CENTER FOR
CYBERSECURITY
POLICY AND LAW

June 13, 2025

VIA ELECTRONIC SUBMISSION

RE: Request for Public Comments on *Subordinate Legislations and Guidelines of the Act on Promotion of Competition for Specified Smartphone Software (Mobile Software Competition Act (MSCA))*

The Center for Cybersecurity Policy & Law ("the Center") appreciates the opportunity to submit the following comments in response to the Japan Fair Trade Commission's (JFTC) Request for Public Comments on *Subordinate Legislations and Guidelines of the Act on Promotion of Competition for Specified Smartphone Software (Mobile Software Competition Act (MSCA))* ("Guidelines"). The Center is an independent organization dedicated to enhancing cybersecurity worldwide by providing government, private industry, and civil society with practices and policies to better manage security threats.

The Japanese Government's competition-oriented reforms of the mobile software industry come at a time when the cybersecurity threat landscape is rapidly degrading. The Japanese Government itself has acknowledged that all policies must take into account the new national security reality. As noted in the National Security Strategy (NSS) of 2022: "The Government will improve coordination with other policies that contribute to the enhancement of cybersecurity, such as economic security and the enhancement of technical capabilities related to national security." Given this evolving threat landscape and the subsequent national security policy emphasis outlined in the NSS, it is essential that the JFTC's subordinate legislations do not inadvertently undermine the very security posture they are meant to support. The security of consumers' data and devices is now inseparable from the broader national security posture of Japan. Our recommendations can be distilled into three high level points:

1. **Maintain Robust Cybersecurity Exceptions**
   The Center strongly supports the JFTC's inclusion of cybersecurity exceptions as 'justifiable reasons' for noncompliance across the MSCA Articles and urges that these be interpreted broadly to allow Designated Providers to proactively protect users, the mobile ecosystem, and national security interests.

2. **Allow Designated Providers to Restrict and Vet Third-Party Apps and App Stores**
   The Center recommends that Designated Providers retain flexibility to conduct robust cybersecurity reviews and to discourage or restrict the use of alternative app stores and unsafe third-party applications, ensuring the security of consumers' devices and data.

3. **Enable Reasonable Restrictions on Link-Outs**
   The Center urges the JFTC to ensure Designated Providers can impose reasonable limits on external linking to mitigate elevated risks such as phishing, identity theft, and fraudulent transactions—aligning with Japan's national campaigns and security strategies.

The Center believes that the security of mobile devices, operating systems, applications, and by extension the trust users have in them, is a core driver of an innovative and healthy mobile marketplace. The security protections in place for most mobile devices — iteratively developed over the last decade — are multi-layered, comprehensive, and more effective than those of traditional computing devices. In our *Mobile Future: Pathways to Continued Improvement in Mobile Security and Privacy* report, we explain how mobile device security offers a model for how security can be done properly while enabling continuous improvement.[1] However, we are concerned that several governments' recent proposals to increase competition, privacy, and other laudable policy objectives in the mobile ecosystem will degrade this work. Specifically, as outlined in our *Trusted App Store: Protecting Security and Integrity* report, we believe that a proliferation of ways to install apps will overwhelm users and open numerous avenues for bad actors to exploit them.[2] In turn, this would create confusion about the trust, safety, and security processes that third-party app stores may or may not implement and whether they are effective. This confusion would significantly impact the user experience and safety of citizens, especially those with poor information technology literacy, undermining both the security and competition of the mobile ecosystem.

The Center appreciates that JFTC explicitly accounts for security considerations in these Guidelines. The Guidelines implicitly acknowledge that the risk profile for third-party applications is different than those developed by Designated Providers and that Designated Providers play a key role in ensuring that consumers benefit from a high level of cybersecurity when using their devices, operating systems, and the first and third-party applications on them. Nevertheless, the exemptions to MSCA requirements for cybersecurity reasons, if not applied expansively enough, could still prevent Designated Providers from protecting the security of users and their products. Our comments focus on our concerns as they relate to JFTC's guidance on Articles 6, 7, and 8 of the MSCA.

Article 6 - Prohibition of Unjust Discrimination or Otherwise Unfair Treatment

---

[1] *Mobile Future: Pathways to Continued Improvement in Mobile Security and Privacy*, May 1, 2021, available at: https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/660ab0cd271a25abeb8004be_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[2] *Trusted App Stores: Protecting Security and Integrity*, February 22, 2024, Heather West & Tim McGiff, available at *https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/660ab0cd271a25abeb8005cc_CCPL_TrustedAppStore.pdf*

Article 6 of the MSCA prohibits Designated Providers from engaging in "unfair or unjustly discriminatory treatment towards third-party app providers" when evaluating whether and under what conditions those third-party app providers are allowed to use the Designated Provider's basic operation software or application stores. However, according to JFTC's Guidelines, Designated Providers may conduct reviews of third-party software–and potentially prevent them from using basic operation software or application stores–if doing so is necessary to "ensur[e] cybersecurity."

The Center strongly supports JFTC's inclusion of this cybersecurity exception, which is not present in similar legislation in other jurisdictions, such as the European Union's *Digital Markets Act*.[3] This exception is crucial because it allows Designated Providers to maintain a high level of cybersecurity in their products by conducting routine, multi-layered cybersecurity reviews (i.e., pre- and post-installation reviews) of third-party applications. These reviews of third-party providers are essential because, while Designated Providers can inherently trust their own internal cybersecurity practices, they cannot extend the same level of trust to third-party providers without verification. Although consumers claim to prefer secure products, and their demand somewhat influences third-party app security, this alone is insufficient to guarantee robust cybersecurity across all applications. Additionally, consumers are not always equipped to make these judgements themselves, and generally rely on Designated Providers to set controls and policies that protect them. Indeed, in the case of malicious actors, their technical claims around security may not be ones that a consumer can effectively evaluate. Given this, disallowing certain kinds of review to verify the cybersecurity of third-party applications could cause significant harm to users. For example, imagine a user is able to download a compromised third-party application from an alternative application store. If this compromised application automatically has access to the same core operating system functionalities as a Designated Provider's verified apps, it could gain access to sensitive user data. For an average Japanese user, this could include the user's financial information (e.g., credit card numbers), MyNumber national ID card, and other private information. Given the critical role of app vetting in device cybersecurity, the Center urges the JFTC to clearly and explicitly interpret broad "reasonable grounds" for treating third-party app providers differently. This ensures that Designated Providers can take all necessary steps to secure their devices and protect their users, thereby supporting the growth of a competitive mobile ecosystem.

Article 7, Item 1: Prohibition on Hindering the Provision of Alternative Application Stores

Article 7, Item 1 of the MSCA prohibits Designated Providers of basic operation software from "limiting application stores" to only those they provide and from interfering with other businesses providing alternative application stores on the basic operation software. However, JFTC's Guidelines state that "ensuring cybersecurity … may qualify as [a] 'justifiable reason' for noncompliance [with requirements under Article 7, Item 1] if these objectives are difficult to achieve through other, less competition-restricting actions."

[3] Regulation (EU) 2022/1925, available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng

The Center strongly supports JFTC's inclusion of "ensuring cybersecurity" as a "justifiable reason" for noncompliance with the requirements related to alternative application stores. As noted in our *Trusted App Store: Protecting Security and Integrity* report, alternative application stores are often less diligent in policing their listings than a Designated Provider is for its own application store, which is likely why "major mobile OSs have not historically allowed third-party app stores by default."[4] This can expose users of alternative application stores to unnecessary cybersecurity risks. For example, many alternative application stores list trojanized apps that hide unwanted and harmful behaviors, such as harvesting sensitive information, behind a seemingly benign app (e.g., flashlight app) or a pirated version of a popular paid app. Some alternative application stores may even exist for the sole purpose of getting users to install these malicious apps. Similarly, many alternative application stores list older or pirated versions of apps that not only provide a diminished user experience, but also lack up-to-date security patches and vulnerability mitigations. Compounding these issues, a Designated Provider's basic operating system might not be architected to account for applications originating from untrusted sources.

JFTC's Guidelines for Article 7, Item also denotes several hypothetical scenarios of actions Designated Providers can not take regarding alternative application stores. Specifically, it states that the following are not permitted:

- **Uniform warnings without review:** "When designated providers, without conducting any reviews or examinations for any alternative application store, uniformly issue warning messages to smartphone users attempting to download and install alternative application stores, suggesting that such stores are unsafe from the perspective of ensuring cybersecurity or protecting user information."
- **Warnings encouraging users to abandon installation:** "Between the installation of the alternative application store and the installation of individual software via the alternative application store, engaging in actions or placing displays that induce users to abandon installation. For example, presenting warnings that convey an exaggerated sense of risk associated with the installation, repeatedly showing screens requesting permissions for necessary access rights without reasonable grounds, or requiring users to change settings each time an installation is performed."

The Center urges the JFTC to remove these hypotheticals from the Guidance and adopt a more expansive view of the practices needed to "ensure cybersecurity" concerning alternative application stores. While the Center understands the JFTC's intent to prevent Designated Providers from unfairly disadvantaging application stores, we believe these hypotheticals do not

[4] *Trusted App Stores: Protecting Security and Integrity*, February 22, 2024, Heather West & Tim McGiff, available at *https://cdn.prod.website-files.com/660ab0cd271a25abeb800460/660ab0cd271a25abeb8005cc_CCPL_TrustedAppStore.pdf*

accurately reflect their risk profiles. In fact, the risks associated with all alternative application stores are dynamic and depend on a variety of factors that a Designated Provider may not have first-hand insight into. These include a third-party application store's internal policies, a third-party application store's financial capacity to support security efforts, evolving geopolitical tensions, and Tactics, Techniques, and Procedures (TTPs) being used by malicious actors. For example, an alternative application store that safely lists apps today could cease moderating those listings tomorrow. This means that the only accurate way for Designated Providers to describe risk is to acknowledge the inherent uncertainty. Therefore, the only way to ensure users are accurately informed is to allow Designated Providers to issue uniform warnings and encourage users to abandon installation in certain circumstances.

Article 7, Item 2: Prohibition of Hindering the Use of Functions Related to Smartphone Operation

Article 7, Item 2 of the MSCA prohibits Designated Providers of basic operating software from "preventing other businesses from using OS functions [(e.g., APIs and other tools)] for the provision of individual software with equivalent performance." However, JFTC's Guidelines clarify that Designated Providers "may conduct reviews or examinations based on necessary standards for cybersecurity, and if a business fails to meet those standards, … may restrict use of those specific OS functions."

The Center strongly supports JFTC's inclusion of this cybersecurity exception, but would encourage a more expansive approach that clearly allows restrictions on third-party access to sensitive OS functions. In the context of cybersecurity, sensitive OS functions such as user authentication, access control, memory protection, file protection, and encryption play a role in protecting the device from threats and are protected from use or interference by third parties. However, under the MSCA, any third-party, including malicious actors, could request access to OS features and technologies that protect sensitive information or functionality, and have not been designed for broad use. This means that malicious actors could access sensitive functionalities in order to find vulnerabilities in an OS, access user data, or interfere with the functionality of other apps. Although the JFTC Guidelines seem to account for this by allowing Designated Providers to reject certain requests, this might not be sufficient at scale, especially if the Designated Provider is required to review each individual request based on detailed criteria. Similarly, third parties could request access to OS functions regardless of whether they intend to use them for the use case for which they were engineered, for unintended purposes, or for malicious ends. For example, Designated Providers have previously used contact tracing functionality built into operating systems to trace Covid-19 and provide Exposure Notifications. Under the MSCA, a third party could request to access this functionality for a wholly different purpose (e.g., a dating app tracking close interactions in the physical world). This has implications not only for cybersecurity but also for privacy should third parties abuse these functions. Therefore, the Center urges the JFTC to establish proportionate limiting principles in the Guidelines, including strict consideration of associated risks in the use of device functionality.

Article 8, Item 2: Prohibition of Hindering the Provision of Goods or Services Through Related Web Pages, etc.

Article 8, Item 2 of the MSCA prohibits Designated Providers of application stores from "imposing conditions that prevent individual app providers from displaying pricing or other information about goods or services offered through web pages or other individual software outside their own software (hereafter, "related web pages, etc.") during the operation of their individual software." It also "forbids designated providers from prohibiting individual app providers from including external links ("link-outs") that direct users to web pages outside the individual software."

The Center believes that linking out may pose particularly elevated risks to users and thus urges the JFTC to implement this requirement in a manner that allows for reasonable restrictions on linkouts. Since Designated Providers lack visibility into payment transactions conducted on the web, they cannot verify if an app delivered the product or feature for which a user paid, and cannot conduct anti-fraud monitoring on transactions made on external websites. This risk is real and significant. According to Apple, in 2022, it protected customers from over $2 billion in potentially fraudulent transactions and stopped nearly 1.7 million risky and vulnerable apps and app updates from defrauding users. Linking out also poses elevated risks of identity and data theft, account hijacking, exposure to child pornography, and distribution of malware. The Japanese Government itself acknowledges this, having recently run a campaign on "Don't open unfamiliar links." The Center supports this warning, especially considering that phishing has historically been a primary initial access vector for cybercriminals, attracting Japanese users. Given these risks and Japan's own public awareness campaigns around not opening unfamiliar links, it is clear that requiring unrestricted link-outs in apps could lead to an increase in phishing attacks and related cyber threats targeting Japanese users.

Conclusion

The Center appreciates the balance that the MSCA and the JFTC's Guidelines strike between facilitating competition in the mobile ecosystem and encouraging cybersecurity. However, as highlighted in the National Security Strategy of 2022 and underscored by the current, increasingly sophisticated threat environment, it is vital to recognize that the security of consumers' devices and data is deeply intertwined with Japan's national security. We urge the JFTC to ensure that the scope of exemptions provided for Designated Providers remains broad, enabling them to proactively address emerging cybersecurity risks and protect the security of their most vulnerable users. Without such exemptions, there is a genuine risk that otherwise well-intentioned policies will inadvertently weaken Japan's broader security posture, leaving both consumers and the nation more vulnerable to these evolving threats.

We welcome the opportunity to discuss these issues further with your team and are grateful for your willingness to engage in this vital dialogue. Please let us know if you have any other questions.

Sincerely,

Heather West
HEWest@Venable.com

Adam Dobell
ARDobell@Venable.com

Luke O'Grady
LJOGrady@Venable.com