to the cost of payment processing. However, payment processing is just one element of the array of services provided by a software platform, which include: immediate availability through hundreds of millions of devices; marketing through the app store; privacy features embedded in the platform; assistance with intellectual property protection; and security features built into the platform. The App Association urges Brazil to conclude that complaints about the costs of developer services paid to platforms are overstated because such costs are being compared to a much less substantial service and do not warrant an expansion of antitrust law or the creation of a new regulatory regime to reduce the price of developer services.

The other evidence advocates offer to show harm to competition occurs in making software available on the open internet free when it is not; software distribution on a platform costs money. As discussed above, selling software on the open internet requires the seller to take on several tasks the software platform bundles together (including marketing, intellectual property policing, privacy controls, security features, and payment processing). And even taking it at face value, the premise has the inconvenient characteristic of proving the opposite point—that is, selling software on the open internet can be a substitute for selling software on a platform. Notably, detractors of software platforms say they have no choice but to submit to software platform demands and then openly admit that they need not submit to software platform demands because they sell their software on the open internet instead. It is hard to imagine that this internal inconsistency goes unnoticed, and observers likely cannot help but discern from this that software sellers have options. Indeed, many other developers have made the transition between and amongst platforms without claims of anticompetitive conduct. Substitutes, even when they are not identical, are common in market economies and tend to signal healthy competition.

The other conclusion policymakers and enforcers should draw from these arguments is that policymakers should be wary of opportunistic behavior by well-resourced competitors disguised as antitrust concern. Those that are most vocal often imply they are speaking for the app economy as a whole, but in reality, they tend to be larger companies seeking to use antitrust law or other policy levers to undermine competitors. Right now, the largest software platforms generally charge the same (as a percentage of revenue) for developer services regardless of the company's size or political clout, or in some cases less for smaller developers. We note that Brazil omit

directly stating that the significant majority of developers pay no commission to software distribution platforms at all, though Brazil acknowledges the competitive and other pressures that have resulted in a reduction of fees, for those that do pay them, over time; a straightforward assessment of fees paid by developers to software distribution platforms is critical to Brazil's decision making, and we urge for revisions to be made to its report accordingly. Overtures to have policymakers involve themselves in developer-platform relations, therefore, may benefit the largest software companies on the platforms while leaving the small developers the App Association represents worse off. If large software companies convince policymakers to require software platforms to give them a better one-off deal, App Association members and their clients and customers are forced to subsidize the resulting discount for these larger companies. Adding insult to injury, many App Association member companies compete with these larger firms, so the benefit handed to the larger companies, in raising market barriers, would directly disadvantage App Association members.

Even as the antitrust concerns expressed in this area are often overstated, a competition analysis of these dynamics is not always the final say, and antitrust concerns may conflict with countervailing policy priorities. For example, policymakers have raised alarms over measures software platforms use to protect consumer privacy; in one instance, a software platform faced antitrust concerns after a decision to curtail apps' ability to track a consumer's location even when the app is not running unless the consumer clearly consents. Advocates exert a steady stream of pressure on software companies and platforms to improve their privacy practices, especially with respect to location data, often pointing to how companies collect such sensitive personal information. In reality, privacy controls at the platform level address this perceived problem by making it easier to set collection rules for all or specific apps.

Policymakers have long made it clear that companies should embed privacy into the design of their products and services. Accordingly, the purpose of a privacy prompt from the platform's operating system should not be to confuse a consumer into selecting an option that gives away more data than they intended. It follows that requiring platforms to make it easier to provide location data, even when an app is not running, than it is to protect that data—because doing so would help a specific app developer—runs headlong into the policy imperative of privacy by design. Moreover, the more privacy-protective approach of one software platform differentiates it competitively from other platforms that arguably make it easier for developers to collect sensitive data. In resolving these policy tangles, the focus should be on what works best for consumers. Antitrust law by itself rightfully addresses consumer welfare — it does not seek to benefit competitors. So, if a platform has an offering that a consumer prefers over the offering of an independent developer, policymakers should ask whether the complaints of powerful competitors necessitate legislating away that choice.

App Association members are selective about the markets they enter, but they compete aggressively. And the presence of a powerful and well-resourced competitor is not always enough to totally discourage entry. Having plentiful resources is an

undeniable advantage as a competitor (whether it is a platform or not), but our member companies exist because they fill a niche with a differentiated product, they can compete on price, or they can simply outmaneuver the larger competitors. The continued existence and success of camera apps on app stores is an example of companies competing directly with a platform. Thus far, Brazil's consideration has not fully explored the tradeoff between the platform and developers which funds platform integrity, which is critical to a holistic understanding of the development and utility of software distribution platforms.

But that is not to say a company with a competing offering should never be purchased by a larger company. There are three main definitions of success for a small company: passing the company along to the next generation; being purchased by a larger company; or (much less often) an initial public offering (IPO). Being purchased is often the best of these three options for the business owner and consumers. A purchase that helps produce better products or services for consumers is both a natural and beneficial end for some companies and healthy from a competition perspective.

e. Platforms' Role in Establishing and Maintaining Consumer Trust for Small Business Application Developers

At first, developers were reluctant to join platforms, worried that the model might not accommodate their need to launch fast and iterate their apps. But successful platforms changed the app ecosystem by providing app developers with ubiquitous access to a broader swath of consumers. Platforms provide a centralized framework for app developers to engage and secure visibility with billions of app users worldwide. With lower costs and barriers to entry, both fledgling and established app developers can find success.

One of the central markets at issue is the market for developer services, where a developer pays a platform for assorted services including distribution, marketing, etc. This market also experiences vigorous competition. As discussed *infra*, the market is much wider and includes a wide range of platforms.

i. *Platforms' Role in Addressing Cybersecurity and Privacy, Piracy, and Data Manageability and Migration*

Before the introduction of the smartphone and software distribution platforms, software developers built consumer trust slowly and at great expense, and that trust was and remains essential for a software developer to bring a product to market. Most did not have a widely recognizable brand to endorse the software. Prior to mobile platforms, software developers often had to break through the trust barrier by handing over their products to companies with a significant reputation. Even shareware products that could be digitally distributed would end up partnering with reputable brands to gain consumer trust. Today, consumers can download games like these for free on

platforms. These platforms not only lower costs by taking care of the significant overhead involved in selling their product, but they can also reach consumers much more easily. Today, consumer trust requires constant maintenance and vigilance because the loss of trust hurts both the platforms and the developers who rely on them.

A large majority of consumers regard privacy and security as an important aspect in deciding whether and where to interact with a software distribution platform. To compete with one another and attract both consumers and developers, leading platforms must provide a highly effective preliminary layer of defense against malicious apps. Rather than permitting users to download malicious apps in the hope that the last line of defense—the device operating system—will block the app's activities, the most competitive platforms utilize app review processes that screen apps for malware before they can be accessed by consumers. Such platforms also provide further protection by preventing apps from requesting unnecessary permissions that could jeopardize user privacy.

ii. *Platforms' Role in Addressing Piracy*

Before platforms, software developers struggled to safeguard their intellectual property (IP) against piracy and theft. Software companies faced serious challenges in protecting their products in retail stores because the licensing codes remained active and easy to steal. Once developers overcame the significant barriers to bring their products to market, they were faced with the threat of piracy and theft which limited their volume of business and hurt their bottom line. As far back as 2006, it was estimated that, on average, software developers lost BRL 31.9 million in revenue per year.

Before software developers could leverage dispute resolution mechanisms provided by platforms, developers were left with the significant burden of intellectual property infringement litigation in court, which could leave the legitimate IP owner with several thousand dollars per month in legal fees and months or years diverted from company matters. When the infringement originated abroad, software developers were at the mercy of foreign judicial systems, some even lacking rule of law and impartiality. Software developers and copyright holders continue to benefit from platforms' cost-effective avenues, such as their dispute resolution mechanisms referenced above, to distribute and protect the integrity of their products.

Despite all these platform-enabled advantages, for developers looking to reach a general audience, using the web is an alternative, especially for companies that are looking for different kinds of distribution or search services than those available on platforms. As discussed above, the differences between software platforms illustrate the diversity in the market for distribution methods, as developers may prefer one model over another.

Software platform safety and security are essential elements of developer services, particularly for enterprise app developers. Software platforms' security features have improved markedly over the course of their existence yet must continually adapt to address new vectors and threats. While unlocking a device used to require simply a four-digit passcode, devices are now capable of biometric authentication and software platforms make these authentication measures available to developers as well so that they can also offer these heightened security measures to their customers to build and maintain trust. But the game of cat-and-mouse between cybersecurity professionals and hackers will never end, and security must continue to evolve to meet and beat the threats. Although some platforms do not control device security, developers want the platform's security features to work seamlessly with any relevant hardware and account for all attack vectors. Software platforms should continue to improve their threat sharing and gathering capabilities to ensure they protect developers across the platform, regardless of where threats originate. Moreover, they should approve and deploy software updates with important security updates rapidly to protect consumers as well as developers and their clients and users.

Across the App Association's membership, consumer data is collected consistent with relevant laws and regulations for a range of purposes including "app functionality only" as well as "functionality and targeted advertising." Again, with the wide range of platforms available to our members, experiences and practices differ between platforms. The App Association believes that companies should build privacy into their products and services from the earliest stages and is committed to responsible and transparent data stewardship. Privacy prompts from a platform's operating system should result in an informed decision by a consumer about how their data is collected and used. Looking at the issue solely from a competition lens is, therefore, an incomplete view. Moreover, the more privacy protective approach of one software platform differentiates it competitively from other platforms that make it easier for developers to collect sensitive data. In resolving these policy tangles, the focus should be on what works best for consumers. Brazilian antitrust law by itself rightfully addresses adverse effects on competition and consumer welfare. So, if a platform has an offering that a consumer prefers over the offering of an independent developer, CADE (and other policymakers) should ask whether the complaints of powerful competitors necessitate legislating away that choice.

App Association members collect data that is tailored to the functioning of the services they offer and permitted by law/regulation and relevant platforms. App Association members also go to great lengths to use the latest technical protection mechanisms (e.g., end-to-end encryption) to protect any sensitive data they collect. Various platforms include features to allow for greater control of privacy by consumers themselves, which the App Association supports and benefits from through greater trust by consumers. The App Association works with members to ensure that privacy policies used to communicate with consumers reflect three key principles: (1) the policy should be clear, transparent, and outline not only data collection practices, but also data protection practices; (2) the policy must be clear about any third parties that are worked with (like advertisers, analytics services, etc.) and explain the access they

have to consumers' data and how they are expected to treat it; and (3) consumers should have the ability to access, change, and delete their data within a reasonable degree.

We strongly encourage Brazil to consult further with digital economy stakeholders who take measures to combat illegal contents and IP issues, as well as those who rely on such efforts, before advancing any proposals that would materially impact the ability to manage and mitigate piracy.

iii. *Platforms' Role in Supporting Data Manageability and Migration*

Due to platforms' efforts to enable purchases through a consumer's account with the platform, and the low switching costs between software distribution platforms, it is easier for consumers to manage their data and subscriptions, including by moving them to new devices, sharing them with family members, reviewing their purchase histories, and implementing parental controls. Besides providing convenience, this centralization helps protect consumers against subscription and data fraud and other violations that could result from sharing their financial information with unscrupulous developers. Consumers are thus willing to download more apps and spend more money on in-app purchases than they would if they had to manage their data and subscriptions across numerous platforms created by different developers.

Rigorous standards, app review processes, and in-app payments build consumer trust, which allows even small app developers to distribute their apps widely through the platforms. Indeed, when users trust a platform, they are more likely to try out new software applications, creating more opportunities for small business developers. This built-in consumer trust attracts developers to platforms and has led to consistent growth in the number and quality of apps available. And the commercial realities of the two-sided platforms being considered by Brazil thus belie unsupported claims of monopolization and anti-competitive conduct.

Relatedly, transparency in platform ranking and featuring, while helpful to our members, is not "crucial" to their success in a platform. While further insights into app store rankings would be beneficial (e.g., technical specifications, tools available to business users, etc.), software platforms may appropriately avoid disclosing all their related business operational details, such as their ranking specific algorithms. Other regulators, such as the European Commission (EC), have suggested various mandates in this area such as a transparency scorecard, including aspects like explanations given, ranking, and data captured/used. The App Association strongly cautions against new mechanisms that would unduly interject mandates into app store rankings that are evolving, exhibiting increased transparency, and which benefit small business developers.

i. *Platforms' Role in Supporting Data Manageability and Migration*

Just as app makers strive to build privacy into their offerings from the ground up with privacy by design, they also have a strong incentive to ensure people with all abilities can use them effectively. For example, the developer of an app that helps caregivers remotely screen and monitor patients with neurological disorders needs to ensure that those with cognitive disabilities can effectively use it. Similarly, an augmented reality app designed to tour homes could include voice descriptions of what appears on the screen for users with vision impairments.

For small app companies, these features historically existed as add-ons for consumers to seek on their own and too often did not present themselves as practical options for integration into the app everyone downloads. Some examples of screen readers would certainly require sight to install and set up, but also at least some facility with software (although setting up on mobile operating systems appears to be easier for some tools than on a desktop). Requiring people with disabilities to lean on others to integrate these features for them as aftermarket tools is a costly method of providing accessibility and is not ideal for app companies that want their offerings to be accessible out of the box.

This is where software marketplaces have improved the landscape for developers and consumers with disabilities, with developers heavily relying on such platform innovations today. For example, today's platforms allow a consumer to activate it with a verbal command on the device. As another example of how platforms provide developers with open access to a wide range of application programming interfaces (APIs), if a developer wants to ensure their app is accessible for those with vision impairments, they can integrate the VoiceOver API instead of building a separate functionality themselves. Or they could rely on their customers downloading third-party aftermarket tools, which has previously been the norm.

Further, proposals to prohibit software platforms from preferencing their own offerings on the platforms would reduce offerings of these accessibility tools as they are structured now. The problem with this outcome is that their integration with the operating systems and devices people use is a major part of what makes them feasible, effective, and affordable for developers and consumers. Not only that, but their disappearance from the marketplace would turn back the clock for smart device owners with disabilities so that they would once again have to rely primarily on aftermarket options. And those options would entail a greater resource investment in integrating them, a higher and unnecessary cost over and above the built-in feature option.

ii. *The Potential of Mandated Sideloading and the Harms to the Mobile App Economy*

As discussed above, software distribution platform review processes solve a collective action problem. Although a few unscrupulous developers might prefer to exploit users' private information for gain, allowing such apps onto a platform would erode consumers' trust in (and willingness to use) the platform. Small business developers rely on platforms' efforts to preserve the value of their platforms through such means as scrutinizing all apps on the platform to protect users' privacy and security. Indeed, efforts of such platforms to proactively require measures to protect data security and privacy in connection with data collection and storage widely benefit developers who need to gain and maintain end user trust and are a primary means of protecting the privacy of those same end users, a dynamic that enjoys wide support amongst the developer community (much to some outlier developers' chagrin who wish to upend today's mobile app economy simply to escape paying fees for access to platforms' benefits).

In general, mobile device users in Brazil download their apps through app stores that come preinstalled on their devices' operating systems. Operating systems and app stores come bundled together so that the operating system that runs the device can enforce the app store's terms of service and prevent unapproved apps from accessing device controls and consumer information. Unfortunately, a few of the largest companies in the app economy began a campaign to recruit policymakers to prohibit software platforms from managing the ability for consumers to download apps from outside the main app store. In other words, they want the government to require software platforms to allow sideloading, and in the case of some proposals, prohibit the platform from even warning a consumer of the potential harms of sideloading apps.

Notably, two major software platforms take robust measures to prevent sideloading of unvetted software that could harm consumers. For example, because iOS prohibits sideloading (downloading software onto a smart device from outside the main app store), and Apple's App Store's terms of service bar copyright theft, sideloaded apps that steal content are difficult to install on an iOS device. Similarly, Android presents problems for copyright thieves, because the Google Play store also generally declines apps that engage in or facilitate piracy, and by default, the current (and recent) versions of Android disallow sideloading; however, by going into the settings, users can allow sideloading from "unknown sources," one at a time.

Software platform features that discourage sideloading protect consumers from malicious actors using malware installed on sideloaded apps to access personal information and commit criminal acts. Moreover, copyright owners, from the individual to major entertainment companies, use tools available under current law to remove counterfeit apps and apps that stream movies, music, and television illegally. Still, sideloaded apps appeal to consumers primarily because they are often free and offer access to streamed content without paying, including the most popular streaming and

TV shows. Statutory or court-ordered mandates on software platforms to allow unvetted software onto these platforms will come at a cost to copyright owners and their customers.

Proposed government interventions that would stop platforms from prohibiting sideloading will weaken the effectiveness of the notice-and-takedown procedures (such as laws that support software platforms to remove illegal apps by providing limited liability for online service providers that implement certain measures to prevent piracy, including quickly responding to requests from copyright owners to takedown infringing material). We strongly urge Brazil (and other policymakers and stakeholders) to consider how ineffective takedowns under Brazilian laws would be if a software platform must allow any app or app store on mobile devices. For example, if a fraudster specializing in stolen video content, posing as a fake Disney+, sought to have consumers sideload their video apps in order to upload malware onto as many personal devices as possible, pro-sideloading proposals would bar a platform like Apple from removing that app and from blocking its access to device features or personal information because it nominally competes with Apple TV+. The presumption of illegality would apply even if Disney filed a takedown notice. This situation would tie the platform's hands, and they could face liability for compliance with a takedown notice, effectively eliminating a platform's ability to address piracy.

Government mandates for app stores to allow unvetted third-party apps onto smart devices will increase consumer exposure to risk of malware giving hackers access to users' personal information. For most consumers who want to sideload third-party apps, they have to either "jailbreak" their device or use device settings to allow trusted apps to be downloaded. This layer of restrictions provides simple but effective barriers to malicious actors having access to unwitting consumers. Counterfeit software apps can and do lead to consumer data loss, interruption of service, malfunctioning devices, loss of access to content, voiding device warranties, identity theft, fraud, and even civil and criminal prosecution for copyright infringement.

Clearly, the cost to consumers is great, but so too is the harm to a business's reputation and revenue. Businesses providing content and services have a strong interest in protecting their customers. Piracy and counterfeit software apps threaten end-user confidence and can lead to reputational damage. These costs may be difficult to quantify, but they are nonetheless undeniable. It is critical that regulators including Brazil do not put counterfeit apps on equal footing with legitimate apps in the mobile ecosystem, leaving consumers exposed should they download the wrong one. Software platforms perform a necessary and important role in providing a safe online market that benefits both content providers and their customers. Having several options and flexibility to manage smart devices is also good. But letting cyber criminals set up shop inside the app marketplace will result in more piracy, lost revenue, and customer dissatisfaction. For these and the above reasons, we strongly caution Brazil against pursuing legislation that prevents software platforms from removing counterfeit apps and other stolen content.

f. Signs of Competitive Health in the Mobile App Economy: Platforms Unlock New Markets

As successful as the past decade plus has been for the app economy, the next decade could be even better. As noted above, exponential growth for software apps distributed through curated app stores continues to positively transform countless consumer and enterprise use cases and markets. This growth and job creation strongly indicates that the developer-platform model is still succeeding. Moreover, app economy growth is likely to endure because developers are continuing to create new products, services, and markets that did not exist prior to platforms. A notable example of the app economy's ingenuity was in combatting the COVID-19 pandemic, where mobile apps have been effectively utilized for contact tracing notifications to assist in minimizing the spread of the disease, saving countless lives.

Perhaps most importantly, the universe of platforms is continuing to evolve and expand as diverse kinds of hardware connect to the network. For example, new platforms are cropping up for wearables. Connected home devices and cars drive cross-platform interoperability so that voice-assisted capabilities can communicate with other devices — further weighing against conceptions of platform markets where a single player wields market power and indicating that developer services will continue to improve and evolve along with demand.

Another area where platforms enable developers to reach new audiences is through accessibility tools. Mobile operating systems are built with powerful accessibility tools for developers to use in creating apps that enhance the lives of the disabled. Whether it is voice directions in a mapping app for the visually impaired or text to speech tools for those with a speech-language disorder, offering these tools as part of a developer tool kit assists any app in reaching a wider audience.

In addressing transparency in digital platform operations, Brazil has raised the issue of featuring and ranking in app stores. App Association app developer members often are featured based on their design of a sleek user interface and intuitive user experience, updating their app(s) regularly, optimizing app localizations, making the app accessible to those with disabilities, gathering reviews, and creating an app preview. On the App Store, for example, sharing information with the App Store editorial team (through https://developer.apple.com/contact/app-store/promote/) can be an optimal way to get featured. Google Play is more algorithm-driven (rather than editorial-driven); on Google platforms, it is more important to get discovered by users and start trending to be noticed, and the app title, number of downloads, good ratings, and price are the main factors that determine search rank. Other platforms take different approaches, which are differentiators for them as the platforms compete against one another.

Generally, platform transparency, including with respect to ranking and featuring in app stores, is important to our members and any business users to increase their

ability to plan ahead and attain legal certainty for their business but is not crucial to our members' success in a platform, and we appreciate Brazil's examination of this issue within its Inquiry. The App Association believes that there are different levels of transparency and notes that while more information on some levels can be beneficial (e.g., technical specifications, tools available to business users), platforms should not be obligated to disclose all their business operational details, such as their ranking-specific algorithms. Full and complete transparency would make search ranking manipulation nominal and fill the app stores with spam. It is important to allow the platforms enough flexibility to continue to optimize their search and ranking algorithms and stay ahead of those who are trying to game the system.

g. The Negative Impact of Platform Mandates on Global Trade

Policymakers should recognize DMA (and similar competition platform interventions) as a trade barrier intended to discriminate against those viewed as foreign competitors in the digital economy, in particular Brazilian digital innovators. Notably, the United States Trade Representative did so recently when it categorized DMA as a barrier to digital trade in its annual National Trade Estimate.[10] The DMA is antithetical to the free and fair trade principles and conditions that have enabled mobile economy success and growth, and the potential of its replication in other important markets is a threat to innovation and job creation. This conclusion emerges through analyses of the DMA from several angles:

- The DMA's "Gatekeeper" Scope
- DMA Prohibitions as Non-Tariff Trade Barriers (NTBs)
- Non-Discrimination under World Trade Organization Agreements
- DMA Trade Concerns in a Global Context

The DMA's "Gatekeeper" Scope. Even on its face, the scope of the DMA raises discrimination concerns. The DMA applies only to entities the European Commission (EC) deems to be "gatekeepers." In making such a determination, the EC analyzes whether a given entity meets each of these three *qualitative* criteria: (1) "it has a significant impact on the internal market"; (2) "it provides a core platform service that is an important gateway for business users to reach end users"; and (3) "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."[11] However, a set of *quantitative* factors creates a presumption for the EC that an entity meets the qualitative test: "(1) it had annual EU

[10] UNITED STATES TRADE REP., NAT'L TRADE ESTIMATE REPORT ON FOREIGN TRADE BARRIERS (Apr. 2023), *available at* https://ustr.gov/sites/default/files/2023-03/2023%20NTE%20Report.pdf.

[11] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, Art. 3(1), *available at* https://eur-lex.europa.eu/eli/reg/2022/1925/oj [Digital Markets Act (DMA)]

turnover of at least EUR 7.5 billion in each of the last three financial years, or where its average market capitalization or its equivalent fair market value was at least EUR 75 billion in the last financial year, and it provides the same core platform service in at least three Member States; (2) it provides a core platform service that in the last financial year has at least 45 million monthly active end users and at least 10,000 yearly active business users in the EU; and (3) the thresholds in (2) were met in each of the last three financial years."[12]

Although the qualitative factors give the EC wide discretion to deem large businesses "gatekeepers" and subject them to the DMA, much of the debate has focused on the quantitative factors, since those create the presumption that the qualitative factors are met. The presumption appears tailored to apply to large platform companies while excluding European counterparts with which they compete. Even the largest European companies that operate online marketplaces, such as Spotify, may not meet the criteria: although Spotify's value has fluctuated recently, it remains well below the EUR 75 billion enterprise value threshold. Europe's other largest companies do not appear to meet the qualitative thresholds at this point, so Spotify tends to be cited most in the context of whether DMA declines to cover all European platforms or just almost all of them. Interestingly, Booking.com is frequently cited by EU policymakers as a European company that could be subject to the rules, but it is a fully-owned subsidiary of Booking Holdings headquartered in Connecticut, further underlining the de facto reality that the rules only apply to non-EU firms. Regardless of what the numbers say, there is evidence that European policymakers intended to cover foreign companies in an effort to support European firms. Members of the European Parliament have publicly confirmed as much.[13]

On top of this legislative history, the DMA targets several online marketplaces and platforms with business models that have very little in common and that compete in completely different markets. The fact that the same DMA provisions apply to both a social media platform—which derives a substantial amount of its revenue from behavioral advertising—and to a retail platform, which derives revenue from sellers and subscribers, is a clear indicator that the scope's purpose is unrelated to the kind of markets in which covered entities compete or whether any harm to customers, competition or the EU Internal Market has occurred. One would expect policymakers to tailor regulations intended to mitigate harms to competition and consumers more to companies that compete in at least the same kinds of markets, such that potential harms arising from their conduct have similar enough attributes to be subject to common rules. In a period of high inflation, reducing competitive pressure between retailers, for example—some of which are regulated under DMA and some of which are not—could be counter-productive.

---

[12] Vanessa Anne-Marie Turner, "The EU Digital Markets Act – A New Dawn for Digital Markets?" AMER. BAR ASSOC., Vol. 37, Issue 1 (Fall 2022), *available at* https://www.americanbar.org/groups/antitrust_law/resources/magazine/2022-fall/eu-digital-markets-act/?login (citing DMA, Art. 3(2)).

[13] "EU should focus on top 5 tech companies, says leading MEP," FIN. TIMES, *available at* https://www.ft.com/content/49f3d7f2-30d5-4336-87ad-eea0ee0ecc7b (paywall).

The evidence from both the legislative intent of the DMA and its quantitative factors suggests that the scope itself of the DMA may raise discrimination questions under a WTO agreement analysis. Under the General Agreement on Trade and Services (GATS), a member government may exhibit discriminatory conduct if it accords to competitors based in another member's jurisdiction "less favourable" treatment than "like services and service suppliers" based domestically. Ironically, one of the DMA's pillars is a prohibition on favorable treatment by a covered platform for its own services offered via the platform. So it may be that the EC is culpable of the same kind of discriminatory conduct the DMA sets out to mitigate and prevent. A notable difference, however, is that the DMA's scope is not limited to companies with demonstrable market power that might enable price increases or output restrictions that would go unpunished by market discipline. The EC, meanwhile, may exercise political power in substantial excess of any form of market power contemplated under EU competition law analyses or Brazilian antitrust law doctrine. That is, it can unilaterally affect the output or price of a market or market actors with the adoption of a new law. Therefore, there is at least an equally strong, trade-related public interest in scrutinizing the use of government power to discriminate against certain companies based on their national origin, as there is in pursuing a law to prevent analogous discrimination in online markets.

DMA Prohibitions as Non-Tariff Trade Barriers (NTBs). Inextricable from the question of whether the scope of the DMA is discriminatory is the problem of whether the content of its requirements imposes unjustifiable burdens on marketplaces and platforms within its scope. Although Member States have yet to adopt WTO agreements specific to *competition* policy in the context of NTBs, there are relevant analytical and diplomatic frameworks to draw from on this issue. For example, Member States agreed to establish "a working group to study issues raised by Members relating to the interaction between trade and competition policy, including anti-competitive practices, in order to identify any areas that may merit further consideration in the WTO framework."[14] Similarly, the recently established U.S.-EU Trade and Technology Council (TTC) provides a bilateral venue for negotiators to address potential NTBs and align policy approaches on a variety of tech-related issues.[15] In fact, one of TTC's subgroups—Working Group 5—specifically covers "data governance and technology platforms."[16] In the U.S.-EU joint statement establishing TTC, the signatories stated that they "recognize the global nature of online platform services and aim to cooperate on the enforcement of our respective

[14] Singapore Ministerial Declaration, World Trade Org., (adopted Dec. 13, 1996), *available at* https://www.wto.org/english/thewto_e/minist_e/min96_e/wtodec_e.htm.

[15] U.S.-EU TRADE AND TECH. COUNCIL, OFFC. OF THE U. S. TRADE REP., EXEC. OFFC. OF THE PRES. (announced Jun. 2021), *available at* https://ustr.gov/useuttc.

[16] Euro. Comm'n, EU – US Trade and Tech. Council, Working Group 5 – Data Governance and Tech. Platforms, *available at* https://futurium.ec.europa.eu/en/EU-US-TTC/wg5.

policies for ensuring a safe, fair, and open online environment."[17] The recognition of the global nature of online platforms may help guide whether and to what extent a signatory's policy related to online platforms constitutes an NTB or similar barrier under any agreement the parties choose to adopt.

Two sets of DMA obligations may interfere with the global nature of platforms as well as the extent to which they can foster a safe, fair, and open online environment. First, the DMA's Art. 6(4) would require a covered gatekeeper to "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."[18] Two caveats attempt to ameliorate the obvious security and privacy issues this mandate would create. The first is that the gatekeeper "shall not be prevented" from taking measures to ensure that third-party apps or app stores do not "endanger the integrity of the hardware or operating system," but only to the "extent they are strictly necessary and proportionate" and if they are "duly justified by the gatekeeper." The second is that the gatekeeper "shall not be prevented" from applying measures and settings other than defaults that enable end users to effectively protect security against third parties, but again, only "to the extent that they are strictly necessary and proportionate" and "duly justified by the gatekeeper."

Even if the evidentiary burden implied by "strictly necessary and appropriate" and "duly justified" were relatively easy to meet (and it likely is not), limiting the exceptions to threats that "endanger the integrity of the hardware or operating system" is rather narrow and fails to include a wide range of cyber threats and consumer harms. Thus, the presumption in Art. 6(4) weighs heavily against any security measures and certainly precludes the proactive security structure that currently protects small app companies and users, at least presumptively. For example, the major global app stores currently vet apps before approving them for sale, verifying that they limit their data collection activities and access to sensitive device functions like the camera and precise geographic location only to those necessary to serve the apps' purposes. The stores effectuate removal of the apps that trick consumers into allowing collection of more sensitive data for nefarious purposes by revoking their access, which was only granted in the first place based on having passed the vetting process. Now, if the DMA illegalizes that structure, app stores may be required to allow apps that intentionally harm consumers to appear on the store alongside legitimate developers' software, while also eliminating the technical mechanism app platforms use now to revoke access. Unless these issues are addressed in implementation, the result would greatly increase threats to safety and fairness on the platforms and ultimately, to the global nature of the online platforms themselves. These consequences would likely be a

[17] U.S.-EU Joint Stmt. of the Trade and Tech. Council, May 16, 2022, Paris-Saclay, France, para. 12, *available at* https://www.commerce.gov/sites/default/files/2022-05/US-EU-Joint-Statement-Trade-Technology-Council.pdf.

[18] DMA Art. 5(4).

focus of TTC negotiators and other trade venues focused on potential digital trade NTBs.

A second set of requirements in the DMA, Articles 6(7) and 6(10), work together to inadvertently provide an advantage to China-based competitors and bad actors. Specifically, Article 6(7) would require the gatekeeper to provide the same level of interoperability with the operating system and other software and the device features as are provided to the gatekeeper's own offerings.[19] On top of this, Article 6(10) would require the gatekeeper entity to provide "high-quality, continuous and real-time access to . . . non-aggregated data, including personal data . . .."[20] The DMA limits the applicability of the requirement only to personal data that is directly connected to a "use effectuated by the end users in respect of the products or services offered by the relevant business user . . . and where the end users opt-in to such sharing by giving their consent."[21] Unfortunately, this limitation may not be narrow enough to undo the mandate for gatekeepers to share personal information with platforms or online marketplaces owned by foreign adversary-controlled entities. Similarly, Article 6(7) may require gatekeepers to provide the best possible access to European and Brazilian consumers' devices, operating systems, and other software on their devices to entities controlled by foreign adversaries. Just as problematically, such must-carry mandates complicate or thwart efforts to remove business users with a repeated and persistent track record of violating consumer protection law with dark patterns and privacy violations.[22] Coupled with Article 6(10)'s requirement to provide continuous access to sensitive information, the mandates could also be a form of mandatory tech transfer from innovation leaders to governments that do not protect fundamental human rights and democracy. Viewed in this light, the DMA may constitute an extraordinarily costly barrier to trade for Brazilian businesses while also undermining the EU's global diplomatic and economic interests.

Non-Discrimination under World Trade Organization Agreements. In each of the three main World Trade Organization (WTO) agreements, signatory governments must generally treat domestic and foreign goods and services covered under the agreements equally. Specifically, Article 3 of the General Agreement on Tariffs and Trade (GATT),[23] Article 17 of the General Agreement on Trade and Services (GATS),[24] and Article 3 of the Trade-Related Aspects of Intellectual Property Rights

---

[19] DMA, Art. 6(7).

[20] DMA, Art. 6(10).

[21] *Id.*

[22] Letter from Morgan Reed, president, ACT | The App Association, to Senate Commerce, Transportation, and Science leadership, re: Fed. Trade Comm'n settlement with Epic Games, *available at* https://actonline.org/wp-content/uploads/2023-02-15-ACT-FTC-Settlement-Letter-to-Senate-Commerce.pdf.

[23] General Agreement on Tariffs and Trade (GATT), Art. 3, Apr. 15, 1994, *available at* https://www.wto.org/english/docs_e/legal_e/legal_e.htm#GATT94.

[24] General Agreement on Trade in Services (GATS), Art. XVII, *available at* https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm#articleXVII [GATS].

(TRIPS)[25] each outline this non-discrimination obligation. Each of the provisions handles the non-discrimination slightly differently, but the most relevant agreement for purposes of the DMA, GATS, is fairly straightforward in how it likely applies to the regulatory treatment of online marketplaces. Article 17 provides that each Member, "shall accord to services and service suppliers of any other Member . . . treatment no less favourable than that it accords to its own like services and service suppliers."[26] The obligation only applies once a service has entered the EU market, and it is likely that the major online marketplaces and platforms meet that threshold, given how widespread their use is in Europe.

DMA Trade Concerns in a Global Context. As policymakers continue to discuss trade implications of tech-related policies, the DMA's potential discriminatory effect on online marketplaces will undoubtedly be a focus. Given the EC's willingness to assert its own interests, policymakers should not shy away from firmly articulating critical national and global interests of the innovators and consumers they seek to support. The objections policymakers should have run deeper than the fact that the DMA's scope intends to capture only certain platforms and that compliance with it is costly. The content of the DMA's restrictions also potentially contravenes treaty-based commitments to protect the global nature of these valuable platforms as well as their ability to foster fair and safe online exchanges and commerce, including in constructs such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). It will also be hard for negotiators to ignore that the imposition of costs specifically on their marketplaces would hamper their ability to invest heavily in research and development of cutting-edge technologies. A substantial diminution of our industry leaders' investment incentives would weaken our economic and national security. Protecting against this outcome must be a high priority for trade policy officials.

These issues arise at a critical time when several countries are seriously considering similar regulatory frameworks targeting online marketplaces. These proposals have, albeit in slightly different ways, tentatively sought to incorporate some of the fundamental elements of DMA into their frameworks. Not only that, but the EU has also built on the basic DMA framework in further legislative work. For example, EU legislators have begun to carry the "gatekeeper" concept into new legislative proposals like the EU Data Act. Under this new legislation a DMA gatekeeper would be prevented from exercising rights given to other companies, regardless of its competitive strengths or weakness, thus further reducing competitive pressures. The DMA's trade implications, therefore, warrant further study and analysis to better understand why policymakers should resist its wholesale importation to the rest of the globe and to inform its implementation by the EC. Policymakers should take note and push back on the key assumptions that undergird DMA, and similar proposals, to help

[25] Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Art. 3, Apr. 15, 1994, *available at* https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm.

[26] GATS Art. 17, para. 1.

government officials around the world evaluate the significant costs interventions like it would impose with open eyes.

III. App Association Responses to Specific Questions Posed by Brazilian Policymakers

Based on the above, the App Association provides the following responses to questions posed by Brazilian policymakers, which are relevant to this consultation:

1. **Related to "essential facilities" in the universe of digital markets, can commenters give examples of platform assets in the digital market operating in Brazil where at the same time: a) there are no digital platforms with substitute assets close to these assets b) these assets are difficult to duplicate efficiently at least close to the owning company c) without access to this asset, it would not be possible to operate in one or more markets, as it constitutes a fundamental input?**

The App Association strongly discourages the application of the essential facilities doctrine to digital markets. The essential facilities competition law doctrine, which CADE has incorporated into Brazil's competition policy, is based on U.S. law that places an obligation on a company to provide access to "essential facilities" under certain conditions to support competitive goals in the face of high costs and the impossibility and infeasibility of replication of the good (not mere inconvenience or at the cost of some economic loss). As discussed above, digital platforms exhibit significant signs of strong competition due to the low barriers and costs of collaboration with, and even the creation of, digital platforms. Further, as discussed above, digital platforms can be bypassed by consumers and businesses (websites offer alternatives to digital platforms for retailers). Nor do significant barriers to entry in the form of permissions and licenses from the government (such as those required for electricity infrastructure) exist for digital platforms. In sum, the prerequisites for applying the essential facilities doctrine to digital platforms are not present.

Notably, CADE has already rejected the application of the essential facilities doctrine to digital platforms and services in the context of Google Shopping, finding that Google's first page of search results is not irreplaceable as there are many other ways for consumers to find what they need online and that Google does not mediate website access; CADE further determined thatf its intervention would only accomplish forcing Google to make its search less effective, which would push consumers to other search engines.[27] CADE's thoughtful approach in that case sets an important precedent that certainly applies in the context of Bill 2768/2022 causing the essential facilities doctrine to be applied to digital platforms writ large. No digital platform is

[27] Commissioner Mauricio Maia's reporting majority decision in Administrative Procedure No. 08012.010483/2011-94 (Defendants: Google Inc. and Google Brasil Internet Ltda.).

presently the only option available or the sole point of access between consumers and businesses.

2. **Is regulation necessary to guarantee access to the asset (s) of the example (s) from question 1? What should such regulation guarantee so that access to the asset enables third parties to enter those digital markets?**

No. A Brazilian regulation applying the essential facilities doctrine to digital platforms would be overburdensome, is not necessary, and would prevent innovation for countless small businesses that rely on digital platform competition to grow and create jobs. Every day, App Association members leverage seamless entry into and across digital platforms and distorting this pro-competitive dynamic via government regulation would, effectively, entrench existing digital platforms that our members seek to disrupt and compete with, as government regulation has the effect of making it easier to access existing offerings under circumstances set by that regulation in comparison to creating alternative solutions. The application of the essential facilities doctrine would, for the digital economy, also promote exclusion of our members from platforms. We strongly encourage careful consideration of the unintended consequences of applying the essential facilities doctrine to digital platforms, after which it must be concluded that such application is entirely inappropriate and would be unprecedented.

3. **Can commenters describe cases in digital markets where there is at least one other company with substitute assets close to these assets of the main company, but none of the digital platforms that hold the asset provide access to it. In other words, even if there is more than one asset in the market, there is still a problem of accessing the asset. How could Bill 2768/2022, especially its article 10, be improved to improve access to essential supplies?**

The App Association objects to this question's presumption that the essential facilities doctrine should be applied to digital platforms, as described in previous answers above. A mere preference between one or more assets does not begin to approach the threshold needed to deem an asset "essential."

4. **Can commenters describe cases in which the ownership of data in digital markets creates a barrier to entry that makes it very difficult or even impossible for incumbent digital platforms to enter the market. How could Bill 2768/2022 mitigate this problem, reducing the barrier to entry represented by access to data?**

For small businesses, access to large amounts of data is not necessary to enter digital markets. Success for a small business in the digital economy will primarily center on how innovative a product or service it is offering for end users. Holding large amounts

of data does not assure success in any digital markets. Further, as described above, small businesses significantly benefit from the services platforms offer that are built on data, and they gain access to many vital datasets via those same platforms.

5. **Can commenters cite to cases in which a company in the digital market in Brazil used third-party data because of its characteristic as an essential input provider, harming the third party competitively?**

No, the App Association knows of no applicable scenarios, and again objects to the presumption that the essential facilities doctrine should be applied to digital platforms.

6. **Can commenters describe cases in which a difficulty in interoperability with a company's systems makes it very difficult or impossible to enter one or more digital markets. How could PL 2768/2022 mitigate this problem, reducing the barrier to entry represented by lack of interoperability?**

An interoperability mandate should only be enacted in response to well-demonstrated harms and a market failure (and not hypotheticals or rare edge use cases). As discussed above, the digital platform market has no indicators that would support such a mandate.

While the example is from another jurisdiction, one example of where such an interoperability mandate was enacted is in the context of electronic health record data in the United States.[28] This policy was only enacted after extensive study of a strong evidence base demonstrating bipartisan recognition of systemic issues distorting that market.

7. **The European Digital Market Act (DMA) chose to implement absolute prohibitions (per se) on some conduct in digital markets, such as self-preferencing, among others. Brazil's Bill 2768/2022, on the other hand, chose not to do any prohibited conduct ex ante. Should there be one or more conducts with absolute prohibitions (per se)?**

Past proposals, including Bill 2768/2022, have appropriately avoided declaring per se prohibitions and should not shift to mirror the DMA's one-size-fits-all approach to digital platform practices. Such practices should be evaluated on a case-by-case basis and addressed through a scaled approach to mitigating demonstrated harms.

The DMA's implementation, which is ongoing, continues to illuminate how blanket bans across diverse markets in the digital economy are intensely difficult to operationalize and comply with, and calls into question how the DMA's provisions will

[28] https://www.healthit.gov/topic/information-blocking.

accomplish European policymakers' goals. Rather than build a regulation around technology- and modality-neutral goals, the DMA has put a framework in place responding to unique and edge use cases that it is applying to the entire digital economy. Brazil's approach has not, and should not, shift to mirror the approach to digital platform regulation in the DMA; at a minimum, Brazil should observe the impacts of the DMA's implementation before considering adopting similar approaches.

8. **Would there be behaviors in digital markets that would have a high potential to entail competitive problems, but which can be justified as generating greater efficiency for companies, transactions, and markets? Give examples of these behaviors? How should these behaviors be treated? In particular, a "reversal of the burden of proof" would be appropriate, in which such conduct would presumably be anti-competitive, but would it be appropriate to authorize a defense of digital platforms based on these efficiencies? Should these behaviors be considered not prohibited per se, but as a "reversal of the burden of proof"?**

Evaluating behaviors in digital markets should be approached like non-digital markets in the sense that policy changes or enforcement actions should be based on established harms. In multi-sided markets, like with digital platforms, a behavior may have both competitive and anti-competitive effects, and each case should be approached consistently. Therefore, creating a presumption of anti-competitive effects for certain behaviors by shifting the burden of proof is inappropriate, particularly for new and dynamic markets like digital platforms. Small businesses lacking in resources will be pushed away from entire use cases and markets should their behavior be automatically assumed to be anticompetitive.

9. **Is there a need for a regulator? If so, which regulator would be better able to implement the regulation (Anatel, CADE, ANPD, another existing or new regulator)?**

It is not possible to assess the creation of new institutions or use of an existing regulator without clear definition of the issues that Brazilian digital platform regulatory proposals seek to correct; since the problems this bill would address are not clear, recommending a regulator is not possible. Today, rules enforced by various Brazilian regulators, such as CADE, address the actors and behaviors Brazil seeks to focus on. Creating a new agency, or expanding the authority of agencies like ANPD, would discard the need for the important role Brazil's different enforcers have today, which support digital economy competition and would overlap or conflict with the authorities some of these agencies have to address competition, whether in a digital or other modality. The App Association therefore believes that new platform regulation in Brazil is unnecessary and harmful.

10. Do you think that there could be any risk of bis in idem between the regulator and the competition authority with the same conduct being analyzed by both?

Yes, new regulation would raise significant risk of overlap with Law No. 12,529/11, creating double liability for the same acts found to be harming competition. This is a significant problem that must be addressed before any new regulations move forward.

Brazil's existing legal frameworks provide a comprehensive set of tools to address anti-competitive conduct, and current competition law and its enforcement therefore already captures and is resourced to address principles included in proposals such as Bill 2768. Digital economy issues at issue in this consultation, (e.g., interoperability, data portability, etc.) can already be addressed within the purview of exclusionary conduct and foreclosure theories of harm and can readily be addressed using the current legal framework. Specifically, CADE already exercises its authority across all sectors, including digital markets, in order to promote the fundamental principles of competition policy (for example, to avoid anti-competitive conduct), which include all the risks listed in the consultation. Further, CADE investigations consistently focused on specific facts and circumstances, which is an appropriate approach to enforcement as discussed above.

11. Is it necessary to tie revenue to a designation of essential service-to-service access control power?

The App Association believes that Article 9 is misguided because there is no demonstrable and consistent relationship between a company's revenues and having "essential access control power." As discussed above, revenue and other quantitative measures such as user count are not necessarily indicative of market concentration or dominance. Nor do such metrics consistently or accurately indicate market failures (e.g., significant monopolistic abuses can and do occur in low revenue and low user count scenarios). We strongly encourage alignment with time-tested antitrust principles (e.g., the availability of substitutes) described above, which also already rest in existing Brazilian competition law.

12. What are your views on the potential of a Digital Platforms Supervisory Fund (e.g., in art. 15 of Bill 2768/2022)? Is there another way to finance this type of government regulatory activity?

The App Association strongly encourages for a clear definition of the distinct and new problems that must be solved, based on evidence demonstrating systemic issues, before putting a new funding mechanism in place. When examining this question, we urge for consideration of the burdens on the App Association's small business community, both directly and indirectly.

13. To what extent do you believe that alleged problems addressed in Bill 2768/2022 are already adequately addressed by competition law, more specifically by CADE, with the instruments of Law No. 12,529 of 2011?

All of Bill 2768/2022's concerns, to the extent they are clearly defined, are already addressed by existing competition law. Risks associated with interoperability, data portability, data processing, use, storage, and concentration all fall within the purview of exclusionary conduct and foreclosure theories of harm and can readily be addressed using the current legal framework in Article 36, lines V, VIII IX, and X of Law No. 12,529/11. Current competition law and the application of international best practices in competition enforcement will best account for risks across digital markets stemming from market concentration and abuse of economic power while fostering competition and innovation.

Brazil's 2011 Competition Law was enacted after extensive legislative debate led to an agreement to strengthen CADE's investigative powers because of a recognition that there was evidence that identified harms could not be addressed through the existing regime. The existing legal framework has proven to be flexible, and CADE has achieved a high degree of success using it to protect competition. To accomplish these goals, CADE can bring forward court proceedings, accept court enforceable undertakings, impose the "accounting and functional separation" measures, issue infringement notices, issue public warning notices, adopt injunctions in urgent matters, resolve matters administratively, and undertake education campaigns and other compliance initiatives (some of which Bill 2768/2022 would duplicatively assign to ANATEL).

14. What problems could be generated for the innovation activity of digital platforms if there is the regulation of digital platforms by the Brazilian government?

Building on our extensive comments above, there are clearly significant problems that would be generated from the regulation of digital platforms proposed in Brazil. Small businesses in the digital economy rely on platforms for features that streamline privacy, security, intellectual property, and the provision of accessibility for those with disabilities, and this dynamic would substantially alter this symbiotic relationship (which has still not been taken into account throughout consultations and debate of Bill 2768/2022 to date). As discussed above in our general views and in answers to previous questions, harms of enacting new platform regulation in Brazil include reducing opportunities for small businesses and startups to engage in the digital economy, reduced trust in the digital economy due to heightened privacy and cybersecurity exploitations, and, ultimately, harm to Brazilian consumers through reduced choice and higher prices. We again caution against mirroring provisions in the DMA, which have not yet been implemented and for which their impacts have not been measured or understood.

15. What would be the practical difficulties of applying digital platform regulation in Brazil?

The danger of imposing general rules and obligations on digital platforms is, at its core, that there will be immense uncertainty about its scope and application due to the subjective nature of its requirements. The business community, and the small business innovator community that the App Association represents specifically, will have great difficulty for a minimum of years (until adequate judicialization occurs) understanding how to operationalize the impacts of this new policy in Brazil, chilling their ability to take risks in Brazilian markets.

We again caution Brazil against mirroring the unproven and not fully implemented DMA and encourage the careful study of its implementation before moving forward with similar regulation in Brazil. Our discussion above elaborates on the dynamics of digital platforms that bring immense benefit to small business developers.

16. Do you see a lot of room for the judicialization of digital platform regulation?

Yes, absolutely. Proposals like Bill 2768/2022, which mirror the DMA and its definitions, goals, and means of enforcement are ambiguous and susceptible to wildly different interpretations. Because of so much uncertainty, litigation will certainly be required to clarify the meaning of the broad language adopted in the bill, unless it is drastically improved.

17. Are the definitions in Brazilian platform regulatory proposals (e.g., article 6 of Bill 2768/2022) adequate for the purpose of this proposal?

No. Article 6 mirrors definitions in the DMA, which is written to target specific companies in different sectors with different business models and utilizes a blanket approach to the digital economy and competition that contradicts Brazil's approach to regulation by CADE discussed above. Article 6's definitions would perpetuate this one-size-fits-all approach that ignores differences between business models and the differences between different markets, also giving rise to conflicts with existing Brazilian law protecting competition. For example, proposing a scope that applies to digital or online services presents a subjective scope contributes to uncertainty and reduces confidence in the rule of law in Brazil, discouraging new market entrants and their innovations. The App Association urges further study and consideration to address this problem and others described elsewhere in this comment.

18. Instead of pure ex-ante regulation, would any other type of monitoring and/or regulation of digital markets make sense?

The App Association reiterates that competition law enforcement must be based on strong evidence and careful economic analysis to ensure that enforcement is appropriate and is addressing actual harms to competition. Indeed, monitoring of any market for signs of harm to competition is appropriate to support this enforcement. Current Brazilian competition law already addresses the possibility of ex post enforcement applicable in digital markets and enables the government to understand markets and to protect consumers over time.

19. Are the set of solutions described in art. 10 of Bill 2768/2022 adequate?

Bill 2768/2022 describes four subjective principles that cannot be consistently interpreted by the small business community or others, and states that an enforcement authority may impose further obligations for abuses such as in the context of data portability and interoperability. The unspecific nature of Article 10 will enable ANATEL to enforce remedies in the digital economy unchecked and invites inconsistent approaches to enforcement that will create uncertainties and harm innovation. Ideally, the powers (and limits to those powers) of an enforcement authority like ANATEL will be clearly defined to provide clear rules of the road for all actors.

20. Are the sanctions provided for in art. 16 of Bill 2768/2022 adequate?

Bill 2768/2022 fails to define the precise situations in which ANATEL would be allowed to impose penalties and does not clarify whether the 2 percent penalty applies to global or Brazilian revenue. Further, Bill 2768/2022's sanctions appear to overlap with those in Law No. 12,529/11, creating double liability for the same acts found to be harming competition. This is problematic and should be addressed so that a unified approach to sanctions is taken.

21. Article 10 of Bill 2768/2022 provides for several obligations in a non-exhaustive list on which the regulator could impose other measures. Should an exhaustive list of measures be created?

The App Association recommends that the evaluation of behaviors be approached on a case-by-case basis, and that measures imposed by regulators be based on evidence and economic analysis to ensure that antitrust enforcement is addressing actual harms to competition. The development of such a list to describe other measures that could be taken can be helpful in setting expectations of potential obligations that may be imposed, which will provide some certainty. Before creating such a list to support ex ante regulation of digital platforms, a full understanding of the sector is vital to inform these decisions by the regulator; unfortunately, we do not believe that such an understanding has been fully developed in Brazil yet, and we call

for further outreach to all communities impacted by this proposed regulation, including the small business innovator community the App Association represents.

22. Regarding pricing and assortment, in order to promote competition and encourage innovation, should a regulator protect potential competition even at the expense of efficiency?

Regarding pricing and assortment, protecting competition should be balanced with preserving efficiency for the benefit of consumers. As discussed in other answers above, Brazil's current framework and enforcement capacity provide an appropriate approach to achieving this balance.

23. Should the regulator intervene in large acquisitions in relevant market segments, if in place?

The success of a startup or small business can take a variety of forms and be achieved through different means, including, but not limited to, being acquired by a larger company with the resources and expertise to improve the product and/or expedite market entry or an initial public offering (IPO), all to the benefit of end consumers. Acquisition is often the best of these options for the business owner(s) and consumers, as IPOs are expensive and fraught with risk and therefore reduce the likelihood of consumer benefit. App Association members generally enter into business with the understanding that once we have realized our idea, our business may be acquired, allowing us to move on to develop new businesses. The Brazilian economy and consumers have benefited immensely from our freedom to combine the new products we create with the resources, technical expertise and business know-how of companies that later acquire our innovations. A merger that helps provide better products or services to consumers is often the desired and desirable outcome from a competition policy perspective.

Any changes to Brazilian competition policy for mergers and acquisitions should maintain deference to full economic analysis as the basis for any review or application of mergers, and reflect the above.

24. How should a regulatory authority determine the best course of action in circumstances of potential market dominance, where one player would prevent the entry of other competitors with the ability to deconcentrate it? Furthermore, is such a preventive action legitimate?

Brazil's current framework provides an adequate environment to combat abuse of market dominance. The risks associated with interoperability, data portability, data processing, use and storage, and concentration all fall within the scope of exclusionary conduct and foreclosure theories of harm and can be readily addressed using the current legal framework in Article 36, lines V, VIII IX, and X of Law No.

12,529/11. Current competition law and the application of international best practices in competition enforcement will best address the risks in digital markets arising from market concentration and abuse of economic power, while promoting competition and innovation.

Brazil's 2011 Competition Law was enacted after extensive legislative debate that led to an agreement to strengthen CADE's investigative powers due to the recognition that there was evidence that the harms identified could not be addressed through the existing regime. The existing legal framework has proven to be flexible and CADE has had a high degree of success in using it to protect competition. To achieve these objectives, CADE may initiate legal proceedings, accept judicial enforcement commitments, impose "accounting and functional separation" measures, issue infraction notices, issue public warning notices, adopt preliminary injunctions in urgent matters, resolve issues administratively, and carry out educational campaigns, and other compliance initiatives (some of which Bill 2,768/2022 would duplicatively assign to ANATEL).

IV. Conclusion

We strongly urge Brazil to holistically evaluate the mobile app ecosystem and capture its strongly competitive and innovative nature, described above, in its Summary Report. Brazil should also avoid policy changes that would improperly insert government mandates into this dynamic ecosystem that would unnecessarily disrupt innovation, growth, and job creation in Brazil.

The App Association appreciates the opportunity to provide its views and urges for careful consideration of our interests. We are committed to working with policymakers and regulators in Brazil and around the globe to bring the benefits of the dynamic app economy to all consumers and businesses through the development of balanced consumer protection and competition policies.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005
United States