ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION
SCHUMPETER PROJECT ON COMPETITION POLICY

700 K Street NW Suite 600
Washington, DC 20001

COMMENTS OF ITIF

to the

Japan Fair Trade Commission (JFTC)

Office of the Counselor for Digital Affairs

In the Matter of: Mobile Software Competition Economy Act Subordinate Legislations and Guidelines	)	Public Comment

June 13, 2025

CONTENTS

Introduction 2
Analysis of Draft Guidelines 3
Prohibited Conduct 3
Article 5 3
Article 6 4
Article 7 5
Article 8 6
Article 9 7
Compliance Measures 8
Articles 10 and 11 8
Articles 12 and 13 8
Recommendations 9
Conclusion 10

INTRODUCTION

The Information Technology and Innovation Foundation (ITIF) appreciates the opportunity to respond to the Japan Fair Trade Commission's (JFTC's) public consultation on its Mobile Software Competition Act Subordinate Legislations and Guidelines ("Draft Guidelines").[1] ITIF commends the JFTC's proactive effort to issue these detailed Draft Guidelines as part of a broader effort to ensure clarity and transparency regarding the enforcement of its landmark "Act on Promotion of Competition for Specified Smartphone Software" or "Mobile Software Competition Act" ("the Act").[2]

ITIF has previously expressed concerns that the Act was both unnecessary given the thriving nature of Japan's smartphone industry and substantially risked chilling procompetitive behavior.[3] Similarly, ITIF is worried that although the Draft Guidelines provide guidance for stakeholders as to how the Act will be enforced, they do not adequately ensure that harms to mobile innovation and Japanese consumers will be minimized.

This comment proceeds in three parts. First, it provides an analysis of the Draft Guidelines' discussion of the Act's general prohibitions and compliance measures. Next, ITIF provides general recommendations to the JFTC based on this analysis to minimize the harms caused by the Act. A brief conclusion follows.

---

[1] JFTC, Mobile Software Competition Act Guidelines (Draft) (May 2025) [hereinafter Draft Guidelines].

[2] Press Release, JFTC, Regarding the passage of the Act on Promotion of Competition for Specified Smartphone Software (June 12, 2024).

[3] Joseph V. Coniglio and Lilla Nóra Kiss, Comments to Japan's Fair Trade Commission Regarding the Smartphone Software Competition Promotion Act | ITIF (Sept. 3, 2024) [hereinafter ITIF Comment].

ANALYSIS OF DRAFT GUIDELINES

Prohibited Conduct

Article 5

Article 5 of the Act constitutes a broad prohibition of data misappropriation that, as the Draft Guidelines explain, is designed to prevent designated operating system, app store, and browser providers from using third-party data to obtain "advantages in marketing, development, etc., compared to third-party app or website providers."[4] This data can include user information like name, age, IP address, and bank account numbers, as well as service specific data like downloads (operating system), purchase history (app store), and bookmarks (browser), but excludes publicly available data.[5] The Draft Guidelines also make clear both that the relevant "competitive relationship" will be defined broadly to include "hypothetical" competitors, and that whether data is used to benefit a designated operating system, app store, or browser provider's ancillary product will be determined holistically and by analyzing the purpose underlying the usage.[6]

ITIF has several concerns with the Draft Guidelines' exposition of Article 5. First, the Draft Guidelines expressly state that the specific examples of third-party data listed therein, while extensive, are non-exhaustive, such that the Act will in principle apply to any use of third-party data by an operating system, app store, or browser provider to benefit their ancillary good or service. This is likely to impose tremendous compliance burdens on designated providers and prohibit many uses of data that do not raise concerns about anticompetitive behavior. Moreover, the inclusion of hypothetical competitive relationships is only likely to increase Article 5's overbreadth: Designated providers may potentially compete with a number of third-party goods and services, and preventing them from using the latter's data will likely result in a substantial number of false positives. Third, the Draft Guidelines explicitly do not distinguish between individual and aggregated data, even though use of the latter is far less likely to have anticompetitive or anti-consumer effects.

As ITIF has previously explained, "using data across multiple markets can be a crucial way to correct information asymmetries and, in particular, better target applications to satisfy consumer preferences" and thus constitute procompetitive behavior that benefits consumers.[7] However, the Draft Guidelines do not appear to provide any clear basis for allowing designated providers to put forward procompetitive justifications for using third-party data to improve an ancillary good or service in a way that could mitigate the risk of over-enforcement noted above. In particular, while the Guidelines state that "data processing [that] has been carried out in a way that can only be used for providing goods or services in a competitive relationship" will be strongly presumed to be "used for providing goods or services in a competitive relationship," and thus treated as presumptively unlawful, the Draft Guidelines do not allow for third-party data processing which has procompetitive purposes to not be considered a violation of the Act.[8]

---

[4] Draft Guidelines at 3.

[5] *Id.* at 4-7.

[6] *Id.* at 8-9.

[7] ITIF Comment at 10.

[8] Draft Guidelines at 9.

Article 6

Like Article 5 of the Act, Article 6 represents another general prohibition on designated operating system and app store providers, and specifically a broad non-discrimination provision that restricts them from "engaging in unfair or unjustly discriminatory treatment towards third-party app providers."[9] This ban includes proscribing discriminatory treatment in connection of "reviews or examinations" involving the third-party app's ability to receive platform access."[10] Importantly, and unlike Article 5, the Draft Guidelines make clear that discriminatory treatment may be permitted if there are either "reasonable grounds" for doing so, or a cybersecurity, ethics, or dark-pattern related justification, or alternatively if the discrimination enables "a certain level of consistency."[11] Moreover, in addition to establishing a non-discrimination regime, Article 6 bans "otherwise unfair treatment," which the Draft Guidelines explain "refers to actions that restrict the business activities of third-party app providers or cause them disadvantages without reasonable grounds."[12]

As with Article 5, Article 6's overbroad prohibitions are bound to encompass a huge swath of conduct that does not raise any prima facie competition concerns. What's more, whereas Article 5 is designed to prohibit exclusionary behavior in the form of leveraging third-party data, Article 6 is focused on preventing exploitative behavior, either in the form of non-discrimination or unfair practices. While the concept of exclusionary conduct is well-defined—conduct that harms competitors and in turn harms the competitive process and consumers—determining what constitutes "unfair" discrimination or practices is inherently more subjective, and only exacerbates the extent to which Article 6 will result in false positives. Indeed, it is inherent in any market that firms will engage in unilateral practices that result in their benefit, and the mere fact that a counterparty may be disadvantaged should not in itself constitute prima facie unlawful conduct.

As ITIF noted prior, unfair and discriminatory behavior may often have a "welfare enhancing nature," and especially when it comes to perceived exploitative behavior being a way to recoup the costs on investments in innovation on a mobile platform.[13] While the Draft Guidelines are clear that discriminatory and other exploitative behavior may be justified if "reasonable grounds" exist, they not only provide little clarity as to what sorts of rationales will be accepted, but appear to preclude justifications if there are "alternative measures to achieve the same purpose," if the conduct "results in cost reductions that are not returned to smartphone users or third-party app providers,"[14] or if there are sufficiently large "disadvantages incurred by third-party app providers."[15] But requiring an analysis of less restrictive alternatives, showing that efficiency gains are passed on to consumers, or balancing" of harms and benefits, are, as U.S. courts have found, not appropriate for this type of unilateral behavior as a general matter and risks stifling procompetitive conduct.[16]

---

[9] *Id.* at 10.

[10] *Id.* at 10-11.

[11] *Id.* at 11.

[12] *Id.* at 16.

[13] ITIF Comment at 5.

[14] Draft Guidelines at 14.

[15] *Id.*

[16] *See* Verizon Communications Inc. v. Law Offices of Curtis V. Trinko, 540 U.S. 398 (2004).

Article 7

In addition to the general provisions in Articles 5 and 6, the Act also includes more targeted interoperability prohibitions involving the behavior of mobile operating systems. Specifically, Item 1 prevents designated providers of mobile operating systems from "limiting application stores provided through their basic operation software solely to those provided by the designated providers themselves."[17] Item 2, by contrast, requires designated providers to broadly make their mobile operating systems accessible to third-parties "with equivalent performance for the provision of individual software, when such OS functions are used by the designed provider."[18] In both cases, the Draft Guidelines explain that these refusals to deal with third-parties can be justified under certain circumstances, such as empowering cybersecurity, protecting user privacy, safeguarding younger users, preventing criminal behavior, and ensuring physical safety.[19]

ITIF has concerns about the Draft Guidelines as they pertain to both Items 1 and 2. First, with respect to Item 1, while it does not suffer from the overbreadth issues that plague Articles 5 and 6, and instead focuses on a specific potentially anticompetitive practice, the Draft Guidelines do not appear to acknowledge any justification for such restrictions related to the ability for firms to recoup their investments in intellectual property ("IP"). For example, firms like Apple and Google have invested billions in their mobile ecosystems and, as U.S. courts have explained in the context of evaluating restrictions on rival app store access, "IP-compensation is a cognizable procompetitive rationale."[20] Indeed, forced sharing not only disincentivizes mobile platforms from engaging in innovation, but reduces the incentives of rivals to innovate, who instead of innovating to compete can use antitrust to free-ride of the investments of others.[21]

Item 2 raises similar issues. The lack of any justification based on the ability for firms to recoup the investments they make in their platforms is likely to chill innovation both by mobile operating systems and third parties, as "[c]ompelling such firms to share the source of their advantage is in some tension with the underlying purpose of antitrust law, since it may lessen the incentive for the monopolist, the rival, or both to invest in those economically beneficial facilities."[22] Indeed, this concern about reduced investment is especially acute for Item 2 given its broad scope relative to Item 1, as rather than just focus on ensuring access for third-party app stores, "OS functions broadly encompass functions related to smartphone operation."[23] Moreover, the Draft Guidelines' clarification that access must be provided in a way that is "equivalent" to the platform's own apps ignores, as ITIF has explained elsewhere, that mobile operating systems and their

[17] Draft Guidelines at 20.

[18] *Id.* at 34.

[19] *Id.* at 25-29.

[20] Epic Games, Inc. v. Apple, Inc., 67 F. 4th 946, 986 (9th Cir. 2023).

[21] Verizon Commc'ns, Inc. v. Law Offices of Curtis V. Trinko, 540 U.S. 398, 407-08 (2004).

[22] *Id.*

[23] Draft Guidelines at 35.

ancillary services can exhibit "considerable synergies that, in many cases, will not be practically achievable for third-part[ies]."[24]

Article 8

Article 8 is focused on prohibiting specific payment restrictions, "anti-steering" practices, and other types of tying and design behavior by app store providers. Specifically, Item 1 of Article 8 "prohibits designated providers of application stores from imposing conditions that prevent individual app providers from using alternative payment management services."[25] Item 2 "prohibits designated providers of application stores from imposing conditions that prevent individual app providers from displaying pricing or other information about goods or services."[26] By contrast, Item 3 limits tying between an app store and its browser, whereas Item 4 does the same with respect to an app store's "display of the user verification method they provide."[27] Importantly, the Draft Guidelines suggest that some of the practices in Article 8 will not be deemed automatically unlawful, but rather that the justifications identified in Article 7 will be considered.[28]

ITIF's concerns with Items 1 and 2 are related to those noted above in the context of Article 7. When assessing the competitive merits of these restrictions, U.S. courts have highlighted the importance of an IP compensation justification which is omitted from the Draft Guidelines.[29] What's more, with respect to Item 1, to the extent that app stores are required by the Act to allow third-party apps to utilize external payment processors, ITIF has emphasized the pro-innovation justification for an app store charging a sufficient commission for these linked transactions, as otherwise its "ability to recoup its investments … is put at risk" given that "this relief would create a pathway for developers to bypass [an app store's] commission altogether."[30] Moreover, in addition to worsening user experience, Item 2 also risks significantly infringing on an app store's creative rights not to be forced by the government to "accommodate messages it would prefer to exclude."[31] And yet, although the Draft Guidelines recognize non-economic justifications, they do not appear to recognize any defense based on the also socially important goal of protecting speech rights.

The Draft Guidelines evince other deficiencies with Items 3 and 4. First, Item 4 does not appear to allow designated app store providers to present any justifiable reason for their behavior, despite the fact that such user verification practices may enhance user security and privacy, which the Draft Guidelines elsewhere recognize as a legitimate justification. And, for Item 3, conditional refusals to deal like the tying of an app store and browser can also have a number of procompetitive justifications, such as ensuring the best user

---

[24] Joseph V. Coniglio, Comments to the European Commission Regarding Proposed Measures for Interoperability Between Apple iOS and Devices | ITIF (Jan. 17, 2025).

[25] Draft Guidelines at 47.

[26] *Id.* at 55.

[27] *Id.* at 64, 69.

[28] *Id.* at 51.

[29] Epic Games, Inc. v. Apple, Inc., 67 F. 4th 946, 986 (9th Cir. 2023).

[30] Brief for the Info., Tech., Innovation Found. as Amicus Curiae, at 5, *Epic Games, Inc. v. Apple, Inc.*, No. 25-2935 (9th Cir. 2025).

[31] *See* Moody v. NetChoice, LLC, 603 U.S. 707, 731 (2024).

experience, even if it involves some "technical restrictions, contractual terms, or other conditions regarding the adoption of alternative browser engines."[32] However, the Draft Guidelines do not seem to include any express justification that could encompass this benefit, and thus risk chilling pro-consumer behavior.

Article 9

Article 9 of the Act prohibits designated providers from engaging in self-preferencing using a search engine, or "giving preferential treatment to their own goods or services over competing goods or services without a legitimate reason when displaying search results."[33] Like Article 6, Article 9 represents a non-discrimination regime, whereby here search results must be not be "unfair or discriminatory" in a way that gives a designated provider "an advantage to its goods or services over other competing goods or services in the display of search results."[34] The Draft Guidelines explain that a "legitimate reason" justifying self-preferencing using search will be analyzed both "in light of the purpose of such preferential treatment" as well as "the availability and nature of other less competition-restricting alternative means to achieve that purpose."[35] Importantly, the Draft Guidelines do not appear to contemplate any quantitative weighing of harms and benefits—in notable contrast to Article 6—but instead deem that search self-preferencing "will not violate the provisions of [Article 9] if there is a legitimate reason for such treatment."[36]

Unfortunately, the Draft Guidelines appear to narrowly restrict the set of purposes that can constitute a "legitimate reason" for self-preferencing using search. For example, while the Draft Guidelines acknowledge that "an explanation will be provided concerning the improvement of the quality of search services for smartphone users, including the responsiveness and accuracy that smartphone users expect from search services," they clarify that such a justification will be discounted in a variety of conditions.[37] To be sure, while some of these exclusions are appropriate—such as if the justification is merely a pretext for "the intent to exclude other goods or services in a competitive relationship with the designated provider's goods or services"—other conditions, such as whether "other goods or services are unjustly treated in an inferior position" are likely to result in pro-consumer self-preferencing being chilled: All self-preferencing invariably and in some way puts rivals in an inferior position that they may feel is "unjust."[38]

Moreover, like the non-discrimination rules in Article 6, Article 9 makes clear that a legitimate reason only exists if the preferential treatment is not "necessary" to achieve any procompetitive purpose.[39] However, as noted above, while it is true that this type of antitrust analysis is often used to evaluate procompetitive justifications in the area of concerted action, U.S. courts like in the landmark *United States v. Microsoft* case do not typically apply it in the context of unilateral behavior, including technological tying that takes the

[32] Draft Guidelines at 65.

[33] *Id.* at 70.

[34] *Id.* at 74.

[35] *Id.* at 76.

[36] *Id.*

[37] *Id.* at 77.

[38] *Id.*

[39] *Id.*

form of self-preferencing.[40] And the reason is simple: Antitrust law should not give license "to insist that a monopolist alter its way of doing business whenever some other approach might yield greater competition."[41]

Compliance Measures

Articles 10 and 11

ITIF understands the dual purpose of Article 10's data disclosure requirements "to ensure compliance with the prohibited conduct set forth in Article 5" as well as to enhance "transparency in transactions" in a way that "is expected to contribute to the promotion of innovation."[42] However, given the extensive disclosures the Draft Guidelines require, as ITIF has elsewhere made clear, the "creating and maintaining of such a repository of material would place a substantial burden" on designated providers.[43] Indeed, unless properly tailored and proportionate, "making such information available is bound to risk further diminishing the innovation incentives…by sharing what, in many cases, would otherwise be treated as highly confidential and sensitive business information."[44] Moreover, while the Draft Guidelines put forward a number of measures that a strong data management framework "could" include, it appears to nowhere establish a safe harbor such that "compliance with Articles 5 and 10 of the Act can be confirmed," which limits the effectiveness of the Draft Guidelines in providing designated providers with sufficient certainty about disclosure obligations.[45]

Article 11, by contrast, includes an extensive data portability requirement which "obliges designated providers…to ensure that smartphone users' data…can be seamlessly transferred to the user or a designated recipient at the user's request."[46] However, while the Draft Guidelines correctly seek to exclude from this obligation "data that is entirely impossible for the designated provider to transfer," and do not appear to require designated providers from collecting additional data, the Draft Guidelines appear to provide no carve outs for certain categories of data let alone bright line rules about what data will need to be transferred, but instead suggest that this determination will be made on a case-by-case basis and "after comprehensively considering smartphone user needs" before providing a number of examples of eligible data.[47] What's more, broad forced data sharing with competitors can also chill incentives to innovate in a way that is unnecessary to promote compliance with the Act.

Articles 12 and 13

Article 12 requires designated providers to generally make sure that certain default settings are easily modifiable, including through a choice screen, implement other measures to ensure user consent when new

[40] United States v. Microsoft Corp., 253 F.3d 34, 59 (2001).

[41] Verizon Commc'ns, Inc. v. Law Offices of Curtis V. Trinko, 540 U.S. 398, 415-16 (2004).

[42] Draft Guidelines at 82.

[43] Joseph V. Coniglio, Comments to the European Commission Regarding Proposed Measures for Interoperability Between Apple iOS and Devices | ITIF (Jan. 17, 2025).

[44] *Id.*

[45] *Id.* at 84.

[46] *Id.* at 87.

[47] *Id.* at 90.

features are added to the platform, as well as safeguard the ability for users to easily delete software, and in particular with respect to default search settings for browsers.[48] However, not only is there a general risk of the JFTC itself designing a designated providers' products—as opposed to simply telling them what behavior they cannot engage in—but it has been recognized that the imposition of a choice screen in connection with the EU's case against Google did not meaningfully improve competition.

Article 13 reflects a broad disclosure obligation for designated providers to make sure that third-parties using their platforms "can seamlessly respond when changes are made," which includes "measures to ensure a reasonable period and disclose the content and reasons for the change" as well as "measures to establish a system for handling complaints and other matters related to changes in specifications."[49] However, although a system for responding to third-party complaints to comply with the Act is inevitable part of compliance, the Guidelines attempt to unduly micromanage how designated operators will engage in this process, such as by placing conditions on how they must "understand the opinions and other circumstances of individual app providers" and "establish an appropriate mechanism to effectively utilize the opinions and other circumstances of individual app providers." [50] This unnecessarily inserts the JFTC into the process of commercial negotiations, as opposed to simply ensuring the outcomes of these discussions satisfy the Act's requirements.

RECOMMENDATIONS

For these reasons, ITIF respectfully offers the following recommendations:

- **Guidelines should narrowly tailor broad obligations.** Several of the articles in the Act, such as the data misappropriation ban in Article 5, the non-discrimination provision in Article 6, and the interoperability requirements in Article 7's Item 2, are likely to impose tremendous limitations and compliance burdens on designated operators as well as unreasonably chill conduct that does not present anticompetitive concerns. Revised guidelines should provide more clarity about the specific non-hypothetical circumstances where the JFTC is concerned that this behavior could plausibly harm consumers (e.g., when a designated provider has market power in an application that is benefiting from the use of a third-party rival's competitively sensitive individual data obtained on the platform).
- **The Draft Guidelines unduly limit company justifications.** Not only do the Draft Guidelines appear to provide no ability for designated operators to present an IP compensation justification for their conduct, which will chill platform investment and innovation, but they similarly omit any general efficiency justification that recognizes the procompetitive benefits that practices like tying and the cross-platform use of data can provide. What's more, in cases where the possibility to make these types of justifications do exist, they are improperly narrowed by requirements that, for example, the practice constitute the least restrictive alternative to achieve the efficiency benefits.
- **Guidelines should economize, not micromanage, compliance.** Whereas Articles 10, 11, 12, and 13 place substantial additional compliance burdens on designated operators and in some cases appear to contemplate the JFTC—rather than the company itself—determining the most effective way to

[48] *Id.* at 92-95.

[49] *Id.* at 103.

[50] *Id.* at 113.

comply with the Act, they appear to include no safe harbors or carve-outs that designated operators can rely on to minimize the costs incurred by the Act. By including compliance safe harbors and carve-outs, Guidelines can not only reduce the compliance costs imposed on companies, but also the administrative burdens on the JFTC in enforcing the Act.

CONCLUSION

ITIF is encouraged by the JFTC's effort to issue comprehensive and detailed guidelines about how the Act will be enforced and the compliance measures companies must take, and is grateful for the opportunity to submit this comment to the JFTC. While ITIF believes that the Draft Guidelines do provide stakeholders with important clarity in a number of respects, further measures could be taken to ensure that enforcement of the Act does not chill innovation and place undue compliance burdens on designated operators, including large American technology companies, at a time when the United States and Japan must be prioritizing the cooperation necessary to counter the threat posed by China's quest for global techno-economic dominance—rather than using regulation to stifle innovation of leading technology firms that have played a critical role in the growth and success of Japan's mobile industry.

Thank you for your consideration.

Joseph V. Coniglio
Director, Schumpeter Project on Competition Policy
Information Technology and Innovation Foundation