

13 June 2025

Japan Fair Trade Commission
1-1-1 Kasumigaseki
Chiyoda-ku, Tokyo, 100-8987
Japan

Digital Trade Environment Development
Office
Information Economy Division
Commerce and Information Policy Bureau
Ministry of Economy, Trade and Industry
1-3-1 Kasumigaseki
Chiyoda-ku, Tokyo 100-8901
Japan

RE: ACT | The App Association Views Regarding the Japan Fair Trade Commission's Call for Opinions on the "Draft Cabinet Order Partially Amending the Cabinet Order Prescribing the Scale of Businesses Pursuant to Article 3, Paragraph 1 of the Act on Promotion of Competition Pertaining to Specified Software Used in Smartphones"

ACT | The App Association represents small business application developers and connected device companies, located both in Japan and around the world. These companies drive a global app economy worth more than JPY 800 trillion¹ and are responsible for approximately 570,000 jobs across Japan.² App Association members leverage the connectivity of smart devices to create innovative solutions that introduce new efficiencies across consumer and enterprise use cases and rely on a predictable and fair approach to digital economy regulation to succeed and create new jobs. Therefore, the Japan Fair Trade Commission's (JFTC) development of its policies for interventions into digital platform markets is directly relevant to the App Association.

As we have explained in previous comments to JFTC, Japanese government intervention into the digital platform ecosystem creates a substantial risk of undermining Japan's digital economy, which is supported by platforms that compete with each other to provide small business developers with a means for secure and ubiquitous access to customers at low cost and with few barriers to entry. Further, Japanese government intervention into the mobile ecosystem would give rise to conflicts with Japan's trade commitments and would subvert its international competitiveness.

¹ <https://actonline.org/global-appcon22-competition-and-privacy/>.

² <http://www.progressivepolicy.org/wp-content/uploads/2016/11/Japan-App-economy-paper.pdf>.

The Value of Platforms to the Small Business Digital Economy Innovator Community

The single most important factor in the app ecosystem's dynamic growth and success is the presence of curated platforms, including app stores. Trusted app stores serve as a vital foundation for the growing uses of apps across industries and enterprises. Three key attributes led to the revolution in software distribution. Today every successful platform for mobile, desktop, gaming, and even cloud computing must provide these features or risk failing in the marketplace:

1. The provision of a bundle of services that reduces overhead costs;
2. Instantaneous and cost-effective consumer trust mechanisms; and
3. Cost-effective access to a global market.

One of the central markets at issue in the debate around the role of antitrust in the platform ecosystem—informally, we could call it the market for developer services, where a developer pays a platform for various services including distribution, marketing, etc.—also experiences vigorous competition. There is a tendency to include only two platform providers, Apple and Google, in a list of “app stores.” For small business developers, the market is much wider than two platform providers (Google Play and Apple's App Store), with different choices being most desirable based on the use case and potential customer base. Certainly, Apple's App Store and Google Play offer immense value that developers realize through lower overhead and compliance costs, built-in customer trust, increased speed to market, and wider distribution and market access. With lower costs and barriers to entry, both fledgling and established app developers can find success. These platforms provide a centralized framework for app developers to engage and secure visibility with the 5 billion app users worldwide while also serving consumers and enterprise users, representing a vibrant two-sided market. In addition to Apple's App Store and Google Play, App Association members leverage many further options for developers. A game developer can choose platforms like Epic or Steam, and enterprise developers can look to hundreds of proprietary, custom platforms (or they could create their own). Japanese government intervention into the mobile ecosystem would impact these platforms, as well as Google Play and Apple's App Store.

For developers looking to reach a general audience, using the internet is an alternative, especially for companies that are looking for different kinds of distribution or search services than those available on platforms. Further, some other options available are “aggregators” that connect people with information and run on data, as opposed to managed online marketplaces for consumers and app developers to transact directly. The variety of choices available to developers illustrates the diversity in the market for distribution methods, as developers may prefer one model over another.

The App Association notes that, although developers can choose from multiple distribution channels, there is no such thing as a perfect platform. Many developers pay a fee to platforms for developer services, and they expect those services to meet their needs. Just as online companies must clearly communicate their data practices to consumers, so must platforms clearly define the requirements and details of their terms of service to developers. For example, when platforms change their developer guidelines, they must ensure developers understand what the changes mean for them and their customer relationships. The App Association is committed to facilitating this critical dialogue amongst developers and platforms to support their pro-competitive symbiotic relationship, which ultimately benefits countless consumers.

Safety and security features are also important elements of developer services. The security features app stores provide have improved markedly over the course of their existence. Over the years, app reviews—which include automated and human analyses for privacy and security issues—have become more efficient, more transparent, and more effective. On the major app stores, developers can count on their apps being listed alongside other apps that will work as advertised, are not fake apps, and will not compromise consumers’ devices. But the high stakes game of cat-and-mouse between cybersecurity professionals and hackers will never end, and security must continue to evolve to meet and beat the threats. Platforms should continue to improve their threat-sharing and -gathering capabilities to ensure they protect developers across the platform, regardless of where threats originate. Moreover, they should approve and deploy software updates with important security patches rapidly to protect consumers as well as developers and their clients and users. The same is true when it comes to privacy controls. App developers strongly desire platform-level privacy controls they can adapt for their products and services. The types and nature of these controls vary among platforms and this variation should result in continuously improving options that iterate with end user expectations and privacy risks.

Similarly, platforms play an important role in helping small developers enforce their intellectual property (IP) rights. Our member companies’ IP helps eliminate the inherent disadvantages of being a small, innovative company by enabling them to protect the fruits of their ingenuity from larger firms that might want to take it. Unfortunately, some of our member companies fall victim to IP thieves that succeed in selling the pirated content or using it to steal ad revenue on platforms. Ad networks can and do help mitigate the pirated ad revenue problem, but platforms must also vigorously police their app stores for stolen content. With vast online stores, it is difficult for a platform to verify legitimate requests to remove allegedly pirated content. But a single app developer should not need the help of a legal team or trade association to resolve the issue. In recent years, IP resolution processes have improved across the board, and they are important and in-demand developer services that platforms should improve in order to compete for developers.

We strongly urge Japanese policymakers to recognize pro-competitive examples of vertical integration where such practices can produce greater efficiency, better quality, or lower costs for consumers. Because there are minimal antitrust issues when users and developers can easily switch to another platform, such practices should not be prohibited through government mandates. Considering that smartphones are music players, cameras, and multimodal communications devices, a narrowly focused view of one of these features without recognizing the value derived from other aspects of smart devices is incompatible with the way consumers experience them. Moreover, Japanese policymakers should expect competition to discipline harmful impacts to consumers and developers because both can leave the platform due to demonstrably low switching costs. Antitrust enforcement is generally only appropriate where the firm at issue has demonstrated market power *and* where that firm is using that market power to harm competition and consumers.

Further Study and Deliberations are Needed Before Intervention into the Mobile Ecosystem

We maintain that in considering whether, and to what degree, Japanese government intervention into the mobile ecosystem is warranted, it is vital that Japanese policymakers carefully consider the above, and that a strong evidence base is developed to support any changes to Japanese laws impacting digital economy innovation before changes are made. The foundation for making digital economy policy changes should be based on well-established and systemic harms, not edge use cases or hypotheticals. At this time, the Japanese digital economy exhibits strong indicators of healthy competition and growth, and Japanese government intervention into the mobile ecosystem is therefore unnecessary and irresponsible.

In addition, sufficient study should be done to examine whether existing Japanese laws already provide the means for ensuring competition and consumer protection in the digital economy and whether the DMCH's and JFTC's proposed legislation appropriately avoids overlapping regulation with existing law.

The European Union's Digital Markets Act (DMA), which DMCH and JFTC have indicated is an inspiration for their proposed legislation, is unquestionably a protectionist anti-trade measure that Japanese policymakers should carefully avoid aligning with. The implementation of the DMA to date has demonstrated that the law is having significant unintended consequences, and its impact on domestic and international digital commerce is not fully understood. Japanese policymakers should carefully track the DMA's implementation and its effects before mirroring the European Union's protectionist digital economy policies (which have not propelled the EU to global leadership in the digital economy to date). Japan has the advantage of observing another major jurisdiction's experimental intervention into a nascent and dynamic digital economy and should fully capitalize on its opportunity to build on the lessons learned through the creation and implementation of the DMA. On this basis alone, further Japanese government intervention

into the mobile ecosystem is ill-advised. Relatedly, the App Association notes that U.S. policymakers have rejected legislative proposals consistent with the DMA.

Finally, in addition to the public policy and feasibility issues discussed above, we urge Japanese policymakers to carefully consider whether Japanese government intervention into the mobile ecosystem would create risks of violating obligations under important trade agreements. These include Article 16 of the General Agreement on Trade in Services, which requires that all regulations affecting trade in services “are administered in a reasonable, objective and impartial manner;” as well as commitments made by Japan in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership and the U.S.-Japan Digital Trade Agreement, amongst others. Separately, we have noted President Trump’s opposition to harmful digital economy regulations being applied in a discriminatory manner for Minister Ryosei Akazawa, and have requested that Japan take steps in negotiating a new trade agreement with the United States to support access and innovation in new and emerging technology markets, such as digital platforms, by securing commitments to non-discrimination, transparency, and adequate notice and consultation.³

Recommendations on the JFTC’s Proposed SSCPA Implementation (Draft Rules and Guidelines) and Enforcement of Relevant Provisions

We offer the following specific recommendations on JFTC’s proposed rules and procedures for enforcement of the SSCPA:

Scope of Application: As JFTC determines the scale of businesses that will be subject to Article 3, Paragraph 1 of the Act on Promotion of Competition Related to Specified Software Used on Smartphones (SSCPA), we urge for the careful consideration of the small business community that will be deeply impacted by distortions to digital platform competition and innovation resulting from Japanese government interventions. Accordingly, the App Association urges JFTC to reconsider its approach to a threshold of 40 million domestic users that use the app marketplace at least once a month in each month of the marketplace’s fiscal year. As proposed, this definition would not consider non-smartphone users, effectively only applying to the Apple and Google app stores. We strongly encourage JFTC to ensure that its SSCPA regulations are applied in an objective and non-discriminatory manner, which must reflect the nature of the digital platform ecosystem as described above. JFTC can do this by counting users of any digital platform. Unless its approach to scale is altered to reflect digital platform market bounds and realities, JFTC’s implementation of the SSCPA will be selectively applied to portions of digital platform markets, distorting pro-competitive dynamics that have enabled immense small business growth and job creation in Japan.

³ <https://actonline.org/2025/05/19/act-the-app-association-letter-to-the-japanese-government-on-trade-negotiations-with-the-united-states/>.

Unless its approach to scale and enforcement is revised, JFTC will also create risks of violating obligations under important trade agreements. These include Article 16 of the General Agreement on Trade in Services, which requires that all regulations affecting trade in services “are administered in a reasonable, objective and impartial manner;” as well as commitments made by Japan in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership and the U.S.-Japan Digital Trade Agreement, amongst others.

Protect Users from Online Fraud, Financial Crimes, and Scams: Requiring covered digital platforms to host external download links materially elevates the risk to users of malware and phishing attacks, particularly as mobile platforms are increasingly targeted by criminals and most malware is distributed from sources that do not perform comprehensive checks of applications they provide. The rollout of the SSCPA should focus on safeguarding users, given the heightened threat of online fraud, financial crimes, and scams. When requirements involve handling or sharing user information, or direct users away from secure environments, JFTC regulations should empower platforms to implement practical measures that protect individuals, as directing users to third-party sites carries notable dangers which Japan’s Ministry of Internal Affairs and Communications and the National Police Agency have noted for the public.⁴ While we appreciate that the SSCPA will obligate major app marketplaces to allow in-app links for Japanese consumers to alternative purchasing channels outside the app itself, as discussed above, the App Association’s community is deeply concerned with JFTC policy promoting users to venture beyond a platform’s protected environment where they will face increased exposure to scams and fraudulent schemes, particularly where financial data is involved. Such a dynamic undermines the foundations of trust in digital platforms that have enabled unprecedented innovation and growth by the independent small business developer community. We request that the JFTC’s guidelines provide clear guidance for covered platforms to effectively address and mitigate risks related to external purchasing links, including stipulations for how these links and their destination pages are presented to users and how these pages are managed, since random weblinks could potentially lead users to unsecure websites.

Protect Small Businesses and Consumers by Supporting Intellectual Property Rights: IP is crucial for small business software developers to protect their innovations and brands but also to safeguard user safety. When IP rights are enforced, users are less likely to encounter counterfeit or malicious software that could compromise their devices or data, as unauthorized copies often lack the security and quality assurances of legitimate products. Strong IP protection ensures that users can trust the authenticity of the software they download, reducing the risk of malware, fraud, or data breaches. In particular, JFTC should note that the safety and credibility of app marketplaces is critically important to

⁴ https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/end_user/general/02/.

small developers, given that small developers' names are not known to users, but users need to feel comfortable with downloading apps provided by unknown developers. Therefore, the app marketplace needs to be reliable, and digital platforms play a vital role in this ecosystem by implementing robust measures to defend IP and brand integrity, such as monitoring for infringement, facilitating swift takedown of unauthorized content, and providing clear mechanisms for resolving disputes efficiently. It is vital that JFTC support these platform-led protections to empower small developers to compete fairly and to maintain a safer digital environment for all users. While the SSCPA does not contain a distinct exception (i.e., "justifiable grounds") for digital platforms to protect IP, we strongly urge JFTC to detail in guidance that IP enforcement is important to user protection and is therefore a consumer protection issue, and to detail in guidance how reasonable measures by covered digital platforms to protect IP are permitted and supported.

Maintain User Functionality and Convenience: Regulatory interventions that increase access for only certain developers should not undermine the overall quality or advancement of a covered platform's offerings. JFTC should explicitly recognize user experience as a key consideration when evaluating a covered digital platform's adherence to SSCPA requirements, including as a legitimate basis for assessment in the Cabinet Order. This approach would help ensure that enforcement remains balanced and avoids unnecessary negative impacts on users, enabling continued utility of the digital platforms that App Association members rely on to compete and innovate. Notable clarifications that JFTC should provide include:

- In the context of restrictions on external purchase links, allowing platforms to highlight integrated billing systems which will minimize users' risk and confusion, particularly when they make payments;
- In the context of default switching rules, permitting platforms to design mechanisms that reduce complexity and facilitate seamless transitions for users;
- That covered platforms will not be required to allow unnecessary uninstallation of apps, since users can inadvertently delete apps and have trouble reinstalling them;
- That a covered platform's choice screens do not need to be shown once users have made choices, or consumer welfare decreases;
- That restrictions on covered platforms will not be enforced in a way that impairs or prohibits enhancing functionality or convenience; and
- That covered platforms will not be required to integrate with third-party services for features (i.e., third-party developers' access to OS feature) still under development to comply with SSCPA requirements, which could lead to suboptimal user experiences, to comply with the SSCPA; the provision of technology to third-party services should be accepted only after digital platforms fully test such feature through their own apps and ensure safety and quality of such access.

We again urge JFTC to build on the lessons learned from other governments' ex-ante digital platform regulations, which do indeed take steps to ensure that consumer benefit and ease of use are central to the evaluation of potential violations. Notably, the UK's Digital Markets, Competition and Consumers Act (DMCCA) includes a "countervailing benefits exemption," which allows certain conduct if it delivers substantial advantages to users, thereby striking a balance between competition enforcement and user welfare.

We also urge JFTC to continue to secure an opportunity for us to engage after enforcement.

Conclusion

The App Association requests that JFTC consider the views of the small business digital economy community above. We welcome the opportunity to provide further perspectives and data and appreciate the ability to share our views on this critical proposal.

Sincerely,

A handwritten signature in black ink that reads "Morgan Reed". The signature is fluid and cursive, with the first name "Morgan" and the last name "Reed" clearly distinguishable.

Morgan Reed
President

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

ACT | The App Association
1401 K St NW (Suite 501)
Washington, District of Columbia
United States of America