

Comments of the International Center for Law & Economics

*RE: The Japan Fair Trade Commission's Guidelines on
the Japanese Smartphone Act's (SSCPA) Subordinate
Laws and Regulations*

June 13, 2025

Authored by:

Dirk Auer (Director of Competition Policy, International Center for Law & Economics)

I. Introduction

Thank you for the opportunity to submit our comments on the "Guidelines (Draft) for the Promotion of Competition in Smartphone Software." The International Center for Law & Economics (ICLE) is a nonprofit, nonpartisan global research and policy center founded with the goal of building the intellectual foundations for sensible, economically grounded policy. ICLE promotes the use of law & economics methodologies to inform public-policy debates and has longstanding expertise in the evaluation of competition law and policy. ICLE's interest is to ensure that competition law remains grounded in clear rules, established precedent, a record of evidence, and sound economic analysis.

Our comments make the following overarching points . First, the SSCPA violates liberal economic principles by enabling discretionary intervention by the JFTC in the face of active competition in the smartphone ecosystem. The draft Guidelines do not significantly cabin this discretion. More objective criteria are called for, with limited regulatory discretion and deference to technical decisions made by Apple and Google. Second, and relatedly, the discretion is not consistent with the provisions and interpretations of the Antimonopoly Act regarding unfair or unjust discrimination. Third, the SSCPA and the draft Guidelines unfairly target Apple's integrated "end-to-end" ecosystem, and the provisions related to data use, alternative app stores and browsers, interoperability, payment systems, and pricing controls impose unobjective and overbroad standards on Apple. Fourth, these measures risk degrading device security, performance, and user experience, while discouraging investment and innovation. We provide specific examples of ways in which this may occur.

We want to express our gratitude to Professor Toshiaki Takigawa (Professor Emeritus, Faculty of Law, Kansai University) for his significant contributions to the preparation of these comments.

II. Violation of Liberal Economic Principles by Discretionary Intervention of the JFTC in the Face of Active Competition in the Smartphone Ecosystem—SSCPA General

The SSCPA broadly deems actions that are generally not recognized as illegal for private companies, or actions that should only be judged for illegality following the Antimonopoly Act, as inherently unlawful, which is contrary to the principles of a liberal economy. Excessive intervention in corporate actions undermines innovation and reduces consumer benefits. These Guidelines, regarding regulated actions related to, for instance, data usage, firstly list several specific actions like those that are recognized as illegal. However, many of these listed actions do not inherently possess unfairness. The Guidelines do not explain the reasons for deeming the

listed actions as unfair.

Secondly, for example, as stated by the Guidelines, "The specific examples are merely illustrative, and the application of Article 5 of the SSCPA is not hindered concerning data not illustrated below," the presented examples are not exhaustive, so the Guidelines do not serve to narrow the discretion of the Fair Trade Commission (hereafter, "the JFTC") and relevant government agencies, which enforce the SSCPA.

The SSCPA legitimized its adoption of *ex ante* rules (namely, per-se illegal rules) for the lack of a competition mechanism in the smartphone ecosystems. This assertion is based on the Japanese governmental study report—the Final Report on the Competition Assessment of the Mobile Ecosystems (16 June 2023), which highlighted the network effect and scale merit of the digital platform markets. However, the network effect and scale merit have their limits, so the smartphone ecosystem is not a monopoly but an oligopoly, with vigorous competition between Apple and Google. Both companies have prepared applications that simplify the process of transferring data between their platforms, enabling users to switch seamlessly between iPhone and Android devices.

iOS and Android continuously innovate to differentiate themselves, with Apple prioritizing seamless integration and security, while Android offers openness and customization. This rivalry has led to significant advancements in user experience, security, and app-ecosystem development.

Moreover, as an important recent phenomenon, the rapid development of generative AI has ushered in a new competition in the smartphone ecosystem. For instance, see Richard Waters, "Apple faces the most disruptive threat it has seen in the iPhone era", Financial Times (1 March 2024) (stating that OpenAI, the operator of ChatGPT, announced a plan for a "GPT store" – a place for developers to sell AI-powered services built on top of OpenAI's models, which pose challenge to app stores).

III. Discretionary Interpretation Not Based on the Antimonopoly Act Regarding Unfair or Unjust Discrimination—SSCPA Articles 6, 9, and Other Sections

The Guidelines does not reduce the flaws that the SSCPA automatically deems illegal the types of conduct whose illegality should be determined comprehensively under the Antimonopoly Act, nor does the Guidelines reduce the flaws in the SSCPA that the JFTC have discretionary powers to determine whether conduct is fair or unjustly discriminatory without being subject to the provisions of the Antimonopoly Act. In particular, the Guidelines' statement that "unfair

discriminatory or other unfair treatment violates the provisions of Article 6 of the Act [SSCPA]" (Guidelines, hereinafter "GL", p. 12) merely repeats the provisions of Article 6 of the SSCP. For the JFTC to arbitrarily determine unfair or unjustly discriminatory conduct without being subject to the Antimonopoly Act and to intervene in corporate conduct would shake the foundations of a free economy.

In addition to Article 6, the SSCP and its Guidelines also contain provisions prohibiting unfair or discriminatory practices. Notably, Article 9 of the SSCP specifically outlines "prohibited acts of a designated business operator [Google] in relation to search engines." The Guidelines state that "if the search algorithm standards themselves are unfair or discriminatory and are designed to favor the products or services of a designated business operator, etc., the settings themselves will be deemed to provide preferential treatment to the products or services of the designated business operator, etc. [and consequently violate Article 9]" (GL, p. 70).

However, it is crucial to recognize that Google's search display should not be evaluated solely based on the ambiguous discretionary standards of "unfair or discriminatory" or "providing preferential treatment." Instead, it should be assessed under the framework of the Antimonopoly Act.

Google's search display has already been subject to regulation under the competition and antitrust laws of both the European Union and the United States. In the EU, the General Court upheld the European Commission's decision in the "Google Search (Google Shopping)" case, Case T-612/17 Google and Alphabet v Commission (Google Shopping) (10 Nov. 2021), finding that Google violated the law. Conversely, in the US, the Federal Trade Commission essentially acquiesced in Google's actions, asserting the importance of respecting the autonomy of the company implementing the act, which can be interpreted in various ways. See the FTC File Number 111-0163 (3 Jan. 2013).

Currently, Google's dominant position in the online search market is being challenged by the emergence of generative AI. An Apple service executive has indicated that Apple is contemplating entrusting search functionality in Safari on iPhones and iPads to generative AI startups such as Perplexity rather than Google. See the Financial Times article titled "Alphabet shares slide as Apple seeks AI alternatives to Google search," published on 8 May 2025. The implementation of stringent ex ante regulation by the SSCP and the Guidelines on the online search industry, which is currently experiencing intense competition, poses a significant risk to innovation.

Moreover, Apple imposes various restrictions on app providers in order to ensure the integrity of the iPhone's technology, operability, and user convenience. The Guidelines state that "the criteria

for review from the perspective of ensuring uniformity are not deemed to be problem-free in the light of Article 6 of the SSCPA without limit, but rather their validity will be considered in light of the SSCPA's purpose of promoting competition among basic operating software and app stores, including the improvement of quality" (GL, p. 12). "In light of the Law's purpose of promoting competition" is a standard that is biased toward protecting app providers and does not consider consumer interests, resulting in excessive intervention. Ensuring the uniformity of the iPhone's technology and operability is extremely important in order to ensure the quality of the iPhone and its convenience for users, and for the JFTC to intervene in the technical details of the iPhone from the outside falls into the pitfall of "micromanagement", harming the convenience of iPhone users.

IV. Price Control of Fees—SSCPA Articles 7, 8, and Other Sections

The Guidelines clarify that SSCPA Article 7 (prohibited acts of designated businesses related to basic operating software), Item 1 (prohibition of hindering the provision of alternative app stores, etc.) includes restrictions on the level of fees that Apple can impose on app providers. Namely, "imposing an excessive financial burden on other businesses" (GL, p. 21), "considering whether the level is such that an efficient business can continue its business...considering the level of financial burden, such as fees, required by designated businesses when using alternative app stores" (GL, p. 22), "imposing an excessive financial burden" (GL, p. 22). The Guidelines also provide similar explanations for several articles other than SSCPA Article 7.

Governmental authorities' intervention in the prices that private businesses set for their products and services, by forcing businesses to set specific prices, constitutes "price control", which economists unanimously have condemned as having a major negative impact on the free economy. The reasons given in the Guidelines for price regulation - "excessive financial burden" or "level at which business can continue" - are criteria that lack objectivity and do not address the criticism of price controls. For the JFTC to conduct price regulation on such arbitrary standards amounts to transforming the JFTC into a rate-setting regulatory agency,

Indeed, a self-interested business user will always argue that the current level of fees is excessive. This exercise naturally stops wherever the most cost-conscious business users want it to stop, potentially even reaching zero. A zero-commission mandate, however, would enable free riding on the targeted companies' substantial investments in building and maintaining their operating system, encourage free riding, and undermine competition in the long term by punishing innovation and investment while rewarding reactivity and rent-seeking. But even if the commission is set above zero, the JFTC has no way of knowing what the "right" commission is,

simply because nobody knows what the “right” commission is. The risk of such price controls is twofold. First, they will need to be revised on a continuous basis to cater to the demands and complaints of both parties, which will require not only economic omniscience from the JFTC but also substantial resources. The decision is ultimately as likely to be guided by what is politically palatable as what is economically “optimal.” The JFTC is ill-equipped for such kingmaking and market micromanagement. To recoup their losses, incumbents are likely to introduce other fees, which will make someone in the ecosystem worse off. For example, Apple might start charging all app developers every time their app is downloaded from the App Store, etc.

V. Price Prohibition of Use of Data Acquired by Apple—Article 5 of the SSCPA

Article 5 of the SSCPA generally prohibits Apple from using data acquired from app providers in the course of operating the iPhone. Although the title of Article 5 states "prohibition of improper use of data," the text of Article 5 generally prohibits the use of data acquired by Apple from app providers in connection with the provision of iOS, etc., thus not being limited to "improper use." Although the Guidelines list several types of data such as those whose use is prohibited, this is not a limited list. Namely, "the specific examples of data are merely examples, and do not prevent the application of the provisions of Article 5 of the Law to data not listed below." (GL, p. 5).

It is common for private companies to use data acquired from business partners in their business activities, as long as it does not violate intellectual property rights laws and other laws, so that data use is not an act that should generally be prohibited. Even if restrictions should be imposed on data use, the scope of the prohibitions should be limited and listed in the Guidelines. The open-endedness of the list contemplated in Article 5 gives little certainty to the covered companies of whether their data collecting practices comply with the SSCPA, thus potentially chilling pro-competitive conduct that could improve products and benefit consumers.

VI. Price Restrictions on Apple's Review of Alternative App Stores—SSCPA Article 7, Paragraph 1

SSCPA Article 7, paragraph 1 prohibits Apple from prohibiting the establishment of alternative app stores to the iPhone's App Store, and prohibits Apple from "hindering" app store operators or users from using the alternative app stores.

Since the permission to open alternative app stores is required by SSCPA Article 7, paragraph 1, Apple has no choice but to allow them. However, it is extremely important for Apple to review alternative app stores in order to protect user safety and maintain the performance of the iPhone.

However, the Guidelines explain that Apple's review violates SSCPA Article 7, paragraph 1 by "imposing unreasonable technical restrictions or contractual conditions on other operators while allowing the provision or use of alternative app stores" as a "hindering" act (GL, p. 21). "Unreasonable" is a discretionary standard that has no limitations. Similarly, the Guidelines state that "For the actions of a designated business operator [Apple and Google] to be deemed as actions that hinder the provision or use of alternative app stores, it is not necessary that the provision or use of alternative app stores is completely impossible. Rather, the applicability of the actions as actions that hinder the provision or use of alternative app stores shall be determined based on the degree of likelihood of such an outcome" (GL, p. 21). Like "unreasonable," "likelihood of the outcome" is an unobjective standard, allowing the JFTC to restrict Apple's screening criteria at their discretion.

In order to protect the safety and performance of the iPhone, it is necessary for Apple's engineers and experts who are familiar with the details of the iPhone to screen alternative app stores. Allowing the JFTC, which is a novice when it comes to iPhones, or external engineers commissioned by the JFTC to intervene at their discretion would undermine the safety and performance of the iPhone and harm the interests of iPhone users. The Guidelines should specify more specific and limited reasons for the cases in which the JFTC can intervene in Apple's screening, rather than vague criteria such as "unreasonable." Short of regulating exactly how Apple should run its business and design its products, the GL should establish clear standards of reasonableness and likelihood for interventions by the JFTC.

VII. Infringement of Intellectual-Property Rights, Security Risks, and Reduced Consumer Benefits Caused by the Obligation to Open Up OS functions, Forcing Interoperability—SSCPA Article 7, Paragraph 2

SSCPA Article 7, Paragraph 2 stipulates that Apple must enable third-party companies to access iOS, the iPhone's basic OS, under the same conditions as Apple, resulting in forcing interoperability on Apple. The Guidelines explain the purpose of this as "promoting competition in individual software by prohibiting acts that prevent other businesses from using OS functions to provide individual software with the same performance as that of the designated enterprises [Apple and Google]" (GL, p. 34).

However, iOS is equipped with Apple's intellectual property rights. Intellectual property rights are rights recognized in intellectual property laws, such as the Patent Act, from the perspective of promoting innovation. Forcing Apple to offer third-party companies access to iOS, which is equipped with intellectual property rights, under the same conditions as Apple is contrary to the purpose of intellectual property laws, which are aimed at promoting innovation. The view of the Guidelines that opening up one's intellectual property to third-party companies, including competitors, "promotes competition" amounts to denying the purpose of intellectual property rights, leading to innovation degradation in the long term, thereby harming economic development and consumer benefits.

Not only that, opening up iOS, with the result of forced interoperability, poses a high risk of causing unexpected harm to iPhone users. For example, third-party companies will be able to access the camera function of iPhone iOS on an equal footing with Apple, which could lead to third-party companies using the iPhone camera to spy on users.

Moreover, forced interoperability poses a serious detrimental impact on device reliability and performance. This is evidenced by the Microsoft/CrowdStrike outage that kept airlines, hospitals, banks, and other businesses down for hours in July 2024. See Josephine Wolff, professor at Tufts and author of 'Cyberinsurance Policy', "Software crash exposes tensions between security and competition" (warning against giving software companies that kind of access to an operating system), Financial Times, 29 July 2024.

Furthermore, as a countermeasure to Article 7, Paragraph 2 of the SSCPA and its Guidelines, which force Apple to offer to third-party companies access to iOS under the same conditions as Apple, Apple might postpone the adoption of new functions such as Apple Intelligence in Japan only, resulting in reducing the benefits for iPhone users in Japan. This is exactly what happened in the EU due to uncertainties surrounding the Digital Markets Act and the AI Act.

VIII. Micromanagement of Smartphone Design and Specifications Through External Intervention—SSCPA Articles 7, 8, and 12

The iPhone's design and specifications are based on Apple's "end-to-end" (consistent management of hardware and software) philosophy, and are optimized down to the smallest detail by Apple's engineers. In this regard, the JFTC should avoid unnecessary intervention. Based on the SSCPA, external engineers, commissioned by the JFTC, will intervene and make changes to the specifications designed by Apple's engineers, who are familiar with the iPhone. This will have an unexpected negative impact not only on security but also on the performance, operability, and user convenience of the iPhone, falling into the pitfall of "micromanagement." (For information

on Apple's defense based on security, see Section 11 [Justified Defense] below.)

From this perspective, the SSCPA and the Guidelines have shortcomings in that they allow the JFTC to significantly intervene at its discretion. Intervention in smartphone design and specifications by the JFTC or external engineering groups commissioned by the JFTC should be extremely restrained.

Moreover, these Guidelines apparently have been made without consulting Apple and Google, who have specialized, detailed knowledge regarding smartphone engineering and design. For the JFTC (together with relevant agencies) to intervene in the details of smartphone design is a reckless act, putting smartphone users at a serious risk.

IX. Restrictions on Apple's Screening of Alternative-Payment Features—SSCPA Article 8, Paragraph 1

SSCPA Article 8, paragraph 1 stipulates that Apple must not prevent third-party companies from establishing alternative payment methods outside of Apple's App Store. Since the SSCPA requires that alternative payment methods be approved, Apple must screen each alternative payment method for user security.

In the case of payments inside the App Store, iPhone users do not provide personal information, such as credit card information, to individual app providers. However, in the case of alternative payment methods, users must provide credit card information and other information to individual app providers. For this reason, the alternative payment method itself weakens user security. Under this premise, Apple is forced to conduct as much screening as possible to maintain security.

However, the screening conducted by Apple is subject to regulation by the JFTC as an act that "hinders" the implementation of alternative payment methods (SSCPA Article 8, paragraph 1, subsection b). The Guidelines explain that "actions that are likely to make the use of alternative payment management services difficult" and "imposing contractual conditions on individual app providers" are acts that hinder the use of alternative payment services (GL, p. 47). For monetary payments from app providers in exchange for Apple's screening, see Section 3 [Price Control of Fees] above.

The Guidelines' criteria for "highly likely to make use difficult" and "unreasonable" are unobjective and allow the JFTC to broadly regulate Apple at its discretion. If user information, including credit card information, is leaked, it can be misused for online fraud. Sophisticated online fraud equipped with generative AI is astronomically on the rise. From this perspective,

Apple's screening of alternative payment methods is required to be quite strict. The Guidelines should therefore clearly state that Apple's screening will be respected and that regulatory restrictions will be kept to a minimum.

X. Restrictions on Apple's Review of Link-Outs—SSCPA Article 8, Paragraph 2

The act of placing a link that directs users from within an app or website to an external page (link-out) typically refers to the case where a browser is launched and an external webpage is displayed when a button or link within the app is tapped. Before the SSCPAs came into force, general apps could not freely place external links in the iPhone App Store in Japan, and certain conditions had to be met.

Link-outs pose a high risk of directing iPhone users to problematic sites. Users are directed to cyber fraud sites, pornographic sites, and gambling sites. Cyber fraud is rapidly increasing, and Japanese people in particular are suffering huge losses. Given that the Japanese population is rapidly aging and the mental acuity of seniors deteriorates, preventing cyber fraud is extremely important, particularly in Japan. For this reason, it is essential that Apple imposes restrictions on link-outs after the SSCPAs come into force. For example, by limiting destinations to sites operated by the app provider in question.

However, SSCPAs Article 8, paragraph 2 restricts Apple's restrictions on link-outs. Namely, restrictions placed on link-outs by Apple are regulated as "hindering" acts under Article 8, paragraph 2, subsection (b) of the SSCPAs. The Guidelines refer to link-outs as "external redirection information" and explain that Apple must not hinder "links that transition from the individual software to web pages outside the individual software" (GL, p. 53).

Acts by Apple, which are "highly likely to make link-outs difficult," and "to impose unreasonable technical restrictions or contractual conditions on individual app providers, imposing excessive financial burdens on individual app providers, and guiding smartphone users not to receive products or services through related web pages, etc." are considered to be "hindering" acts (GL, p. 55). The Guidelines give numerous examples as hypothetical cases (GL, pp. 56-57). "Highly likely to make difficult" and "unreasonable" are descriptions that allow broad discretion to the JFTC.

Apple has a direct interest in ensuring a high level of security and privacy, given that its reputation is tied to the overall perception users have of the iPhone, and even if harm occurs through a third party, it *still* occurs on an iPhone. The Guidelines must establish where the boundary lies between

a legitimate warning and an undue obstacle to third-party payments. Surely competitors would prefer no friction at all, but that friction, which could be construed as an obstacle, might be justified on account of the risks involved.

For instance, a screen warning users that they are about to leave Apple's secure system, or that Apple is not responsible for any privacy or security issues that arise from the use of third-party payments and link-outs, should not be considered to make the use of alternative payment systems "difficult". It also should be acceptable for Apple to limit the language third-party payment systems that can be used in advertising to users, such as through hyperbole or outright deception.

Because link-outs are inherently an act that is likely to expose users to risk, the JFTC should allow Apple to conduct strict screening. The Guidelines should avoid using discretionary language and provide a more limited explanation of the act of "hindering." Furthermore, it is necessary to consult with Apple, which is familiar with smartphones, to review the examples listed in the Guidelines to see whether all of these examples are appropriate as prohibited actions.

XI. Restrictions on Apple's Review of Alternative Browser Engines—SSCPA Article 8, Paragraph 3

Enabling iPhone users to download apps from the browser and access sites outside of the iPhone may seem convenient at first glance, but it exposes users to various risks. For this reason, Apple allows users to choose alternative browsers other than the default Safari, such as Chrome, but requires Google and other companies to use Apple's designated browser engine (WebKit).

The SSCPA opposes this setting by Apple and prohibits (under Article 8, paragraph 3) Apple from "hindering alternative browsers from being components of the individual software," including the designation of Apple's designated browser engine. Since the designation of a browser engine itself is prohibited by the SSCPA, Apple will protect user security by restricting the specifications of alternative browsers. However, under the "hindering" provision under Article 8, paragraph 3, subsection (b) of the SSCPA, the JFTC will restrict the alternative browser restriction measures adopted by Apple to ensure user security.

The Guidelines explain that this "hindering" behavior includes "actions that are likely to make it difficult to adopt an alternative browser engine for the individual software" and "imposing unreasonable technical restrictions or contractual conditions" (GL, p. 62). Criteria such as "highly likely to make it difficult" and "unreasonable" lack objectivity, allowing the JFTC broad discretion. Apple's restrictions on the specifications of alternative browsers are essential to protect the security of iPhone users. JFTC's discretionary intervention in Apple's measures puts user security

at risk. The Guidelines should not be based on criteria that lack objectivity, but should give the JFTC more limited authority.

Furthermore, the Guidelines provide detailed explanations of seven cases of "hindering" behavior as "assumed examples," and then list spanning over two pages "legitimate examples." This forms an extremely minute intervention in Apple's operation, where smartphone experts gather, falls into the pitfall of "micromanagement." It is best to avoid endorsing such detailed intervention in the Guidelines.

XII. The JFTC Has too Much Discretion in Justification Defense, and Maintaining Smartphone Performance Is Not Included in Justification Reasons—SSCPA Articles 7 and 8

Articles 7 and 8 of the SSCP A provide that prohibited acts are exempt from prohibition when "acts necessary for ensuring cybersecurity, etc., are performed and it is difficult to achieve that purpose through other acts." The Guidelines list justification spanning five pages (GL, pp. 25-29).

However, justification cases are not limited to these hypothetical cases. Apple, which manages and operates the iPhone, will likely bring up various measures necessary to ensure security, etc. The Guidelines state that "the following specific examples are merely illustrative, and whether or not justification is recognized requires individual and specific consideration" (GL, p. 25) and that "it is limited to the extent necessary in light of the purpose" (GL, p. 42), thus allowing the JFTC great discretion. However, the iPhone has made protecting the security of its users its most important principle from the beginning of its launch, and this principle has been supported by iPhone users. Regulators are required to respect measures taken by Apple to ensure security as justification.

Furthermore, it is necessary to interpret "security, etc." as including the purpose of maintaining smartphones' performance, operability, and user convenience. For reference, under the EU Digital Markets Act (DMA) provisions and its implementation by the European Commission, Apple is permitted to take measures to maintain the "technical integrity" of iOS, etc. - CASE DMA.100203 - Apple - Operating systems - iOS - Article 6(7) - SP - Features for Connected Physical Devices (19/09/2024), Para (9).

In this regard, the Guidelines state, "prevention of abnormal smartphone operation" and "measures to prevent smartphones from stopping functioning" (GL, p. 25) as justification examples. This statement indicates that the Guidelines regard maintaining smartphone

performance, operability, and user convenience as not a justification, except in extreme situations such as a stoppage of functioning. It is required to accept measures taken by Apple to maintain the performance, operability, and user convenience of iPhones as justification measures in general, not just in extreme cases.

XIII. Restrictions on Apple's Review of Default Changes—SSCPA Article 12

SSCPA Article 12 requires Apple to take "necessary measures to enable users to change the default settings with simple operations." However, since default changes impact iPhone's design, they may affect the security, operability, and functionality of the entire iPhone, not just the parts that are changed.

In the case of PCs, users who change the default settings are familiar with PCs and change the defaults, aware of their risks. In contrast, many iPhone users, including school-age children, cannot imagine the adverse effects that default changes will have on the security, function, operability, and user convenience of the iPhone. Users will be tempted by solicitations from vendors and others to make default changes that harm their interests.

Unlike Articles 7 and 8, SSCP Article 12 is positioned as a "mandatory provision" and does not allow Apple to use a justification defense. However, the "necessary measures" in Article 12 are an expression that allows room for interpretation as to what extent Apple must take to be considered to have taken the "necessary measures."

The Guidelines explain that "standard settings related to the basic operating software" in SSCP Article 12, item 1, subparagraph (a) means "settings that launch a specific browser under the control of the basic operating software and display the linked web page" (GL, p. 87). On current iPhones, the browser that launches from the "basic operating software" (iOS), the default browser, is Safari. Apple is required by SSCP, Article 12, item 1, subparagraph (a) to take "measures necessary to enable smartphone users to change the standard settings with simple operations."

The Guidelines specifically state that "necessary measures" include "creating categories in the smartphone settings app that consolidate and display individual software that is the target of the standard settings, and making it possible to centrally change the standard settings from those categories" (GL, p. 88). This means, for example, that when an iPhone user boots up the iPhone for the first time, a browser "selection screen" should be displayed, allowing users to choose between Safari, Chrome, Firefox, etc.

However, on current iPhones, although users can select Chrome and other browsers and make them the defaults, Safari is set as the initial default because it is integrated with iOS and functions smoothly, so Safari is given priority. If users select a browser other than Safari without knowing this fact, they will experience unexpected inconvenience. Therefore, Apple should be allowed to take other measures rather than making it mandatory to display the "selection screen." Even if it becomes mandatory to display the "selection screen," Apple should be allowed to display Safari first.

Moreover, the Guidelines stipulate that Apple should provide a selection screen similar to that for browsers regarding Apple's default apps, like Apple Calendar and Apple Maps (GL, pp. 89-90). However, just as with Safari, Apple Calendar, and Apple Maps are the default apps on iPhones because they are integrated with iOS and function smoothly. If iPhone users select apps other than Apple's, unaware of this fact, they will experience unexpected inconvenience. Furthermore, even with current iPhones, users can download from the App Store, for example, Google Maps or Google Calendar. Therefore, the JFTC should avoid requiring Apple to display a "selection screen", allowing Apple to take alternative measures. Furthermore, even if the JFTC requires Apple to display a "selection screen," the JFTC should allow Apple to display Apple Calendar or Apple Maps at the top.