ACT | The App Association Responses -- JFTC Request for Information regarding Smartphone Software Competition Promotion Act

Q1
ACT | The App Association
Brian Scarpelli

Q2
ACT | The App Association
1401 K St NW
Ste 501
Washington, DC 20005

Q3
Brian Scarpelli
Senior Global Policy Counsel
+1 517-507-1446
bscarpelli@actonline.org

Q4
Non-profit

Q6
ACT | The App Association represents the global small business software application and connected device developer community, located both within Japan and around the globe. These companies drive a global app economy worth more than 224.3 trillion JPY, and this economy continues to grow. 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.

Q9
The small business technology developers represented by the App Association distribute their software products and services through all major app stores. The app ecosystem has grown exponentially alongside the rise of the smartphone. 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.

Q20

App Association member companies operate in Japan and around the world and have experienced both the benefits of the current digital market ecosystem and the negative effects of competition laws inspired by the European Union's Digital Markets Act (DMA). The following sections will discuss these benefits and negative effects in greater detail.

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 centralised 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.

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

recognisable 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 utilise 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 jeopardise user privacy.

Platforms' Role in Addressing Intellectual Property Rights and 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.

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. So, if a platform has an offering that a consumer prefers over the offering of an independent developer, Japanese 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 App Association members support and benefit 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 Japanese policymakers 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.

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 centralisation 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 Japanese policymakers thus belie unsupported claims of monopolisation 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.

Platforms' Role in Supporting Data Privacy

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.

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 scrutinising 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 across Japanese 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 Japanese policymakers (and other policymakers and stakeholders) to consider how ineffective takedowns would be if a software platform must allow any app or app store on mobile devices. For example, if a fraudster specialising 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 Japanese policymakers 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 Japanese policymakers against pursuing policy changes that prevent software platforms from removing counterfeit apps and other stolen content.

The Negative Impact of Platform Mandates on Global Trade

Policymakers should recognise 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 digital innovators across Japanese. 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 Organisation 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 analyses 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."[1] However, a set of *quantitative* factors creates a presumption for the EC that an entity meets the qualitative test: "(1) it had annual EU turnover of at least EUR 7.5 billion in each of the last three financial years, or where its average market capitalisation 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."[2]

[1] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on con testable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/182 8, Art. 3(1), *available at* https://eur-lex.europa.eu/eli/reg/2022/1925/oj [Digital Markets Act (DMA)]

[2] Vanessa Anne-Marie Turner, "The EU Digital Markets Act – A New Dawn for Digital Markets?" AMER. BA

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.[3]

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.

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

---

R 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)).

[3] "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).

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 Japanese policy. 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 scrutinising 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."[4] 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.[5] In fact, one of TTC's subgroups—Working Group 5—specifically covers "data governance and technology platforms."[6] In the U.S.-EU joint statement establishing TTC, the signatories stated that they "recognise the global nature of online platform services and aim to cooperate on the enforcement of our respective policies for ensuring a safe, fair, and open online environment."[7] The

[4] 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.

[5] 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.

[6] 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.

[7] U.S.-EU Joint Stmt. of the Trade and Tech. Council, May 16, 2022, Paris-Saclay, France, para. 12, *avail*

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."[8] 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 illegalises 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

---

able at https://www.commerce.gov/sites/default/files/2022-05/US-EU-Joint-Statement-Trade-Technology-Council.pdf.

[8] DMA Art. 5(4).

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 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.[9] 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 . . .."[10] 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."[11] 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 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.[12] 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 Japanese 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

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

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

[11] *Id.*

[12] Letter from Morgan Reed, president, ACT | The App Association, to Senate Commerce, Transportation, a nd 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.

equally. Specifically, Article 3 of the General Agreement on Tariffs and Trade (GATT),[13] Article 17 of the General Agreement on Trade and Services (GATS),[14] and Article 3 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS)[15] 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."[16] 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

[13] 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.

[14] 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].

[15] 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.

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

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