20 July 2026

Association for Competitive Technology

Ministry of Industry and Trade
Attn: Legal Department (Vụ Pháp chế)
23 Ngô Quyền
Hà Nội, Viet Nam

RE: Comments of the Association for Competitive Technology (ACT) on the *Draft Law Amending and Supplementing a Number of Articles of the Law on Commerce, the Competition Law, the Law on Foreign Trade Management, and the Law on Protection of Consumer Rights*

The Association for Competitive Technology (ACT) has drafted this document to contribute comments to the Ministry of Industry and Trade on the Draft Law Amending the Law on Commerce, the Competition Law, the Law on Foreign Trade Management, and the Law on Protection of Consumer Rights.

ACT's comments are organized as follows:

I. Statement of Interest and Background

ACT represents thousands of small business application developers and connected device companies, located both within Viet Nam and around the globe. These companies drive a global app economy worth more than VND trillion globally[1] and are responsible for tens of thousands of jobs across Viet Nam.[2] ACT 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 the Ministry of Industry and Trade and other policymakers and enforcement authority.

Generally, ACT encourages competition policymakers and enforcers 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.

Below, ACT provides views on digital platforms and competition, as well as reactions and feedback on specific issues raised by policymakers and other governments. In addressing these proposals and questions, we explain how the extraordinary rise of the

[1] https://actonline.org/global-appcon22-competition-and-privacy/.
[2] https://www.progressivepolicy.org/wp-content/uploads/2015/09/2015.09-Mandel_Vietnam-and-the-App-Economy.pdf.

app economy happened in tandem with the development of the smartphone and software platforms. The presence of established, centralized platforms helps to drive the app ecosystem's dynamic growth and unrivalled success. Platforms serve as vital foundations and databases for the growing uses of apps across industries and enterprises. Software platforms do three things for app developers:

1. Reduce overhead costs across the board;
2. Provide instantaneous consumer trust mechanisms; and
3. Enable cost-effective access to a global market.

Today every successful platform for mobile, desktop, gaming, and even mainframe computing must provide those features, or they fail in the marketplace. Apps serve as the driving force in both the popularity and development of the smartphone and in turn, platforms offer lower barriers to entry for software developers into markets worldwide. The two entities' successes are symbiotic, and policymakers should take great care not to upset this healthy dynamic that has widely benefitted consumers and businesses.

We thus strongly urge the Ministry of Industry and Trade and the Government of Viet Nam to carefully consider its proposals for regulated cross-border services before moving forward, and to engage in further consultations with impacted communities like ours before finalizing these proposals. The Ministry of Industry and Trade and the Government of Viet Nam should also discourage policy changes that would improperly insert government mandates into this ecosystem that is continuing to produce innovation, growth, and job creation in Viet Nam.

ACT shares the Ministry of Industry and Trade's goals of advancing competition and innovation in the mobile application ecosystem. On behalf of the small business developer community, we offer general perspectives and recommendations below and respond to various questions posed by policymakers. ACT welcomes the opportunity to assist the Ministry of Industry and Trade in its efforts moving forward.

II. The Evolution of Digital Platforms in Positively Transforming Viet Nam's Economy

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-digital platform 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 significant upfront fees 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 digital platforms, 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.

When developers distribute an app through an internet browser, and not through a platform's digital platform, the developer still benefits from the trust consumers have that the web browser running on their phone is safe to use. In this way, developers can choose not to make use of a platform's developer services and instead use other service providers for functions like distribution and marketing while still reaching the same consumer base.

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

In just over a decade, the app ecosystem has grown exponentially alongside the rise of the smartphone. The global app economy is currently valued at more than VND 47,520 trillion and is responsible for approximately tens of thousands of jobs across Viet Nam, with digital platform revenue increases year-over-year. However, the reasons for 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 digital platforms. Trusted digital platforms 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 cloud computing must provide these features or risk failing in the marketplace. And increased competition amongst platforms has provided an unprecedented avenue for entrepreneurship. With an internet connection and coding skills, anyone can access millions of customers via software distribution platforms, thus, the mobile app economy provides an incredible means for empowerment to those in disadvantaged communities across Viet Nam.

b. Viet Nam's 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 digital 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 digital transformation market is estimated at approximately VND 26,400 trillion in 2024 and is projected to reach about VND 121,440 trillion by 2030, growing at a CAGR of 28.5% from 2025 to 2030.[3]
- Viet Nam's consumer spending on mobile apps more than tripled between 2018 and 2023, and the country's digital economy reached approximately VND 950 trillion in 2024, equivalent to about 8 percent of national GDP,[4] demonstrating rapidly expanding app monetization.[5]
- Viet Nam has approximately 530,000 software developers today.[6]
    - There are 2,330 Vietnamese mobile app developers active on Google Play alone having built over 10,300 apps, with Vietnamese apps averaging about 955,000 downloads each, indicating high app production and strong user engagement.[7]

c. <u>The Applicability of Competition Law to Software Platforms: Two-Sided Market Analysis</u>

i. *Software Platforms and Market Definitions*

A market definition should precede a determination of market power and abuse. While a 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 own quality and advertising, but also that of the vendors who operate over its network.[8]

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

[3] https://www.grandviewresearch.com/press-release/global-digital-transformation-market.
[4] Viet Nam's digital economy reached approximately US$36 billion (about 8 percent of GDP) in 2024. See Cimigo, Viet Nam Consumer Trends 2025, https://www.cimigo.com/en/trends/vietnam-consumer-trends-2025/.
[5] https://www.statista.com/topics/8264/mobile-apps-in-vietnam/.
[6] https://www.designveloper.com/blog/offshore-app-development-vietnam/.
[7] https://42matters.com/vietnam-app-market-statistics.
[8] Mark Rysman, *The Economics of Two-Sided Markets*, 23 J. Econ. Persp. 125, 136 (2009).

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.

Regulators should provide the flexibility for case-by-case market definitions, and a full understanding of a market is required in order 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.

Policymakers and regulators around the world have recognized a number of prominent digital platforms in existence today; however, the ACT 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 there is a persistent tendency to include only two platform providers, Apple and Google, in a list of "digital platforms," 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 digital platforms 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. With lower costs and barriers to entry, both fledgling and established app developers can find success. In addition to the Apple and Google digital platforms, ACT members 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 Twitter, for example, connect people with information and other people (and generate valuable data in the process), while the Google Play store and the 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 although developers can choose from multiple platforms, there is no such thing as a perfect platform. A small amount of app developers pay a fee to platforms for developer services (the majority of small business developers do not pay any fee), 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.

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

Once a market has been appropriately defined, an antitrust analysis would turn to a determination of market power and monopoly power. 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 is not enough for authorities to find competitive harm; regulators must demonstrate that the firm unfairly values its products resulting in harms 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 ACT urges for policymakers' analysis to be updated to clearly define and explore both market power and monopoly power.

Platforms play an important role in tech-driven markets as well as across a variety of economic sectors, bundling sets of services together for sellers and connecting those sellers with specific categories of buyers. Global 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 policymakers and others to avoid relying on unproven allegations made by outlier opportunist companies seeking to upend the harmonious app ecosystem for their own company's benefit, including in current ongoing litigation.

We strongly urge policymakers to review the ACT's amicus brief filed in the *Epic v. Apple* case, also appended to this comment.[9]

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). One of the most often-cited alleged competitive deficiencies on this side of the market is the practice of self-preferencing by platforms. Considering the unique nature of software distribution platforms, self-preferencing is in most cases pro-competitive because it is an example of vertical integration. We urge policymakers, as well as other stakeholders and enforcers, 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. Unfortunately, in other jurisdictions such as the European Union (EU), policymakers have proposed flipping the burden onto platforms to show that self-preferencing has no long-run exclusionary effects and either the absence of adverse effects on competition or an overriding efficiency rationale. The ACT discourages such an approach elsewhere because it would chill market activity that is likely to benefit consumers.

iv. *The Developer Services Side of the Market*

Aside from the antitrust attacks on platform activity in the software half of the two-sided market, critics also allege competition abuses in the developer services side of the market. Policymakers and enforcers should be especially wary of populist calls for the overapplication of antitrust law to digital platform activity in this side of the market. Some are seeking to leverage this trend to use the antitrust laws to punish their competitors and tend to overstate 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

[9] *See* appended amicus brief of ACT | The ACT in *Epic Games, Inc. v. Apple Inc.*, U.S. Court of Appeals for the Ninth Circuit, Case No. 4:20-cv-05640 (1 April 2022).

payment processing. However, payment processing is just one element of the array of services you get on a software platform, which include: immediate availability through hundreds of millions of people's devices; marketing through the digital platform; privacy features embedded in the platform; assistance with intellectual property protection; and security features built into the platform. 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 generally 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. Not only that, 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 off 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. Smaller developers have the advantage in either of these arrangements because they do not have the leverage to negotiate better terms on their own, as larger companies do. Overtures to have policymakers involve themselves in developer-platform relations, therefore, may benefit the largest software companies on the platforms while leaving small developers like ACT members worse off. If large software companies convince policymakers to require software platforms to give them a better one-off deal, ACT members and their clients and customers are forced to subsidize the resulting discount for these larger companies. Adding insult to injury, many ACT member companies compete with these larger firms, so the benefit handed to the larger companies could directly disadvantage ACT 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 ameliorate 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. 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 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.

ACT 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 digital platforms is an example of companies competing directly with a platform.

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 — after all, IPOs are expensive and fraught with risk. 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.

d. 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. There is a tendency to include only a few platforms in this category of competitors, but for developers the market is much wider and includes a wide range of platforms. For example, game developers can choose additional platforms just for games, and enterprise developers can look to hundreds of proprietary, custom platforms or could create their own.

i. *Platforms Role in Addressing Cybersecurity and Privacy*

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 cost 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 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.

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 across Viet Nam download their apps through digital platforms that come preinstalled on their devices' operating systems. Operating systems and digital platforms come bundled together so that the operating system that runs the device can enforce the digital platform'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 digital platform. 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 digital platform), 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 the Ministry of Industry and Trade (and other policymakers and stakeholders) to consider how ineffective takedowns would be if a software platform must allow any app or digital platform 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 digital platforms 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 the Ministry of Industry and Trade 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 the Ministry of Industry and Trade against pursuing policy changes that prevent software platforms from removing counterfeit apps and other stolen content.

ii. *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 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 that they 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 ACT's membership, 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 digital platforms available to our members, experiences and practices differ between platforms. The ACT 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 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.

ACT members collect data permitted by law/regulation and relevant platforms that is tailored to the functioning of the services they offer. ACT 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, such as Apple iOS, which the ACT supports and benefits from through greater trust by consumers. ACT 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 the Ministry of Industry and Trade to consult further with digital economy stakeholders who take measures to combat illegal contents and copyright 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.

Importantly, platforms already provide effective, user-controlled tools for data portability and migration. Consumers can transfer their purchases, settings, and content to a new device during setup, synchronize data across the devices tied to a single account, share apps and subscriptions with family members through family-sharing features, and download or export their data through built-in privacy and data-management tools. These mechanisms give users genuine control over their data while preserving the security and fraud protections that come from a trusted, account-based environment. Mandated data access of the kind imposed by DMA-style rules works very differently. Requirements that platforms provide continuous, real-time access to user and usage data to third parties, as under Articles 6(9) and 6(10) of the EU's DMA, widen the set of parties that can reach sensitive information and create new security and privacy risks, including where the recipients are entities controlled by foreign governments that do not protect human rights or democratic norms. ACT therefore urges the Ministry of Industry and Trade to build on the portability and migration tools that platforms already provide, and to avoid mandates that trade away users' security and privacy in exchange for compelled data sharing.

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 the Ministry of Industry and Trade 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 digital platform 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 ACT strongly cautions against new mechanisms that would unduly interject mandates into digital platform rankings that are evolving, exhibiting increased transparency, and which benefit small business developers.

e. 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 digital platforms 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 is in combatting the COVID-19 pandemic. 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, policymakers have raised the issue of featuring and ranking in digital platforms. ACT app developer members often are featured based on their designing 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, building an innovative app that stands out and letting the App Store editorial team know about it (through https://developer.apple.com/contact/app-store/promote/) is the best 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. The app title, number of downloads, good ratings, and price are the main factors that determine search rank. Generally, platform transparency, including with respect to ranking and featuring in digital platforms, 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. ACT 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 digital platforms 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.

f. The Negative Impact of Digital 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 in Viet Nam. 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."[10] 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 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

[10] 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)]

business users in the EU; and (3) the thresholds in (2) were met in each of the last three financial years."[11]

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. 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.[12]

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 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

[11] 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)).

[12] "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).

discipline. The EC, meanwhile, may exercise political power in substantial excess of any form of market power contemplated under EU competition law analyses or Vietnamese 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 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."[13] 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.[14] In fact, one of TTC's subgroups—Working Group 5—specifically covers "data governance and technology platforms."[15] 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."[16] 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

[13] 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.
[14] 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.
[15] 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.
[16] 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.

relevant core platform services of that gatekeeper."[17] 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 digital platforms 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 digital platforms 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 outlaws that structure, digital platforms 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 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.[18] 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 . . .."[19] 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

[17] DMA Art. 5(4).
[18] DMA, Art. 6(7).
[19] DMA, Art. 6(10).

business user . . . and where the end users opt-in to such sharing by giving their consent."[20] 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.[21] 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 Vietnamese 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),[22] Article 17 of the General Agreement on Trade and Services (GATS),[23] and Article 3 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS)[24] 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."[25] 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

---

[20] *Id*.
[21] Letter from Morgan Reed, president, ACT | The ACT, 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.
[22] 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.
[23] 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].
[24] 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.
[25] GATS Art. 17, para. 1.

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 government officials around the world evaluate the significant costs interventions like it would impose with open eyes. ACT's new report, *The Digital Markets Act at Two Years*,[26] details how a measure framed as disciplining a few large foreign platforms ultimately disadvantages the small developers who depend on open, trusted access to global markets, including Vietnamese developers seeking to scale abroad. As similar frameworks proliferate across jurisdictions, developers face a fragmented patchwork of national rules rather than a single global market, and a country that adopts discriminatory platform measures both burdens its own innovators and invites reciprocal treatment of them in other markets. Protecting the platform ecosystem that enables local innovation, rather than constraining it, is therefore the approach most consistent with Viet Nam's own digital-economy and trade interests.

[26] Appended to this comment letter as **Appendix A**.

III. Specific ACT Input on Various Proposals in the Draft Amendments to the Law on Commerce, Competition Law, Law on Foreign Trade Management, and Law on Protection of Consumer Rights

Key Recommendations

ACT's key recommendations are summarized in the table below and explained in detail in the discussion that follows:

Topic	ACT's key recommendation
Overall approach	Intervene only on demonstrated, systemic harm and rely on existing, technology-neutral competition law rather than ex ante, DMA-style platform mandates.
Article 8(2) enabler liability	Limit liability to parties with actual knowledge and a direct causal link to the harm, with a safe harbor for general-purpose service providers (investors, cloud, payments, ad networks).
Article 26 market power	Do not equate size or number of users with market power; issue guidance and de minimis safe harbors so the broad new digital factors do not sweep in ordinary platforms.
Article 27 prohibitions (new Clause 1a)	Predicate enforcement on case-specific harm rather than per se prohibitions, broaden the security exception, and require an impact assessment before any provision takes effect.
Self-preferencing	Avoid blanket prohibitions and recognize self-preferencing as often pro-competitive vertical integration.
Platform payment terms	Do not extend the Article 27 payment-method prohibition to ordinary platform payment and commission arrangements at large developers' urging.
Merger control	Keep review grounded in demonstrated harm and preserve acquisitions and investment as a growth and exit path for MSME developers; welcome the internal-restructuring exclusion.
Enforcement	Avoid duplicative competition and administrative proceedings and favor guidance over punitive action against MSME developers.
Trade consistency	Review the platform provisions against the CPTPP, the EVFTA, and WTO obligations before finalizing, to avoid non-tariff barriers and reciprocal measures against Vietnamese developers abroad.
Regulatory coherence	Map and eliminate duplication across the Competition Law, the Commerce Law, the Law on Protection of Consumer Rights, and the new Law on E-Commerce.
Learning from the DMA	Study the DMA's two-year record, which shows higher costs and weaker outcomes for small developers, before replicating it in any form.
MSME engagement	Establish a Vietnamese app developer consultative body with ACT.
E-commerce (retail marketplace)	Do not penalize successful platforms or presume bundled marketplace services illegal; predicate enforcement on demonstrated consumer harm.
Digital advertising services	Protect pro-competitive ad-tech integration, keep any rules narrowly tailored, and do not model rules on the EU's Digital Services Act (DSA).

Based on the above, ACT provides the following recommendations on specific proposals in the Draft Amendments to the Law on Commerce, Competition Law, Law on Foreign Trade Management, and Law on Protection of Consumer Rights proposed by the Ministry of Industry and Trade with respect to the digital platform obligations:

- **Build on the progress of digital platforms.** Overall, ACT urges the Ministry of Industry and Trade and policymakers to ensure that its policies reflect the exponential improvements that have been made to software distribution channels over time and the ways that digital platforms have empowered MSME community in Viet Nam to innovate and compete. We strongly encourage legislation to build on the positive evolution and benefits of digital platforms and how their rise has directly correlated to incredible MSME growth and job creation.
- **Recognize a highly competitive ecosystem.** ACT urges the Ministry of Industry and Trade and policymakers to recognize that the app ecosystem is highly competitive and consists of numerous players that continuously compete; and that the "challenges" raised in the draft legislation, to the extent they are challenges, are barriers that are mitigated by leading platforms that create a trusted environment for MSME developers to easily and securely bring their apps to consumers; other "challenges" are, in reality, assets and positive dynamics that empower and enable MSME app developers (e.g., customer loyalty).
- **Barriers to entry have never been lower.** The Ministry of Industry and Trade should also recognize that the barriers to entry for MSME app developers on and between digital platforms have never been lower. The Ministry of Industry and Trade's emphasis on platforms' "intermediary" role appears to reflect broader concerns around gatekeeper "bottleneck". However, that concern overlooks the need for platforms to balance openness to third-party competitors against the control needed to preserve security, quality, and commercial reach. The draft's new Clause 1a of Article 27 seeks to prevent practices that limit business users' access to alternative platforms. Yet ACT members and many MSMEs often operate across numerous cloud and ISP providers, while many developers operate for both iOS and Android. ACT members appreciate the tools that facilitate data portability and switching providers, as they signal active competition in the hosting market. Interoperability mandates that push operating platforms toward a single, homogenized model, risk eliminating the diverse approaches to digital curation.
- **Intervene only on demonstrated, systemic harm.** We urge the Ministry of Industry and Trade to base its proposals on the principle that targeted government interventions into competitive digital platform markets should be based on demonstrated systemic harms. This principle has helped to unleash innovation and has empowered countless MSMEs in and outside of Viet Nam. A light-touch approach is critical for enabling Viet Nam's MSME developer community moving forward. The burden of new ex ante rules falls disproportionately on small developers. Unlike large firms, MSME developers do not have dedicated legal or

compliance teams, so the same obligations that a large company absorbs as a line item can consume a meaningful share of a small developer's budget and engineering time. Experience under DMA-style regimes shows the concrete forms this burden takes, including managing distribution and divergent terms across multiple app stores, releasing and testing multiple versions of an app to satisfy different rule sets, monitoring intellectual-property infringement across fragmented channels, and absorbing legal uncertainty as enforcement positions shift, in some cases leading to apps being removed for technical non-compliance such as out-of-date contact details. ACT urges the Ministry of Industry and Trade to weigh these compliance costs and the associated legal uncertainty, which are easy to overlook because they do not appear in any single platform's fee schedule, when assessing any new platform obligation, and to build in proportionate treatment and clear safe harbors for smaller developers.

- **Avoid blanket self-preferencing prohibitions.** We reiterate that 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 policymakers 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.
- **Study the DMA before replicating it.** We urge the Ministry of Industry and Trade to exercise caution in developing digital platform sub-sector guidelines. We strongly encourage Viet Nam to monitor the impact of the DMA before replicating it in any form, as, to date, the impacts have been objectively negative for MSME developers. To the extent Viet Nam does take action, existing competition law should be relied upon, under which traditional and technology-neutral competition/consumer harm analyses should be employed, with guidance (and enforcement) being based on demonstrated and systemic harms. ACT's status report, *The Digital Markets Act at Two Years*,[27] documents how, two years after the DMA took effect, there is no evidence that it has delivered measurable benefits to small developers. Instead, enforcement has advanced the interests of a handful of large firms at the expense of the broader developer ecosystem, while

[27] Appended to this comment letter as **Appendix A**.

weakening the curated-distribution security and trust mechanisms that disproportionately benefit small developers without established brands. The compliance burden falls hardest on the smallest firms. Based on a 2025 ACT survey of more than 1,000 small technology companies, startups operating under the EU regulatory environment, of which the DMA is a major component, lose on average between EUR 94,000 and EUR 160,000 per year relative to their counterparts in the United States, and six in ten report delayed access to frontier technologies. DMA-related obligations have also contributed to the delayed or withheld launch of major artificial intelligence products in the EU, including Apple Intelligence, Google Gemini, and Meta's Llama, leaving EU developers and consumers a step behind their peers elsewhere. Notably, even the European Commission's own April 2026 review, which declared the DMA "fit for purpose," did not engage with these effects on smaller firms, focusing on competition at the top of the market rather than the broader ecosystem in which MSME developers actually operate.

- **Ensure consistency with Viet Nam's trade commitments.** ACT urges the Ministry of Industry and Trade to ensure that any platform-specific obligations are consistent with Viet Nam's binding international trade commitments. As ACT explains in Section II.f above, DMA-style mandates raise serious non-discrimination concerns under the World Trade Organization agreements, including the national treatment obligation in Article XVII of the General Agreement on Trade in Services. Viet Nam is also a party to the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the EU-Viet Nam Free Trade Agreement (EVFTA), each of which contains electronic commerce and digital trade disciplines that protect cross-border data flows and constrain forced technology transfer and forced disclosure of source code. Provisions that condition platform access on data-sharing, interoperability, or the localized handling of software risk creating non-tariff barriers and inviting reciprocal measures against the Vietnamese developers who seek to reach foreign markets. ACT recommends that the Ministry of Industry and Trade subject the platform provisions to a formal trade-consistency review against the CPTPP, the EVFTA, and Viet Nam's WTO obligations before finalizing them. More broadly, DMA-style platform mandates are increasingly being adopted, in varying forms, across multiple jurisdictions, replacing a single global market with a patchwork of divergent national rules. As ACT's appended status report on the DMA and its impacts documents, that fragmentation raises compliance costs most sharply for the smallest developers, and it would fall directly on Vietnamese MSMEs seeking to reach foreign markets, who must navigate conflicting requirements without dedicated legal or compliance teams. By keeping its competition framework grounded in existing, technology-neutral, and trade-consistent rules, Viet Nam can both protect the trusted platform ecosystem that enables local innovation and avoid disadvantaging its own developers abroad through measures that invite reciprocal treatment.

- **Avoid duplication across overlapping laws.** ACT urges the Ministry of Industry and Trade to ensure regulatory coherence across the overlapping instruments that now govern digital platforms in Viet Nam. The proposed amendments to the Competition Law, the Commerce Law, and the Law on Protection of Consumer Rights intersect with the new Law on E-Commerce, which takes effect on 1 July 2026, and with Viet Nam's personal data protection regime. Overlapping or inconsistent obligations across these instruments would multiply compliance costs that fall hardest on MSME developers and would create a risk of conflicting enforcement. ACT recommends that the Ministry of Industry and Trade map the platform-related obligations across these laws, eliminate duplication, and designate a single lead framework for each category of conduct so that MSME developers face one clear and predictable set of rules.
- **Narrow the Article 8(2) "facilitating" standard.** ACT urges the Ministry of Industry and Trade to reconsider the proposed amendment to Article 8(2) of the Competition Law, which would prohibit organizations and individuals from "facilitating" prohibited competition restrictions or unfair competition acts. As drafted, the provision reaches those who provide information to, campaign or solicit for, coerce, organize, or assist businesses in such conduct, with "assisting" being the broadest of these terms. ACT recognizes the legitimate policy goal of closing legal gaps around third-party enablers of anticompetitive conduct. However, the draft's formulation uses the broad term "facilitating" without defining its scope or requiring proof of intent or knowledge, which risks sweeping in ordinary commercial relationships and platform services into liability exposure. Venture investors, cloud infrastructure providers, payment processors, and advertising networks that provide general-purpose services to platform operators could plausibly be characterized as "facilitators" under an overly broad reading. ACT recommends that any "facilitating" liability standard: (1) require that the facilitator had actual knowledge of the underlying violation; (2) require a direct and material causal link between the facilitation and the harm; and (3) be subject to a safe harbor for general-purpose service providers who have in place reasonable compliance programs. These guardrails would ensure that the provision targets genuine bad actors rather than chilling the commercial ecosystems that support MSME developers.
- **Add guardrails to the Article 26 market-power factors.** ACT acknowledges that the draft's revised Article 26(1) expands the significant market power criteria by adding factors specific to digital markets including data accumulation, network effects, switching barriers, ecosystem integration, and algorithmic control. This reflects a genuine effort to adapt competition law to digital market realities. ACT has long supported the view that traditional market share analysis is an insufficient proxy for digital market power. However, ACT cautions that the resulting expanded and open-ended list of factors risks producing unpredictable outcomes and generating compliance uncertainty for MSME developers who rely on platform services. Specifically, factors such as "the degree and scope of direct

and indirect network effects" and "the ability to use algorithms, artificial intelligence or other digital technologies to coordinate transactions, prices or user behavior" are so broad that they could apply to virtually any digital platform of any scale. ACT recommends that the Ministry of Industry and Trade issue implementing guidelines under Article 26 that: (1) clarify which combinations of factors are necessary (not merely sufficient) to a finding of significant market power; (2) establish safe harbor thresholds below which enforcement action will not be taken; and (3) provide clear guidance distinguishing platforms with genuine market power from those with network effects that reflect healthy, consumer-driven adoption. Without such guidance, the expanded criteria risk deterring pro-competitive platform investment and disproportionately burdening smaller platforms that serve MSME developers.

- **Do not equate size and user numbers with market power.** ACT urges the Ministry of Industry and Trade to define "intermediary digital platform" and the threshold for "significant market power" with precision, and to reconsider any criterion that keys market power to size and number of users alone. As reported publicly, the draft adds a new clause to Article 26 under which the significant market power of an intermediary digital platform would be determined based on its size and number of users. As ACT explains at length in Section II.c above, scale is a poor proxy for power, because a large or growing user base often reflects healthy, consumer-driven adoption rather than any ability to raise prices or exclude rivals. A criterion based on size and user counts, much like the quantitative presumptions in the EU's DMA, risks capturing successful and pro-competitive platforms that serve MSME developers while telling enforcers little about actual competitive harm. ACT recommends that any market-power determination require evidence of durable power and demonstrated harm, and that the Ministry of Industry and Trade establish clear de minimis thresholds that exclude smaller platforms and new entrants from these obligations.
- **Revise the Article 27 platform prohibitions (new Clause 1a).** ACT has specific concerns about the newly added platform-specific prohibitions in Article 27. The draft's newly added Clause 1a of Article 27 introduces a wide range of obligations that mirror, in important respects, Articles 5 and 6 of the EU's DMA framework that ACT has consistently cautioned against replicating (see Section II.f above). In particular, it prohibits self-preferencing through display rankings, algorithms, or transaction terms. As ACT has explained at length, self-preferencing is frequently pro-competitive, representing a form of vertical integration that benefits consumers through lower prices, better quality, and greater efficiency. Blanket prohibition without requiring demonstration of harm is disproportionate and chills legitimate platform investment. It also prohibits bundling or tying of services as a condition of platform access. Such integration is often what makes platforms valuable to MSME developers — reducing their overhead, providing built-in security and trust, and enabling cost-effective access to consumers. It prohibits preventing users from removing pre-installed applications or switching to

competing services "except where necessary to ensure network information security or essential operation." This exception is narrower than the security measures platforms actually need to protect consumers and MSME developers from malicious applications. As ACT's extensive discussion of sideloading above makes clear, platform control over what software is installed is a cornerstone of the security model that protects consumers and small developers alike. It requires platforms to allow business users to access data arising from their activities on the platform. This is analogous to DMA Article 6(10) and risks inadvertently mandating tech transfer to bad actors, including entities controlled by foreign governments that do not protect human rights or democratic norms. ACT urges the Ministry of Industry and Trade to revise these provisions so that: (1) enforcement is predicated on demonstrated, case-specific harm rather than per se prohibitions; (2) the security exception for pre-installed applications is broadened to encompass the full range of cybersecurity threats platforms face, not just threats to hardware or operating system integrity; and (3) implementation is subject to a comprehensive impact assessment before any provision takes effect.

- **Do not broaden platform payment-term rules at large developers' urging.** We urge caution with respect to the Ministry of Industry and Trade's newly added Article 27 prohibition on a dominant digital platform imposing unreasonable transaction conditions relating to payment method, which should not be read to reach ordinary platform payment and commission arrangements. As we discuss above, the Ministry of Industry and Trade should be wary of opportunistic behavior by well-resourced large developers representing under 5 percent of the app ecosystem 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. The Ministry of Industry and Trade should acknowledge that the significant majority of developers pay no commission to software distribution platforms at all, and that competitive pressures have resulted in a reduction of fees for those that do pay them over time. Overtures to have policymakers involve themselves in developer-platform relations, therefore, benefit the largest software companies on the platforms while leaving the small developers the ACT represents worse off. If large software companies convince policymakers to require software platforms to give them a better one-off deal, ACT members and their clients and customers are forced to subsidise the resulting discount for these larger companies. Adding insult to injury, many ACT member companies compete with these larger firms, so the benefit handed to the larger companies, in raising market barriers, would directly disadvantage ACT members.

- **Keep merger control grounded in demonstrated harm and preserve acquisitions for MSME developers.** ACT urges the Ministry of Industry and Trade to ensure that the draft's revisions to the Competition Law's economic concentration provisions support the acquisitions and investment on which MSME developers depend. The draft would empower the Government to define the forms of economic concentration subject to control and would add a mechanism to exclude or simplify notification for internal restructuring transactions that do not change market structure. ACT welcomes the exclusion for internal restructuring, which reduces unnecessary compliance burdens on smaller firms. ACT cautions, however, that an open-ended delegation to define new forms of economic concentration risks expanding merger review unpredictably. For many MSME developers and startups, a merger or acquisition is a key pathway to secure growth capital, scale operations, and deliver returns to early-stage investors, so an overbroad or uncertain merger-control regime would chill the pro-competitive acquisitions and investment that drive the developer ecosystem. ACT recommends that any expansion of economic concentration control be grounded in demonstrated harm, rely on clear and predictable thresholds and a data-driven, fact-based approach to market definition, and preserve workable treatment for internal restructuring and for ordinary acquisitions of and investments in small developers.
- **Avoid duplicative competition enforcement against MSME developers.** ACT supports the draft's stated aim of ensuring that enterprises are not subject to duplicate handling across competition proceedings and administrative sanctions, together with its move toward principle-based handling of competition-law violations. Predictable and non-duplicative enforcement matters most for MSME developers, who lack the resources to absorb parallel or overlapping proceedings for the same conduct. ACT recommends that this protection against duplicative handling be set out clearly in the law itself rather than left to implementing regulation, and that enforcement against MSME developers favor guidance and corrective measures over punitive action where conduct is not shown to cause systemic harm.
- **Establish a Vietnamese app developer consultative body with ACT.** We urge the Ministry of Industry and Trade to work with ACT to establish a Vietnamese developer consultative body that will act as an alternative channel for engagement between developers and major app platforms, consolidate and elevate recurring concerns collectively to those platforms, surface priority issues to the relevant ministry for follow-up, and offer localised advice on platform rules and appeal processes. ACT provides these services for its members in Viet Nam and around the globe today. We welcome the opportunity to collaborate with Vietnamese government to ensure that MSMEs have a voice in government efforts to address operational challenges in app development and management.

We offer the following input on the Ministry of Industry and Trade's proposals with respect to e-commerce (retail marketplace):

- **Do not penalize successful e-commerce platforms.** We urge the Ministry of Industry and Trade and the Vietnamese government to ensure they do not punish leading e-commerce platforms for being successful, and instead focus on predicating enforcement against e-commerce platforms on demonstrated harms to consumers, while recognizing that most small companies have benefited from access to bundled logistics and distribution network.
- **Do not presume bundled marketplace services are illegal.** The ACT contends that treating bundled marketplace services as presumptively illegal would undermine a vital distribution channel for small companies, removing streamlined options that help minimise time, cost, and uncertainty in reaching consumers. The innovations in e-commerce that are driven by market forces already benefit competition and small business, allowing even the smallest sellers nationwide reach and reliable shipping. Putting new legal burdens in place for leading e-commerce platforms would chill innovation and make it harder for startups and independent app developers to compete.
- **Avoid blanket self-preferencing rules here too.** We reiterate that blanket characterizations of self-preferencing should be avoided, as discussed above in connection with the Article 27 self-preferencing prohibition.

We offer the following input on the Ministry of Industry and Trade's proposals with respect to digital advertising services:

- **Protect pro-competitive ad-tech integration.** ACT strongly encourages the Ministry of Industry and Trade to appropriately capture how advertising technology integration helps small tech companies manage advertising, find customers, and benefit economically from scale, and that any steps taken by Vietnamese government should not restrict these pro-competitive dynamics.
- **Keep advertising rules narrowly tailored.** ACT emphasizes that any intervention by Viet Nam into digital advertising services markets should be carefully calibrated so as not to make it cost-prohibitive for small businesses to comply, and any enforcement/action taken by the Ministry of Industry and Trade or the Vietnamese government should be narrowly tailored to address demonstrated harms.
- **Do not model rules on the EU's DSA.** ACT cautions the Ministry of Industry and Trade against using the EU's Digital Services Act (DSA) as a model. The DSA's requirements (such as takedown procedures and public disclosure of trader information) create excessive burdens for SMEs with limited resources, risk overblocking of content and limiting freedom of expression for consumers. Further, the DSA's lack of proportionality and lack of appropriate MSME exemptions exposes smaller players to substantial administrative costs. The

Ministry of Industry and Trade should carefully monitor the DSA's implementation before following the EU's lead.

IV. Conclusion

ACT appreciates the opportunity to provide its views to the Ministry of Industry and Trade and urges for careful consideration of our interests. We are committed to working with the Ministry of Industry and Trade, as well as other policymakers and regulators in Viet Nam 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

Jong Chung
Policy Associate

Association For Competitive Technology (ACT)

APPENDIX A

Association for Competitive Technology

ACT Status Report: The Digital Markets Act at Two Years

About the Association for Competitive Technology (ACT)

The Association for Competitive Technology (ACT) is a global trade association for small and medium-sized technology companies. Our members are small business innovators and startups in the software development and high-tech space around the world. As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping consumers lead healthier lives. Today, the digital economy is worth more than €5.4 trillion annually.[1] We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology.

Key Findings

- After two years of enforcement, there is no evidence that the DMA has delivered measurable benefits to small and medium-sized enterprises (SMEs). Instead, EU enforcement has consistently advanced the interests of a handful of large third-parties at the expense of the broader app developer ecosystem.
- DMA compliance concerns have caused or contributed to documented delays in the EU launch of major AI products and features, including Apple Intelligence, depriving EU SMEs of the same access to frontier technologies enjoyed by their U.S. and UK counterparts.
- ACT's 2025 survey of more than 1,000 small technology companies found that EU startups lose between €94,000 and €160,000 per year, on average, compared to their U.S. counterparts because of the EU regulatory environment of which the DMA is a major component.
- By imposing uniform, top-down obligations and fee structures on the largest distribution platforms, the DMA undermines the inter-platform competition for SME business on revenue share, developer tools, integrated payments, and SME-facing services that historically gave small developers meaningful negotiating leverage. Handcuffing how the largest platforms compete with one another has weakened the position of the SMEs that depend on those platforms.

---

[1] ACT | The App Association, *App Economy Fast Facts*, https://actonline.org/wp-content/uploads/About-the-App-Economy-2023_162023.pdf.

- The DMA's mandates effectively weaken curated app store distribution, undermining the security and trust mechanisms that disproportionately benefit small developers without established brands.
- The 2024 Draghi Report on European competitiveness warned that excessive EU regulatory and administrative burdens hinder the competitiveness of European companies.

What is the DMA?

The Digital Markets Act (DMA) is the European Union's major legislative effort to increase competition in the online platforms market. DMA focuses on limiting the market power of large online platforms, including online search engines, app stores, and messaging services. The law grants the European Commission (EC) the power to designate certain of these platforms as 'gatekeepers' if they meet certain thresholds. Today, the companies the EC has designated as gatekeepers include Alphabet, Amazon, Apple, Booking, ByteDance, Meta, and Microsoft.[2]

To be considered a gatekeeper, a platform must:

- Have a turnover of at least 7.5 billion euro in the European Economic Area for at least three years or a market capitalization of at least 75 billion euro;
- Have at least 45 million monthly active users and at least 10,000 yearly active business users in the EU;
- Have 'an entrenched durable position', which is a qualitative assessment made in part by whether the user numbers have been maintained for three consecutive years.

Once designated a gatekeeper, a company must comply with special obligations established by DMA. These include allowing third-parties to interoperate with their services, allow access to business data generated on the platform, provide tools and information for advertisers and publishers to independently verify the ad business activity they conduct on the platform, and allow business users to contract with their customers outside the platform. Gatekeepers are prohibited under DMA from self-preferencing their own products in rankings, preventing consumers from signing up for businesses outside their platform, preventing the un-installation of pre-installed apps, or tracking users outside of the gatekeeper's platform for targeted advertising purposes without consent. Gatekeepers who do not comply with these obligations and prohibitions could face fines of

[2] https://digital-markets-act.ec.europa.eu/gatekeepers_en

up to 10% of the company's total worldwide annual turnover, or up to 20% for repeated violations, as well as other remedies such as imposed behavioural or structural changes.

DMA is a prime example of an *ex ante* regulation. As opposed to *ex post* regulations that apply to behaviour after the fact, *ex ante* regulations restrict behaviour before actions are taken. Where antitrust laws in other jurisdictions such as the United States provide enforcement powers against actions that have resulted in demonstrable harm to competition, DMA restricts a wide swath of behaviours on the part of gatekeepers before any particular harm has been shown to have occurred. As a result, many behaviours that would not have resulted in harm to competition and may have in fact benefited competition are barred, reducing opportunities for innovation by companies operating within the EU.

This structural feature is the root cause of many of the DMA's most damaging effects on small business innovators. Because the law presumes harm rather than proving it, enforcement priorities are set by political and large-rival lobbying pressure rather than evidence of actual competitive injury, and obligations expand into novel markets, including cloud services that were not contemplated during the formation of the DMA as well as artificial intelligence services that did not exist when the law was drafted, without the procedural discipline that ordinary antitrust review would provide.

Evaluating the DMA's second year

Since DMA's obligations became effective two years ago in May 2024, European regulators have been active in pursuing compliance with the law's provisions. These actions have in some cases led gatekeepers to make significant changes to their business models.

- In April 2025, the European Commission fined Apple €500 million for DMA violations,[3] taking issue with Apple's terms regarding whether and how app developers can direct their users to alternative offers outside of the App Store and allow them to make purchases, a practice known as steering. Given 60 days to comply or face additional fines, Apple instituted new policies that would allow for apps to steer users outside of the App Store while instituting new rules for such purchases as well as a "Core Technology Commission" of 5%.[4] Proceedings to determine the adequacy of these changes to comply with DMA are ongoing, but the steering enforcement action illustrates the DMA's pattern of advancing the interests of large third-party developers seeking to disintermediate gatekeeper commerce systems, while imposing new complexity, new fees, and ongoing regulatory uncertainty on the small developers who depend on those systems and who lack

[3] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085
[4] https://www.cnbc.com/2025/06/26/apple-eu-500-million-euro-app-store.html

the resources to negotiate bespoke distribution arrangements outside trusted digital platform.

- Also in April 2025, The European Commission fined Meta for €200 million for violating the DMA with its policies replacing a previously disallowed 'consent or pay' model, under which Meta provided EU users of Facebook and Instagram with an option to either consent to personal data combination for targeted advertising or paying a monthly subscription.[5] The Commission found that this structure was not allowed under DMA, and Meta eventually replaced it with a new model that used less personal data along with targeted advertising. The €200 million fine was for non-compliance during the eight-month period between the 'consent or pay' determination and the model that replaced it. Meta has challenged this fine before the EU's General Court.
- In December 2025, the European Commission opened an investigation into Meta's policy instituted several months earlier prohibiting AI providers from using a tool within WhatsApp allowing businesses to communicate with customers, which in practice prevents third-party AI assistants from integrating into WhatsApp.[6] Meta has offered compromise proposals while arguing that the Commission is incorrectly assuming the WhatsApp Business API is an important channel for AI chatbots. The Commission's decision to extend DMA obligations to artificial intelligence services that did not exist when the law was drafted, and that were never the subject of any market definition or evidentiary record before designation, exemplifies the mission creep that the DMA's open-ended *ex ante* structure invites.[7] Each such extension creates fresh compliance uncertainty for the entire ecosystem of small developers who build on top of these services.
- In January 2026, the European Commission opened DMA proceedings against Google in two areas related to platform interoperability.[8] The first concerns DMA's requirement that Google must provide third-party developers with hardware and software features controlled by Android, in particular Gemini AI features. The second concerns DMA's requirement that third-party search engine providers have access to Google Search ranking, query, click, and view data. In April 2026, the Commission sent proposed measures for Google to resolve the Search data issue, detailing the scope of the data Google must share, the means of sharing it, who is eligible to receive it, anonymization requirements, and other matters. Such forced disclosures undermine the long-term investment incentives that produced the data

[5] https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1085
[6] https://digital-strategy.ec.europa.eu/en/news/commission-opens-antitrust-investigation-metas-new-policy-regarding-ai-providers-access-whatsapp
[7] https://www.cnbc.com/2026/02/09/eu-interim-measures-meta-whatsapp-ai-policy-antritrust.html
[8] https://digital-markets-act.ec.europa.eu/commission-opens-proceedings-assist-google-complying-interoperability-and-online-search-data-sharing-2026-01-27_en

in the first place, and risk privacy and security consequences for the EU users whose queries generated it.[9]

Overall, the European Commission's actions in the second year of the DMA continued trends of the first year: focusing on the concerns of large third-parties while creating shifting policies and uncertainty for the small companies that rely on the platforms themselves.

The state of small business innovation in the EU

Statistics show that the regulatory environment in the EU has already led to significant disparities in the success and longevity of EU startups compared to those in other competitive markets. For instance, the United States boasts about three times as many startups than the EU.[10] Additionally, in 2022, venture capital investment in Europe was €29.6billion, significantly lower than the €108.8 billion invested in the United States and the €53.9 billion invested in Asia.[11] This investment gap reflects the impact of the current regulatory climate on EU tech startups' ability to scale, innovate, and—ultimately—exist. The stringent requirements of the DMA risk widening this disparity even further, making it more difficult for EU startups to compete globally.

In September 2024, former European Central Bank President Mario Draghi's landmark report on *The Future of European Competitiveness*, which was commissioned by the European Commission itself, warned in stark terms that EU regulatory and administrative burden constrains the growth and competitiveness of European companies, particularly in digital and technology sectors.[12] The Draghi Report calls for simplification of the EU regulatory rulebook, reduction of overlapping reporting requirements, and a shift toward innovation-friendly regulation. The Draghi Report warned that a sweeping *ex ante* framework, layered on top of other EU and Member State regulatory regimes, produces precisely the 'morass of EU legislation that has constrained innovation, especially in the tech sector' that Draghi identifies as a driver of innovation flight from Europe.

[9] https://digital-markets-act.ec.europa.eu/commission-proposes-measures-google-sharing-search-engine-data-third-parties-under-digital-markets-2026-04-16_en

[10] https://mikelmangold.com/usa-vs-europe/; Mario Draghi, *The Future of European Competitiveness*, European Commission, September 2024, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en (citing structural underperformance of the EU startup ecosystem and limited startup creation and scale-up relative to the United States).

[11] https://dealroom.co/guides/global

[12] Mario Draghi, *The Future of European Competitiveness*, European Commission (September 2024), https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

In October 2025, ACT released a report titled, 'The Hidden Cost of AI Regulations for EU and UK Startups and SMEs',[13] which provides a useful snapshot of the state of small business innovators in the EU compared to those in other jurisdictions. Based on surveys of more than 1,000 small technology companies across the EU, United Kingdom, and United States asking about their adoption of AI as users and developers, the report describes a widening transatlantic gap in innovation and opportunity. The EU policy environment, of which DMA is a major component, creates delays in the availability of new technology, which shrinks savings and increases costs; only half of EU startups actively use AI compared to two-thirds in the U.S., six in 10 EU startups face delayed access to frontier models, and as a result EU startups lose on average between €94,000 and €160,000 per year compared to their U.S. counterparts.

Has the DMA helped small businesses? The evidence says no

The DMA is now imposing restrictions on digital platform markets, mandating the development of, and accommodation for, third-party app stores. After two years, has this endeavour proven to be a benefit to small businesses? Based on objective data and the SME digital economy experience writ large, the answer is no.

For years before the passage of DMA, offering an app was simple for SMEs. They could build a new app, submit it to Apple App Store and/or Google Play store, and instantly reach a global market with trusted users. SMEs operated in a market in which major distribution platforms competed against one another for developer participation in areas including on revenue share, developer tool quality, integrated payments, fraud and piracy enforcement, intellectual property protection, marketing support, and discoverability. That inter-platform competition gave SMEs meaningful negotiating leverage because a developer dissatisfied with one platform's terms had a realistic alternative, and platforms had an ongoing incentive to improve the systems on which small developers depend. The DMA's prescriptive, uniform obligations and mandatory fee structures collapse much of that competitive dynamic into a single regulator-defined template, replacing platform-versus-platform competition for SME business with a regulator-versus-platform compliance dialogue from which SMEs are largely absent.

Under the DMA's new rules, many challenges to the previous status quo have arisen:

- **Market Uncertainty:** Because DMA implementation is ongoing and constantly evolving, SMEs find it harder to plan marketing and outreach when market conditions are unstable.

[13] https://actonline.org/the-hidden-cost-of-ai-regulations-a-survey-of-eu-uk-and-u-s-companies/

- **Weak Market Controls:** Some new app stores attempting to capitalise on opportunities created by DMA may lack the important security systems the existing major app stores have developed to stop copyright infringement, malware, or deceptive design. SMEs that find their apps pirated, for example, may have little or no recourse at the app store level. In extreme cases, this can be an existential threat for startups.
- **Lower User Trust:** A significant share of SME revenue depends on consumer willingness to download apps from unknown developers, which in turn depends on the screening, content, and quality controls users associate with the storefront on which an app appears. By mandating that platforms must allow sideloading, third-party app stores, and generally reduce curation in various ways, DMA leads to the predictable result that more apps with harmful features will be permitted onto app store shelves than before. An increase in the share of app store apps containing malware and dark patterns will lead users to hesitate to download apps from companies they do not know. This disproportionately harms SMEs and startups without established brands, making it more difficult for them to reach potential customers. As a prime example, AltStore PAL, one of the earliest alternative iOS marketplaces in the EU established in response to the DMA, in February 2025 launched 'Hot Tub', a pornography app made possible specifically because the DMA-mandated alternative distribution channels are not required to apply the content standards that ordinary app store distribution applies.[14] Such developments have directly eroded trust in alternative distribution as a credible channel for legitimate SME apps and reinforce user wariness of *any* digital platform.
- **Weaker Intellectual Property Enforcement:** Digital platforms historically give SMEs a single, reliable venue for policing piracy, cloned apps, and counterfeit listings, and compete on the strength of those protections. As distribution splinters across new marketplaces with divergent and often weaker enforcement practices, small developers without dedicated legal teams must monitor and pursue infringement across many channels at once, frequently with little or no recourse at the platform level. For startups whose core asset is their own intellectual property, the resulting erosion of enforcement can be an existential threat.
- **Complex Distribution:** More app stores, especially new ones, add extra work in submitting and managing multiple channels. Different app stores also have different terms of service and different practices regarding user data privacy, advertising, and intellectual property protection. All these differences make compliance much more

[14] Sarah Perez, "Hot Tub, the first native iPhone porn app, arrives in EU," TechCrunch (Feb. 3, 2025), https://techcrunch.com/2025/02/03/hot-tub-the-first-native-iphone-porn-app-arrives-in-eu/; see also Chance Miller, "Apple responds after being forced to approve porn app on EU iPhones due to DMA," 9to5Mac (Feb. 5, 2025), https://9to5mac.com/2025/02/05/apple-forced-to-approve-porn-app-on-eu-iphones-due-to-dma/.

complex, and potentially out of reach for a small startup without a dedicated legal or compliance team.

- **Launch Timing Issues:** Each store has its own approval process. SMEs must release apps at the same time across channels to avoid confusing users and losing revenue. This can quickly become a logistical nightmare.
- **Multiple Global Jurisdictions:** As more jurisdictions pursue regulatory frameworks similar to DMA, the cost of compliance for SMEs goes up. Instead of one global market, SMEs increasingly face different rules in each region, which requires more specialised compliance expertise.
- **Fragmented Marketing:** Global marketing now needs different marketing messages, documentation, and development for each market.
- **Increased Development Cost**: Different rules and different e-commerce systems often mean that multiple versions of the app need to be released with different coding paths. This not only takes significant developer resources, but it also increases testing complexity and the chances of errors.
- **Customer Support Challenges:** Recommendations vary by region and store. For example, a user might be in one country but use an account from another. These subtle but important differences affect how users need to be helped.
- **Increased Compliance Burden:** Even for regulations that only target gatekeepers, SMEs now bear more of the regulatory compliance risk. For example, many have had their apps removed in the EU for not updating required contact details on time.
- **Slow Arrival of New Features and Technologies:** The delay of AI availability such as Apple Intelligence, Google Gemini, and Meta's Llama in the EU market results from concerns around obligations under DMA to share data with third-parties. This dynamic could become a feature of technology development in years to come, as platforms hold back new features from jurisdictions under DMA-like legal regimes, preventing SMEs from taking advantage of new capabilities. In June 2024, Apple announced that it would not release Apple Intelligence, iPhone Mirroring, or SharePlay screen-sharing enhancements to EU users at the iOS 18 launch, citing concerns that DMA interoperability obligations risking user privacy and data security.[15] In July 2024, Meta announced that it would not release its multimodal Llama AI model in the EU due to the unpredictable nature of the European regulatory environment, expressly contrasting the EU with the United Kingdom.[16]

[15] Apple statement reported in Sam Shead, "Apple Intelligence won't launch in EU in 2024 due to antitrust regulation, company says," CNBC (June 21, 2024), https://www.cnbc.com/2024/06/21/apple-ai-europe-dma-macos.html.
[16] Ina Fried, "Scoop: Meta won't offer future multimodal AI models in EU," Axios (July 17, 2024), https://www.axios.com/2024/07/17/meta-future-multimodal-ai-models-eu.

> More recently, in June 2026, Apple announced that it would indefinitely delay the EU launch of its Siri AI features in iOS 27 and iPadOS 27, stating that there was no timeline for their availability after the European Commission rejected each of Apple's proposed compliance solutions, including a phased, 18-month rollout safeguarded by a new 'Trusted System Agent' intermediary designed to let third-party assistants securely access the same device capabilities as Siri AI.[17] These delays represent the leading edge of a recurring pattern in which EU SMEs and consumers receive frontier AI capabilities later than, or not at all relative to, their U.S., U.K., and Asian counterparts.

Unfortunately, the European Commission does not appear to be willing to fully grapple with the realities of life under DMA for small business and startup innovators. On April 28, 2026, the Commission released its first review of the DMA[18] and declared the law 'fit for purpose', highlighting options now provided to European users regarding data portability between services and changing default programs on devices. The report did not, however, adequately address the uncertainty that DMA enforcement has generated across the wider ecosystem or mention at all the conflict between DMA enforcement and the privacy and security of EU citizens and businesses. More concerningly, the report was myopically focused on competition at the top of the market, rather than a more holistic view of the broader ecosystem in which small and medium-sized companies operate. The Commission's 'fit for purpose' conclusion is irreconcilable with the evidence its own peers and EU institutions have generated over the past year, including the Draghi Report's findings on regulatory drag, the documented withdrawal or delay of frontier AI products from EU markets, and a widening transatlantic divergence in SME AI adoption. By not engaging with this evidence, the Commission has substituted process metrics in place of outcome metrics, an approach that would be difficult to justify in any other domain of regulatory review.

Despite limited evidence of success, however, many countries around the world are in various stages of developing their own DMA-like legislation, including Brazil, India, Japan, South Korea, the United Kingdom, and even some legislative proposals in the United States. As DMA spreads beyond Europe, the problems for small app developers outlined above will be compounded.

---

[17] Apple Newsroom, "Due to DMA, Siri AI delayed in EU for iOS 27 and iPadOS 27," (June 2026), https://www.apple.com/newsroom/2026/06/due-to-dma-siri-ai-delayed-in-eu-for-ios-27-and-ipados-27/; see also John Gruber, "Apple: 'Due to DMA, Siri AI Delayed in EU for iOS 27 and iPadOS 27'," Daring Fireball (June 11, 2026), https://daringfireball.net/linked/2026/06/11/apple-dma-siri-ai.

[18] https://digital-markets-act.ec.europa.eu/review-highlights-digital-markets-act-remains-fit-purpose-and-has-positive-impact-2026-04-28_en

Conclusion

ACT members believe in and are well familiar with the power of competition to lead to better and more innovative products, services, and technology. Two years after its effective date, it is difficult to see how DMA has achieved this aim. Instead, the most concrete results have been delayed access to new features and technologies, uncertainty regarding implementation and enforcement, and increased work, cost, and risk for SMEs both in the EU and globally. Specifically, ACT urges the European Commission to:

- Pause further extension of DMA obligations to new services, markets, and technologies, particularly artificial intelligence and cloud computing, that were not part of the law's original evidentiary record;
- Narrow enforcement to conduct for which a concrete competitive or consumer harm can be identified, rather than presumed; and
- Reopen the 'fit for purpose' review to incorporate evidence on SME outcomes, security and trust effects, and the documented withdrawal or delay of frontier products in EU markets.

ACT further urges policymakers elsewhere in the world considering DMA-style frameworks to observe and learn from a credible, evidence-based assessment of the DMA before importing its architecture. Indeed, far more workable solutions have been developed in other countries such as the United Kingdom and Japan in the wake of the DMA's adoption and implementation. ACT continues to work with policymakers around the world to advance governance frameworks that empower entrepreneurship and innovation throughout the digital economy.