June 9, 2022

Comments by the Centre for Information Policy Leadership on the Japan Digital Markets Competition Council's Interim Assessment of Competition within the Mobile Ecosystem

The Centre for Information Policy Leadership (**"CIPL"**)[1] welcomes this opportunity to provide comments to the Digital Markets Competition Council (**"the Council"**) on its Interim Assessment of Competition within the Mobile Ecosystem ("**the Interim Assessment**"). CIPL supports the Council's desire to foster competition in digital markets while ensuring effective data protection in Japan's digital economy.

CIPL has previously engaged with the Japanese Personal Information Protection Commission (**"PPC"**) on a number of occasions, including during a PPC side event in the margins of the G20 meetings in 2019, where CIPL and other stakeholders discussed crucial data protection topics, such as data driven innovation, rights of data subjects, accountability, and artificial intelligence. CIPL also organized a multi-stakeholder workshop in Tokyo in May 2017 to discuss Japan's data privacy regime and how it would enable cross-border data flows, innovation, and privacy protections. The workshop included representatives from the PPC, the Ministry of Economy, Trade and Industry (METI), and the Ministry of Internal Affairs and Communications (MIC), as well as private sector representatives.

In furtherance of our commitment to collaborate with digital market authorities in Japan, CIPL would be very pleased to organize a similar workshop/roundtable or in-person meeting with the Council in Japan for a more thorough discussion of the issues addressed below.

CIPL commends the Council for thinking so carefully about the layered structure in the mobile ecosystem—an ecosystem in which CIPL is well versed, given our assessments of the Digital Markets Act[2] (**"DMA"**) and Digital Services Act (**"DSA"**) in the European Union, as well as the proposed Open App Markets Act in the United States. The following comments include views gathered from CIPL member companies and other stakeholders in the course of our engagement on the DMA proposal.

For the sake of brevity, our comments are limited to the following three sections in the Council's Interim Assessment and based on our understanding of the Interim Assessment's English translation prepared by one of CIPL's member companies.

- Sec. I.2.5. Approach to be taken considering the options for response in competitive evaluation
- Sec. II.1.1-1. Operating Systems and Some Browsers
- Sec. II.1.1-2. App Stores

CIPL remains available to provide clarification and/or additional information on these or other topics raised in the Interim Assessment, including in the context of an in-person meeting or roundtable, as proposed above. For any follow-up questions, please contact Bojana Bellamy, President,

[1] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 85+ member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices to ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] References to the DMA in this response come from the version published 3 May 2022.

bbellamy@huntonak.com, and Markus Heyder, Vice President & Senior Policy Counselor, mheyder@huntonak.com.

Sec. I.2.5. Approach to be taken considering the options for response in competitive evaluation

Excerpt: "The committee will consider measures to effectively respond to certain actions by platform operators that can exert influence on multiple layers of the mobile ecosystem (competitive environment), without being constrained by the current legal framework. In doing so, the possibility of utilizing mechanisms such as information disclosure, ensuring fairness of procedures, and monitoring under the Transparency in Digital Platform Transactions Act, one form of ex ante regulation, should also be considered."

CIPL Recommendation – 1: When regulating activities that may adversely affect competition, care should be given that such regulation is coherent with other legal frameworks, such as those designed to address legitimate security and privacy concerns.

CIPL notes that the digital economy requires a regulatory approach that accounts for all interests related to data, ranging from competition, innovation, public safety and interest, consumer and data protection, among others. As the relationship between competition and data protection law is still evolving, and recognizing that the two regulatory areas intend to protect different rights and interests, it is important to consider their horizontal interaction and areas of overlap on a case-by-case and issue-by-issue basis to ensure they are in balance. In other words, it is important to avoid any pre-judgment or assumption that one regulatory area should systematically have priority over the other, or that a competition risk analysis should prevail over a data protection risk analysis (or vice-versa).

While effective data protection should not be used as a rationale to prevent effective competition and economic growth in the digital economy, consumers' legal rights also should not be compromised or degraded in deference to improving market competition. We also recommend a balanced and deliberate approach to examine all relevant rights relating to data rather than rushing into any particular solutions designed to only address competition issues. For example, a right to access certain information (which purportedly fosters transparency and innovation) must be balanced against the risk of unintentionally revealing underlying trade secrets or proprietary algorithms, or compromising data protection rights and security obligations. A balanced regulatory regime should account for all relevant rights and obligations as set out in relevant legislation.

Moreover, the Council should view regulatory issues with a broad lens and not solely from the perspective of (or the potential effect upon) the leading actors[3] in the mobile ecosystem. Any regulatory action will affect all actors in the data supply chain and ecosystem, including individual users/consumers, data recipients and other business partners. The approach will require thoughtful consideration of, and consultation with, both sharing and receiving organizations, irrespective of size. The Council should pay particularly close attention to how it weighs the benefits of particular conduct against its impact on competition and how this is reflected in the design of remedies.

[3] In this response, "**mobile ecosystem leading actors**" refers to the concept similar to "gatekeepers" under the Digital Markets Act in the European Union. On the other hand, the notion of "**mobile ecosystem actors**" refer to all market players in the digital economy covering organizations acting as gatekeepers as well as other business-users.

CIPL Recommendation – 2: Implement any new framework designed to foster a competitive environment in the mobile ecosystem while also recognizing the challenges arising from government intervention.

Recognizing that the current competition law is not sufficient to address all new competition issues in digital markets, CIPL supports forward-looking reforms. Such reforms should clearly articulate the new regulatory expectations to provide certainty for all parties concerning implementation and enforcement and that are sufficiently flexible to anticipate changes in technology and business conduct over time.

In the meantime, CIPL encourages the Council to take the following principles into consideration:

- Scope of data: Particularly with respect to a data disclosure requirement, required disclosures should be limited to data essential to enabling competition (and, of course, otherwise disclosable in accordance with other laws). Data with little or no competitive value and data containing commercially sensitive trade information or proprietary algorithms should not fall within the scope of an information disclosure requirement.

- Data Protection Rules & Principles: The competition framework should work with and complement existing data protection rules and principles under the Act on the Protection of Personal Information (**"APPI"**). Leading actors in the mobile ecosystem should be able to comply with the APPI while fulfilling obligations under the new competition framework. Moreover, it should incorporate a requirement of regulatory cooperation between competition and data protection regulators to address areas of regulatory overlap and dependencies. Competition law and data protection authorities should work together, share knowledge to create and maintain an effective digital regulatory framework with legal certainty, seamless protection of rights that also supports business and innovation.

- Risk Assessment & Liability Allocation: The approach should consider risk factors and safeguards for each player in the mobile ecosystem and should enable a risk-based approach to compliance for regulated organizations. For instance, regulated organizations should be able to evaluate in advance the risks and adverse impacts of providing access to data pursuant to any new competition requirements, and data recipients should be required to implement relevant risk mitigation measures. Careful consideration has to be given to the distribution of liability based on control over the data. Regulated organizations should not be held liable for the acts of data recipients after disclosure; liability for subsequent misuse of data should be borne exclusively by data recipients. Also, liability for data in transit must be carefully considered and apportioned. Consideration should be given to purpose limitation for the transferred (personal) data since new purposes are not foreseeable by the regulated organization and thus cannot be covered by consent.

- Regulatory Incentive: To improve compliance by regulated organizations with any new requirements and to encourage good faith support of the new regime even beyond basic compliance, regulators might consider offering rewards or incentives, or enable endorsements/accreditations for organizations that fulfill the objectives of the new regulatory framework. Such "good actor" accreditations could be achieved through certification by an independent body. They would also be a mechanisms for organizations to demonstrate their presumptive compliance with the new requirements. Of course, such accreditations would be independent of and without prejudice to other certification measures, such as certification under the APEC Cross-Border Privacy (CBPR) regime (in which Japan participates) or other mutual adequacy arrangements.

- Certainty for market participants: The framework must provide certainty for other market participants not regulated by competition remedies such that they are not hindered in operating their commercial activities in line with data protection and other laws.

Sec. II.1.1-1. Operating Systems and Some Browsers

Excerpt: "In response to concerns over the unilateral setting and changing of rules by browser providers, one option may be to establish a package of measures as follows (…) (a) implementing prior notifications that secure sufficient time to respond to rule changes, (b) appropriate disclosure of information about rule changes, (c) establishment of procedures and structures to handle inquiries from developers, (d) implementation of reporting to the government, monitoring by the government and review of the status of operations, (e) joint processes, consultations, and suspensions requiring the intervention of regulatory authorities where there are concerns that serious and imminent damages may occur to business affected by the setting or changing of rules."

CIPL Recommendation - 3: Promote constructive engagement between regulators (domestic and global) and regulated entities before and after the implementation of the new framework. Authorize enforcement remedies that permit not only the implementation of interim disciplinary measures against regulated entities in cases of serious harm to competition, but also address any significant harm arising from a legal obligation to either a regulated entity or other market participant.

The importance of ongoing regulatory dialogue between market participants and sectoral regulators in Japan and around the world cannot be overstated. Multi-stakeholder engagement is essential for ensuring regulatory coherence and building best practices across jurisdictions. CIPL supports the further evolution of initiatives such as EDPS's Digital Clearinghouse and the UK's Digital Regulation Cooperation Forum as important steps towards effective, action-driven regulatory cooperation initiatives to address challenges specific to digital services. Such initiatives are most effective where they are transparent, consultative and involve high levels of participation among all parties.

CIPL acknowledges the legitimacy of the Council's efforts to develop interim disciplinary measures against leading actors when appropriate to avert serious and immediate damage against other participants in the mobile ecosystem. To ensure legal certainty and support business continuity for all parties, there should be prior consultation with both regulated organizations and other market participants on such measures in a transparent manner based on pre-disclosed criteria and subject to regular review to ensure the measures deliver the intended outcome.

CIPL also encourages the Council to acknowledge the possibility of suspension, in whole or in part, or modification of a specific obligation if it would, for example, endanger the economic viability of the operation of the regulated organization or that of third-parties (particularly other market participants including small and medium enterprises, and consumers). Such suspension or modification may be made subject to conditions and obligations to be defined by the Council to ensure a fair balance between relevant competing interests and rights (potentially grounded in other regulatory areas) and the objectives of the new approach.

Sec. II.1.1-2. App Stores

Excerpt – 1: "It may be possible to introduce regulations that mandate that if operating system providers above a certain size provide app stores, they must allow users to (a) install third-party app stores and set those as defaults, (b) directly download apps from the browser, and (c) hide or uninstall the pre-installed app store."

Excerpt – 2: "It may be necessary to prohibit warning signs, complex procedures, and other actions that effectively limit the delivery of apps through side loading. In addition, since sideloading may be effectively restricted by various acts, such as descriptions and designs that impair or mislead end users' judgment, it may be necessary to prohibit acts that induce users to make unfavorable decisions with respect to sideloading."

CIPL Recommendation - 4: While optimizing individual choice and improving market access are important policy goals, the design of remedies should be consistent with privacy and security laws.

CIPL recognizes the role of competition authorities in balancing the consumer benefits of open competition in digital markets with the need to provide a predictable and fair trading environment for regulated organizations and other market participants. When designing remedies, competition authorities should carefully consider all aspects including practical implications when making decisions with respect to sideloading. This should begin with initiating an in-depth analysis of the competing equities involved in this practice and include interdisciplinary experts. Legitimate improvements to the means by which responsible app developers can reach their audiences may yet emerge, but a range of questions must be considered as part of the design process.

For example, competition authorities should consider whether sideloading remedies should be made subject to countervailing interests, such as user privacy, security, fraud prevention, or digital safety (as provided, for example, by the proposed Open App Markets Act in the United States). Consideration should also be given to how to operationalize a balancing or cost/benefit assessment of the competing equities - including privacy and security - in a way that provides the necessary legal certainty for both app store owners and app developers. Similarly, consideration should be given to how app store owners, device manufacturers, and users can protect users against malicious apps (such as state-sponsored cyber-attacks or imposter scams), for example via agreed security protocols.

Competition authorities would also need to consider what other laws might be implicated in the event of a data privacy and security infringement (e.g., content moderation laws) and how it would work with other competent authorities to consider the potential exposure of app stores and device manufacturers to liability under such laws in the event of infringements due to sideloading. Finally, consideration should also be given to the potential long term impacts of sideloading on the entire digital ecosystem and consumers, both positive and negative.