Analysis

Vietnam's Proposed Amendment to its Law on Competition Targeting Digital Suppliers

Introduction

The Vietnam Competition and Consumer Authority's new draft amendment[1] to the country's 2018 Law on Competition,[2] inspired by Europe's Digital Markets Act (DMA), risks significantly increasing legal uncertainty and imposing disproportionate compliance burdens on U.S.-based firms, thereby creating significant barriers for cross-border business models. Although framed as a measure to address the alleged abuse of dominant market position by digital platforms, its broad scoping risks creating a two-tiered enforcement regime. Certain, mostly U.S.-based firms would be subject to unique and wide-ranging conduct obligations, while domestic industries such as telecommunications service providers, brick-and-mortar retailers, and legacy news broadcast outlets would remain exempt, even when offering like services. Thus, in addition to advancing problematic competition policies, this differential treatment implicates Vietnam's international trade commitments. To the extent that these policies materially impede market access, as they would appear to do, they would restrict access to a digital marketplace that is expected to be worth up to $200 billion by 2030.[3]

Background

On June 2, 2026, the Vietnam Ministry of Industry and Trade opened a public consultation[4] on a proposed amendment to the Competition Law. The proposed amendment represents Vietnam's latest effort to advance digital competition regulation, following a January 21, 2026 consultation.[5] This proposal has drawn criticism[6] for imposing expansive and burdensome obligations on large digital firms, including concerns that such frameworks may operate in a discriminatory manner, disproportionately affecting U.S.-based digital services suppliers in cloud computing, digital advertising, online retailing, and digital content sectors.[7] This approach, relying on arbitrary criteria for scoping in particular firms, could reduce competitive opportunities for foreign service suppliers and serve as a *de facto* barrier to digital trade.

---

[1] Vietnam Ministry of Industry and Trade, *Public Consultation Dossier on the Law on Amendment and Supplementation of a Number of Articles* (Jun. 1, 2026), https://moit.gov.vn/du-thao-van-ban/lay-y-kien-doi-voi-ho-so-du-an-luat-sua-doi-bo-sung-mot-so-dieu-cua-luat-thuong-mai-luat-canh-tranh-luat-quan-ly-ngoai-t.html.
[2] LuatVietnam, *Competition Law, Law No. 23/2018/QH14* (last accessed Jun. 10, 2026), https://english.luatvietnam.vn/law-no-23-2018-qh14-dated-june-12-2018-of-the-national-assembly-on-competition-164727-doc1.html.
[3] *See,* International Trade Administration, *Vietnam Country Commercial Guide: Digital Economy Overview* (last updated Apr. 23, 2026), https://www.trade.gov/country-commercial-guides/vietnam-digital-economy-chapter.
[4] *Supra* n. 1.
[5] Vietnam Ministry of Industry & Trade, *Policy Dossier of the draft Law on Amending and Supplementing a Number of Articles No. 23/2018/QH14 of June 12, 2018, on Competition (Competition Law)*, (Jan. 21, 2026), https://moit.gov.vn/du-thao-van-ban/ho-so-chinh-sach-du-an-luat-sua-du-an-luat-sua-doi-bo-sung-mot-so-dieu-cua-luat-thuong-mai-luat-canh-tranh-luat-quan-ly-.html.
[6] *See*, Dir Auer et. al., *ICLE Comments on Amendments to Vietnam Law No. 23/2018/QH14* (Feb. 2, 2026), https://laweconcenter.org/resources/icle-comments-on-amendments-to-vietnam-law-no-23-2018-qh14/.
[7] Tom Simpson, *What is the State of Vietnam's Digital Economy in 2026? A Comprehensive Market Overview*, Digital In Asia (Apr. 3, 2026), https://digitalinasia.com/vietnam-digital-market-overview-2026/.

The amendments make two key changes, described in detail below: additional criteria for establishing market power, focused on digitally-relevant factors; and further elaboration of prohibited conduct, also tailored to digital markets.

Draft Amendment to the Competition Law

Expansive Scope for Determining Substantial Market Power

The draft amendment's proposed changes to Art. 26 broadly defines *substantial market power* by including certain digital-related factors, such as the scale of the number of sellers and buyers on a digital platform; the ability to collect, accumulate, control, process, and exploit data; the ability to use digital technologies such as algorithms and artificial intelligence (AI) to coordinate or control transactions, prices, or user behavior; and several other factors. Although most of these indicia are not explicitly linked to digital suppliers, their prevalence in digital markets suggests that these will be the key criteria used to establish a finding of market power. While market power is a key concept in competition analysis, an overly broad definition risks treating any degree of influence in widely prevalent technologies as sufficient to satisfy the statutory requirement, potentially leading to enforcement based on hypothetical capabilities rather than demonstrable harm.

In practice, such a scope would likely predominantly capture foreign, especially U.S.-based, firms, given their success to date in the Vietnamese market. As the result of a finding of market power, imposing specific prohibitions and obligations primarily on U.S.-based companies could lead to discriminatory or "less favorable treatment" of U.S. service suppliers, potentially infringing on Vietnam's trade obligations under the 2001 Bilateral Trade Agreement,[8] the World Trade Organization's General Agreement on Trade in Services (GATS),[9] and the U.S.–Vietnam Framework for an Agreement on Reciprocal, Fair, and Balanced Trade.[10] The draft amendment's scoping could be construed as preferential treatment to (largely domestic) brick-and-mortar retailers and other traditional suppliers (broadcasters, telecommunications suppliers), who compete directly with U.S. online suppliers, likely leading to discriminatory treatment of U.S. and foreign-based digital firms.

Excessive Conduct Prohibitions and Obligations on Firms

Similar to the European Union's Digital Markets Act (DMA), the draft amendment would impose specific conduct prohibitions and obligations on firms found to have substantial market power, including bans on self-preferencing and tying, limiting access to competing services (multi-homing), data-sharing requirements, and limits on the use of information from third-party sellers (see Annex). Such obligations effectively function as an *ex-ante* regulation: once a supplier is deemed to have market power (i.e., analogous to the EU designation

---

[8] *See*, Office of the United States Trade Representative, *Agreement Between The United States Of America And The Socialist Republic Of Vietnam On Trade Relations* (Jul. 13, 2000), https://ustr.gov/sites/default/files/US-VietNam-BilateralTradeAgreement.pdf.

[9] *See,* World Trade Organization, Art. V (1)(b), "General Agreement on Trade in Services" (accessed Jun. 8, 2026), https://www.wto.org/english/docs_e/legal_e/26-gats_01_e.htm.

[10] *See,* Office of the United States Trade Representative, *Fact Sheet: The United States and Viet Nam Reach a Framework for an Agreement on Reciprocal, Fair, and Balanced Trade* (Oct. 2025), https://ustr.gov/about/policy-offices/press-office/fact-sheets/2025/october/fact-sheet-united-states-and-viet-nam-reach-framework-agreement-reciprocal-fair-and-balanced-trade. The *ex-ante* provisions of the draft amendment would risk increasing the barriers to digital trade, services, and investment.

process), firm-specific conduct restrictions would apply, which do not apply to the market generally.

Specifically, the draft amendment prohibits businesses with a dominant market position from imposing unreasonable conditions on business users to access data generated by their legitimate business activities on the platform, which could lead to increased barriers to entry or consumer harm. The requirement under proposed Art. 27(m), which bears a striking resemblance to Article 6(10) of the DMA,[11] would introduce significant privacy and safety risks.

Mandated data access to users' sensitive on-device data by third-party apps could enable malicious actors to exploit different kinds of data, including: (i) device fingerprinting and user profiling; (ii) data exfiltration; (iii) user interface (UI) spoofing and phishing; (iv) spyware capabilities; and (v) audio capture risks from voice-activations. This would increase users' security risks and expose them to unwanted surveillance, fraud, malware, and abuse by malicious actors. Such obligations can affect device integrity and security, as tools and technologies to fight spam, scams, and other harmful activities would be compromised if third-party apps are not obligated to meet those same standards and allow such tools to work on their networks.[12] Forced data sharing could enable harms such as theft or corruption of data, unauthorized cyber intrusion, widespread disinformation, and manipulation.[13]

The ban on using data derived from business customers to offer competing services (27(n)) is unreasonably broad and has no analogue in the bricks-and-mortar sector, where such data is commonly used to develop white-label alternatives to branded products, often a source of significant consumer benefit.

As has been seen in the EU, similar obligations there have created enormous compliance burdens,[14] significant consumer inconvenience,[15] and a reluctance of suppliers to introduce new services,[16] with little effect on improving the contestability of digital markets. In short: both burdensome and ineffective. At the same time, these burdens have put U.S. suppliers at a

[11] *Regulation (EU) 2022/1925 of The European Parliament and of The Council*, Art. 6(10), (Sep. 14, 2022), https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG&toc=OJ%3AL%3A2022%3A265%3ATOC, ("The gatekeeper shall provide business users and third parties authorised by a business user, at their request, free of charge, with effective, high-quality, continuous and real-time access to, and use of, aggregated and non-aggregated data, including personal data, that is provided for or generated in the context of the use of the relevant core platform services or services provided together with, or in support of, the relevant core platform services by those business users and the end users engaging with the products or services provided by those business users."); European Commission, Digital Markets Act, *Data Access* (accessed Jun. 8, 2026), https://digital-markets-act.ec.europa.eu/developer-portal/data-access_en.
[12] Kati Suominen, New Costs and Cybersecurity Challenges Flagged as DMA Compliance Starts, Center for Strategic & International Studies, (Mar. 22, 2024), https://www.csis.org/analysis/new-costs-and-cybersecurity-challenges-flagged-dma-compliance-starts.
[13] Brandon Pugh, R Street, What does the Google antitrust case mean for cybersecurity? (Oct. 7, 2024), https://www.rstreet.org/commentary/what-does-the-google-antitrust-case-mean-for-cybersecurity/ ("[I]f sensitive data ends up in the hands of an adversary or criminal group—or a company with weak data security and privacy protections—the consequences can be detrimental.").
[14] LAMA Economic Research, *Costs to U.S. Companies from EU Digital Regulation*, CCIA Research Center (Mar. 11, 2025), https://ccianet.org/research/stats/costs-to-us-companies-from-eu-digital-regulation/
[15] Trevor Wagener, *Europe's Digital Markets Act is Failing Users* (Nov. 11, 2025), https://ccianet.org/articles/europes-digital-markets-act-is-failing-users/.
[16] *See e.g.*, Apple, *Due to DMA, Siri AI delayed in EU for iOS 27 and iPadOS 27* (Jun. 8, 2026), https://www.apple.com/newsroom/2026/06/due-to-dma-siri-ai-delayed-in-eu-for-ios-27-and-ipados-27/; Egle Markeviciute, *The EU's Digital Markets Act: Fines, delayed features and unclear benefits*, EuroNews (Jun. 11, 2026), https://www.euronews.com/next/2026/06/11/the-eus-dma-fines-delayed-features-and-unclear-benefits.

competitive disadvantage vis-à-vis domestic and third-country suppliers not subject to the obligations, raising serious issues of discrimination under trade rules.

Conclusion

The proposed draft amendment to Vietnam's Law on Competition would establish an overly broad digital regulatory regime that goes well beyond conduct-based competition enforcement based on a specific finding of harm, and introduces prescriptive prohibitions and obligations for covered companies. While framed as a measure to curb abuse of substantial market power in digital markets, the bill imposes disproportionate compliance burdens on large digital intermediaries, particularly U.S. firms, in ways that markedly diverge from U.S. antitrust enforcement. To the extent the proposal applies to certain digital business models, such as online marketplaces, while exempting their brick-and-mortar competitors offering comparable services, it risks creating a discriminatory and non-neutral regulatory environment, putting U.S. firms at a competitive disadvantage vis-à-vis both domestic and foreign competitors.

ANNEX: LIST OF NEW CONDUCT PROHIBITIONS AND OBLIGATIONS (Art. 27)

Article 27. Prohibited abuse of a dominant position or abuse of a monopoly	**EU Digital Markets Act Analogue**
(g) Prioritizing products or services provided by itself or businesses within its group of affiliated businesses with the platform's owner through display ranking, algorithms, technical conditions, data, or transaction conditions that lead to or are likely to lead to preventing other businesses from entering or expanding their market; or causing or potentially causing harm to users on the digital platform;	Article 6(5).
(h) Imposing unreasonable terms and conditions related to selling prices, payment methods, warranties, or other terms and conditions that lead to or are likely to lead to the entry or expansion of other businesses into the market; or causing or likely to cause harm to users on the digital platform;	Article 5(3); Article 6(12).
(i) Imposing or coercing users to register, use, or maintain the use of one or more other services provided by the digital platform owner or a business belonging to a group of businesses affiliated with the platform owner as a condition for accessing or maintaining access to the digital platform, or for maintaining, expanding, or developing business operations on the digital platform, resulting in or potentially resulting in preventing the participation or expansion of other businesses in the market; or causing or potentially causing harm to users on the digital platform;	Article 5(7); Article 5(8).
(k) Preventing or reducing the ability of business users to access alternative platforms that may lead to or may lead to preventing other businesses from entering or expanding into the market; or causing or potentially causing harm to users on digital platforms;	Article 5(4); Article 6(3); Article 6(6).
(l) Preventing or unreasonably hindering users, directly or indirectly, from removing pre-installed applications or services or replacing them with competing services, except when necessary to ensure network security or essential operations;	Article 6(3).
(m) Refusing to provide or imposing unreasonable conditions or costs for business users to access or exploit data generated from their legitimate business activities on the digital platform, resulting in or potentially resulting in hindering the entry or expansion of other businesses into the market; or causing or potentially causing harm to users on the digital platform.	Article 6(9); Article 6(10).
(n) Using non-public data generated or provided by businesses operating on the platform to compete with those businesses, thereby preventing other businesses from entering or expanding their market; or causing or potentially causing harm to users on the digital platform.	Article 6(2).