August 18, 2023

Comments by the Centre for Information Policy Leadership on the Japan Digital Market Competition Headquarters' Final Report on Competition within the Mobile Ecosystem

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

CIPL has been following Japan's data-related legislative and regulatory developments for a number of years and has frequently engaged with relevant Japanese regulatory bodies handling data-related issues and regulations, particularly the Personal Information Protection Commissioner ("**PPC**") and, more recently, the DMCH. In particular, CIPL submitted comments on the DMCH's Interim Assessment of Competition within the Mobile Ecosystem ("**the Interim Report**")[2] on June 9, 2022, including views gathered from CIPL member companies and other stakeholders in the course of our engagement on the European Union's ("EU") Digital Markets Act ("DMA") proposal.[3] Additional more recent examples of CIPL's engagement in Japan include participating in a multi-stakeholder roundtable in Tokyo coinciding with the G7 Data Protection and Privacy Authorities Roundtable in June 2023 to explore the potential role of the Global Cross-Border Privacy Rules ("**Global CBPR**") in fostering data free flow with trust. CIPL's president, Bojana Bellamy, also moderated an official G7 DPA side event, organized by the PPC, on "Exploring the Prospects of PETs/Data Protection in Use of AI" with key stakeholders and policymakers in Japan and international guests. Both the roundtable and the side event included representatives from the PPC, the Ministry of Economy, Trade and Industry ("**METI**"), and private sector representatives. Finally, CIPL's president, Bojana Bellamy, recently moderated a panel discussion on "Cross-Border Privacy Rules Are Going Global" at the IAPP Asia Privacy Forum 2022, which included a PPC representative, discussing the importance of enabling trusted and accountable data flows through co-regulatory certification

[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 more than 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, and regulators and policymakers around the world. For more information, please see CIPL's website. 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] CIPL Response to the Japan Digital Markets Competition Council's Interim Assessment of Competition within the Mobile Ecosystem, June 9 2022.

[3] Please find two white papers CIPL published in the context of the interplay between the DMA and the GDPR: CIPL Paper on "Bridging the DMA and the GDOR – CIPL Comments on the Data Protection Implications of the Draft Digital Markets Act," and CIPL Paper on "Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences."

mechanisms, such as Global CBPR. In this submission, CIPL offers the following points to help frame the discussion on the substance and nature of the issues raised by the DMCH.

1. General Comments

a. Supporting the "co-regulatory framework" approach

CIPL supports the DMCH's reference to the co-regulatory framework approach adopted by the Act on Improving Transparency and Fairness of Digital Platforms ("**TFDPA**"), i.e., a framework in which the government presents a principle-based framework and entrusts the regulated entities to operationalize the requirements of the framework within specified parameters. This approach is in line with CIPL's call for the need to enable **technology-neutral, future-proof, and outcomes-based digital regulation and rules,** which can be operationalized further by co-regulatory and enforceable mechanisms, such as organizational accountability, codes of conduct, and certifications. However, a TFDPA-like approach is adopted only partially in the DMCH's final report because most of the regulatory directions are ex-ante regulations. This requires careful examination by the DMCH and needs to be assessed in terms of whether or not a TFDPA-like approach is better suited for regulating competition within the mobile ecosystem in Japan. Moreover, the DMCH must bear in mind that the TFDPA came into effect only in 2021 and is applicable to app stores, an important part of the mobile ecosystem. The DMCH should avoid duplicative oversight and must make it clear whether new regulatory proposals are even needed and legitimate, considering the existing TFDPA.

It is also essential that any digital regulation and policy-making include and promote the **principle of organizational accountability** that CIPL has pioneered for more than a decade. Accountability provides flexibility for organizations to tailor compliance measures to their own unique risks and use cases while requiring them to be able to explain and validate their processing decisions when asked by regulators. Accountability enables legal regimes to remain agile and the rules to be principle- and outcome-based, setting the goals and outcomes to achieve, while leaving it to organizations to decide how to achieve these legislative goals.

CIPL believes organizational accountability is a key building block of effective data regulation and its corresponding implementation within companies. Organizational accountability can be used by companies regardless of sector or size. Its risk-based framework provides assurance to government regulators and enforcement bodies that companies are conducting risk assessments and identifying and prioritizing high-risk activities in their compliance efforts. It also simplifies investigations and enforcement actions by requiring companies to be able to demonstrate their risk assessments and compliance efforts. CIPL encourages the DMCH to explore the CIPL Accountability Framework, a recognized standard for the development of best-in-class data privacy and data governance practices as well as organizational

compliance programs.[4] This framework is law agnostic and can be applied to any area of digital regulation, from data protection to content and platform regulation to competition and responsible AI.

b. Ongoing regulatory dialogue and engagement

CIPL believes that to achieve well-functioning digital markets, it is critical to bring different policy and regulatory perspectives together to ensure a well balanced approach to digital regulation. Competition law has to take into account its impact on effective data protection. Equally, the interpretation and implementation of data protection law should take into account its effects on competition. In that regard, CIPL commends the DMCH's efforts in consulting with the PPC, Ministry of Internal Affairs and Communications ("**MIC**"), Consumer Affairs Agency ("**CAA**"), National Center of Incident Readiness and Strategy for Cybersecurity ("**NISC**"), other stakeholders and affected companies when considering regulations for the mobile ecosystem. This dialogue enables exchanges of experiences and views and supports the DMCH's comprehensive understanding of market dynamics, technical implications, and interests of regulated entities and data subjects. This in turn leads to more proportionate and effective rules and outcomes. CIPL believes it to be important to ensure that this kind dialogue and consultation between regulators and impacted businesses is further formally developed and institutionalized as much as possible and implemented on an ongoing basis.

Formalized cooperation between the DMCH, PPC, MIC, CAA, and NISC is critical to building solutions that enable both a well-functioning competitive market and effective data protection. When both objectives cannot be fully achieved, regulators have to work together to understand and agree on the trade-offs that may have to be made. Importantly, cross-sectoral regulatory cooperation must not be limited to the enforcement context only, but also expanded in all stages of consultation, creation, and interpretation of rules, as well as in the use of innovative regulatory tools, such as cross-regulatory sandboxes.[5]

In that regard, the UK Digital Regulation Cooperation Forum ("**DRCF**")[6] and Australian Digital Platform Regulators Forum ("**DP-REG**")[7] could serve as examples of effective and action-driven regulatory

[4] See CIPL resources and papers on organizational accountability.

[5] CIPL also encourages the development of innovative regulatory tools such as a regulatory sandboxes and believes that the interplay between competition and data protection in the context of the mobile ecosystem would be a perfect candidate for a regulatory sandbox. For instance, the Infocom Media Development Authority in Singapore launched Singapore's first PET sandbox in July 2022 for companies who wish to experiment with privacy-enhancing technologies. The Agency recently announced a new partnership with Google to support the PET sandbox initiative.

[6] The Digital Regulation Cooperation Forum ("**DRCF**") brings together four UK regulators, the Information Commissioner's Office ("**ICO**"), the Competition and Markets Authority ("**CMA**"), the Office of Communications ("**Ofcom**"), and the Financial Conduct Authority ("**FCA**"), to deliver a coherent approach to digital regulation for the benefit of people and businesses online. For more information, please see here.

[7] To support a streamlined and cohesive approach to the regulation of digital platforms, the Australian communications and Media Authority ("**ACMA**"), the Australian Competition and Consumer Commission ("**ACCC**"), the Office of the Australian Information Commissioner ("**OAIC**"), and the Office of the eSafety Commissioner

cooperation to address challenges specific to digital and online services. For example, the DRCF work plan for 2023-2024 involves promoting competition and data protection, focusing on online advertising markets, online choice architecture practices, and potential regulatory remedies. Finally, these initiatives also demonstrate an effective way of engaging with the impacted industry stakeholder in a more cooperative and outcomes-based co-regulatory model.

c. Privacy and security justifications preserve individual rights

CIPL notes that the digital economy requires a regulatory approach that accounts for all interests related to data, ranging from competition, innovation, public and online safety, cybersecurity, to consumer and data protection, among others. As we highlighted in our comments on the Interim Assessment of Competition within the Mobile Ecosystem, for a balanced approach, it is important not to assume that one regulatory area should systemically have priority over the other, or that a competition risk analysis should prevail over a data protection risk analysis or vice-versa.

In that regard, CIPL supports the DMCH's acknowledgement that certain conduct of platform operators is taken for the sake of ensuring privacy and security measures; therefore, they can be permissible and justifiable.[8] In line with the co-regulatory framework approach, organizations could perform contextual risk assessment and other compliance measures, including privacy and security, that are demonstrable to the DMCH and other relevant regulators on request. Thus, if there is a concern that privacy and security measures are taken without substantial justification, regulatory and enforcement authorities may be able to determine whether the measures are excessive or appropriate based on agreed and clear criteria that have been developed in collaboration with the industry. However, the DMCH and relevant agencies should embrace privacy and security innovation in light of the increasing risk of privacy-infringing incidents and cyberattacks. While there can be privacy benefits in competitive markets, privacy and security innovations that preserve individual rights are separate and distinct from competition goals. Applying antitrust principles in a privacy domain can undermine individual rights and dilute competition market goals. Therefore, privacy and security justifications should not be only limited to compliance with the relevant legal requirements, e.g., Personal Information Protection Act; instead, organizations should have the opportunity to provide advanced privacy and security measures beyond legal requirements and differentiate themselves in the market based on the robustness of their privacy and security measures.

---

together form the Digital Platform Regulators Forum. The initiative aims to share information between independent regulators about, and collaborate on, cross-cutting issues and activities where the regulation of digital platforms, including competition, consumer protection, privacy, online safety and data issues, intersect. For more information, please see here.

[8] Section I. 3.1. of the DMCH's Final Report. Please note that the Final Report on Competition within the Mobile Ecosystem is structured under two main headings, i.e., Section I refers to General Remarks whereas Section II refers to Specifics.

d. Competition leads to better consumer privacy protection and choices

Today, privacy is more than a compliance concern – it's a key opportunity for differentiation between businesses. As described in the Cisco 2022 Consumer Privacy Survey, 76% of consumers indicated they would not buy from an organization they did not trust with their data, and 81% agreed that the way an organization handles their data is indicative of how it views and respects its customers.[9] Similarly, our report on "Business Benefits of Investing in Data Privacy Management Programs" published jointly with Cisco found that, while organizations historically have been driven by compliance and risk avoidance when investing in privacy programs, there is increasing recognition that a privacy program provides multiple benefits and return on investment beyond traditional legal compliance, such as business enablement, sustainable business, brand reputation, competitive edge, and customer and consumer trust.[10]

Therefore, while regulations require organizations to establish certain levels of privacy and security safeguards for its consumers, organizations have an opportunity to differentiate themselves from competitors to grow their base-line privacy and security measures, particularly with the advent of new technologies that make data privacy a differentiating factor. Indeed, CIPL notes that robust data protection and consumer choices are precursors to a competitive consumer privacy market. Such competition and differentiation for better privacy protection for individuals should be available for any organization regardless of sector and size. Thus, the DMCH should not only consider privacy and security as potential justifications for conduct that might otherwise be considered anti-competitive, but also recognize industry's and consumers' growing demands for better privacy and security for end-users. Any regulation should promote, rather than impede, these efforts.

In addition, CIPL notes that the Final Report predominantly focuses on market players without placing sufficient emphasis on the consumer lens. In that regard, other interested authorities, such as PPC, METI, and courts could be in a better position to explore the demand side, i.e., consumer preferences to have better privacy and security protections.

e. The EU DMA model has a particular objective that is not applicable to Japan's mobile ecosystem

CIPL encourages the DMCH to clearly articulate its regulatory expectations and objectives and evaluate whether the currently existing competition regime can address its expectations and goals, or if there is a need for new regulations. For instance, as we highlighted in our latest paper, "Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences,"[11] the EU DMA was introduced for a particular reason: to achieve harmonization of competition and avoid fragmented, inconsistent rules within the EU's internal market where each nation has its own competition regulator

[9] Cisco 2022 Consumer Privacy Survey, available here.
[10] CIPL/Cisco Joint Report on Business Benefits of Investing in Data Privacy Management Programs, available here.
[11] CIPL paper, "Limiting Legal Basis for Data Processing Under the DMA: Considerations on Scope and Practical Consequences," May 30, 2023.

and independent judiciaries.[12] On the other hand, enforcement mechanisms in other jurisdictions, such as in the United Kingdom,[13] South Korea,[14] Australia,[15] and United States[16] consider their existing enforcement regimes to be capable of considering, on a case-by-case basis, whether gatekeepers are acting anti-competitively.

Therefore, the DMCH could achieve the same regulatory objective without introducing a blanket prescriptive restriction, but instead through pursuing individual and case-by-case analyses of specific anti-competitive behaviors in the market. As we identified earlier, ex-ante regulations make regulators assume facts about future markets they oversee in an attempt to predict what they would look like with or without intervention. The Japanese market subject to such assumptions and predictions is substantively different than the EU market. Japan's global and regional partnerships are also substantively different. In the Asia Pacific region, the focus is on convergence rather than harmonization, as well as to prevent fragmentation within multi-party, multi-country systems. Regulatory convergence considers the disparate characteristics of regulatory frameworks across nations and respects the different values and priorities of the particular cultures that are enshrined in each jurisdiction's legal systems. Inherent in the idea of convergence is the notion that the process of convergence is dynamic and flexible, i.e., adaptable, for example, to changes in technologies, market dynamics, public expectations etc. Yet, Japan would lose such flexibility and future-proof regulatory approach by imposing strict ex-ante regulations. Therefore, Japan should avoid rigid ex-

[12] CIPL looked at the legal basis on which the European lawmakers relied for the Digital Markets Act, i.e., Article 114 of the Treaty on the Functioning of the European Union. In particular, Article 114 TFEU empowers legislators to adopt measures that are designed to approximate national rules and prevent regulatory fragmentation in the internal market, also known as the harmonization clause. According to the DMA Impact Assessment Report and its Explanatory Memorandum, Article 114 TFEU is considered the relevant legal basis due to (i) the intrinsic cross-border nature of the services provided by gatekeepers and (ii) the risk of further fragmentation regarding the functioning of the Single Market for digital services.

[13] The proposed UK Digital Markets, Competition and Consumers Bill provides the UK Competition and Markets Authority a broad discretion (i) to determine whether an organization has "strategic market status" in relation to a give digital activity, and (ii) to design and implement targeted pro-competitive interventions, for instance to enforce interoperability or data portability. With respect to enforcement, the CMA is expected to implement an incremental approach that focuses on light-touch and informal engagement, progressing to formal enforcement only if necessary.

[14] In early 2023, the South Korean Fair Trade Commission published guidance on the abuse of dominance in the digital economy amid growing competition concerns around platforms that have blocked market entry and strengthen their power.

[15] The Australian Competition and Consumer Commission enforces the existing legislation governing competition in digital markets under the Competition and Consumer Act 2010 (Cth) and has conducted three inquiries in relation to digital platforms over the past six years: DPI (Digital Platforms Inquiry), DPSI (Digital Platform Services Inquiry), and AdTech inquiry.

[16] Similar bills such as the Open App Markets Act (OAMA) and American Innovation and Choice Online Act (AICOA) have been debated in the US but have not become law and are unlikely to receive broad support. Diverse individuals and organizations including industry groups, experts, and think tanks point out concerns as they will impact issues such as national security, user security, privacy, and economic competitiveness of the US.

ante regulations that may have the unintended consequence of outlawing legitimate pro-competitive conduct to the detriment of Japanese consumers.

2. Specific Comments

a. Mandatory use of payment and billing systems (Section II. 2.1 of the Final Report)

- **Competition Concern:** Mandatory use of payment and billing systems will hinder the entry of businesses that provide alternative payment and billing methods, hinder developers from providing diverse rate plans and services, and reduce innovation. Users are deprived of choices and cannot receive a variety of services.
- **The DMCH's Direction:** Business operators that provide app stores of a certain size or larger shall be prohibited from obliging developers who use the app stores to use their own payment and billing systems. They shall be required to apply fair, reasonable, and non-discriminatory usage conditions, including fees, for app store business users.

CIPL supports the DMCH's initiative to encourage industry to compete on payment and billing services, providing users more freedom to choose from alternative services. However, the DMCH must ensure that offering alternatives does not compromise privacy or security safeguards nor create confusion on the side of the users. Typically, users would expect to use a payment or billing solution as privacy-friendly and secure as the one provided by the app stores. In particular, in the absence of a well-established framework, malicious actors may attempt to mislead users confronted with multiple services with different levels of organizational practices and different levels of privacy and security protections to refund or customer support policies. Furthermore, allowing alternative payment or billing systems requires app stores to share certain transactional information and other personal data about individuals with alternative service providers. This can result in wider proliferation of personal data and can also increase the risk of data exploitation by malicious actors, especially in the absence of a secure regulatory framework for data sharing.

Regulated organizations should be able to evaluate in advance the privacy and security 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.

Finally, 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 complying with the DMCH's direction.

b. Establishing a competitive environment between reliable app stores (Section II. 2.3. of the Final Report)

- **Competition Concern:** Restrictions on alternative distribution channels for apps have created various competitive issues: (i) loss of opportunities for companies to enter the app store business, (ii) no competitive pressure on app stores fees, and (iii) app reviews that are not always transparent and fair, hindering innovation and user choices.
- **The DMCH's Direction:** Businesses that provide operating systems of a certain size or larger shall allow effective use of alternative distribution channels for apps while also ensuring security and privacy.

CIPL believes that optimizing individual choice and improving market access are important policy priorities, but they should not occur at the expense of privacy and security. Indeed, consumers' concerns over privacy and security should always outweigh the choice of alternative distribution channels for apps. Rather than rushing into fixes to consumer choice and market access, we believe that decision-makers should carry out a broader and deeper analysis of the competing equities involved in this practice. CIPL would like to reiterate the following consideration (previously highlighted in our comments on the Interim Report) that should be taken into account by the DMCH:

- How to operationalize a balancing or cost-benefit assessment of competing equities – including privacy and security – in a way that provides the necessary legal certainty for both app store owners and app developers;
- 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;
- What other laws might be implicated in the event of a data privacy and security infringement (e.g., consumer protection) and how DMCH would work with other competent authorities to consider the potential exposure of operating systems, app stores, and device manufacturers to liability under such laws in the event of infringements due to sideloading;
- Whether there are less risky alternatives to sideloading that could more effectively address consumer choice and competition issues;
- The potential long-term impacts of sideloading on the entire digital ecosystem and consumers, both positive and negative.

We also want to draw the DMCH's attention to the latest regulatory development in the EU DMA's enactment process. Specifically, while the DMA's proposal imposes an obligation on gatekeepers to enable the installation and effective use of third-party applications from alternative distribution channels, the provision in the final text is now subject to countervailing interests, i.e., gatekeepers are not prevented from taking measures to ensure the integrity of hardware or operating systems or to effectively protect end-users' security.[17]

[17] Article 6(4) of the DMA. The final text of the DMA can be found here.

In addition, CIPL supports the DMCH's consideration of adopting a code of practice or guidelines for app stores that will bring legal clarity to the industry and market players. In that regard, CIPL encourages the DMCH to further explore the code of practices that was referenced in the Final Report, i.e., "Secure Coding Guidebook" created by the Japan Smartphone Security Association and "Code of Practice for App Store Operators and App Developers" published by the UK Department for Science, Innovation and Technology (**"DSIT"**). The DMCH should carefully consider disclosure and transparency requirements when developing such a code of practices and keep in mind that not only app developers but also cybercriminals may gain access to data. The UK DSIT, for instance, requires app store operators to provide a publicly accessible summary of security checks performed for apps and updates.[18]

Finally, the DMCH will scrutinize the proportionality and necessity of operating systems when providers take measures to ensure security and privacy. However, this proportionality requirement needs further consideration. Since security risks are increasing, and technology is becoming sophisticated, what "proportionate" could mean is a critical matter of discussion. Generally speaking, regulated organizations must be able to aim for as high a security and privacy protection as possible. The DMCH has to bear in mind that legal compliance with privacy regulations is the minimum required but never sufficient in this fast-changing digital space. In addition, the DMCH (and other interested regulators) need to retain the necessary expert staff with technical knowledge regarding privacy and security as well as dedicate sufficient resources to this work.

c. Pre-installation and default settings (Section II. 4.1. of the Final Report)

- **Competition Concern:** Users tend to use default services due to status quo bias; therefore, default-setting services have competitive advantages, hindering users' autonomous decision-making and choice opportunities. Automatically installing their own apps without clearly showing users' choice to install the apps puts third parties at a competitive disadvantage, hindering users' autonomous decision-making and choice opportunities.
- **The DMCH's Direction:** Businesses that provide operating systems of a certain size or larger shall (i) allow and technically enable users to easily change default settings on their operating systems or browser; (ii) display a selection screen for browser, search engine, and voice assistant to which operating system directs or steers users by default; and (iii) allow and technically enable users to easily uninstall pre-installed apps. However, in certain cases, restrictions on uninstallation should be allowed.

CIPL notes that the DMCH's direction follows an approach similar to that followed by the EU's DMA.[19] Importantly, the DMA allows restriction on uninstallation in relation to software applications that are essential for the functioning of the operating system or of the device which cannot technically be offered on a standalone basis by third parties. Indeed, certain features, such as camera, messaging, and mail apps, are integral parts of the operating systems; therefore, CIPL supports the DMCH direction that provides

[18] Paragraph 1.3. of the UK Department for Science, Innovation and Technology Code of Practice for App Store Operators and App Developers, December 9, 2022, available here.
[19] Article 6(3) of the DMA.

flexibility for operating services to impose restrictions on uninstallation if a feature constitutes a core function of the operating system, particularly in the context of privacy- and security-friendly features.

CIPL encourages the DMCH to revisit its direction that requires operating services to display a selection screen for browsers, search engines, and voice assistants so that users choose whether or not to install from the list of alternative services. Displaying a screen of choice may promote competition, but it may also lead individuals to make uninformed decisions when they are confronted with multiple alternatives. This, in turn, will impact effective privacy and security protections and significantly dilute the value of a choice mechanism. Therefore, the DMCH's direction for a selection screen should be used with caution and only for very specific purposes and where absolutely necessary.

d. Self-preferencing (Section II. 4.2. of the Final Report)

- **Competition Concern:** When searching by query, the search results from various in-house services (maps, videos, finance, flights etc.) are displayed at the top or its vicinity of the organic search frames, making it possible for users to transition to those services at the expense of alternative market players.
- **The DMCH's Direction:** Businesses that provide search engines of a certain size or larger should not give their services any advantage over similar third-party services in displaying search rankings.

While considering the regulation of self-preferencing and search results displays in general, the DMCH should carefully examine potential privacy and security risks that it would entail. It is particularly important to actively consider the potential harms and unintended consequences of any such prohibitions given that no substantive evidence of harm has been provided by the DMCH on this topic in the Final Report. In order to perform many functions, general search engine operators would need to exchange certain types of data with alternative third-party services such as those providing maps, flights, videos, etc. There are hundreds of examples of such third-party service providers, many of which are foreign and include state-affiliated entities in countries that may not have the same focus on human rights, privacy, and security. The types of shared data would, at least, include information about users making the queries and potentially their location data, depending on their preferences. This is not a risk-free activity because the shared data may be processed by organizations that do not comply with privacy rules, or may be subject to excessive government access to data for national security and intelligence purposes in some countries, or not subject to recently adopted OECD Principles for Trusted Government Access to Data.[20] Thus, the DMCH's direction should acknowledge search engine operators' justification grounds if they are concerned that alternative service providers do not have sufficient privacy and security safeguards in place.

[20] OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, Adopted on December 13, 2022, available here.

e. Ensuring data portability by end-users (Section II. 5.3. of the Final Report)

- **Competition Concern:** To facilitate switching and promote competition between operating systems, the current state of data portability is lacking in simplicity and sufficiency.
- **The DMCH's Direction:** Businesses that provide operating systems, app stores, and browsers of a certain size or larger shall provide end users and third parties authorized by users, at their request and free of charge, with tools to facilitate exercise of data portability and continuous and real-time access to data, for enabling effective portability of data generated through the activity of end users.

CIPL's research and experience show that the availability of a standard technical framework and clarity on the respective obligations and liabilities of the sharing and receiving entities are pre-conditions for effective data portability. In the absence of a secure technical framework enabling data portability, it must be left to organizations to put in place a framework that can achieve continuous and real-time access to data without increasing the risk of data being compromised by malicious actors. Furthermore, organizations should have clear guidance from authorities to ensure that data recipients are authorized entities; otherwise organizations' compliance with a data portability obligation may create a violation under applicable data protection rules. Finally, once the data has been securely transmitted to the correct recipient, the responsibility of the regulated entity should shift to the recipient, who must process the received data in compliance with data protection rules and bear all the attached liabilities.

f. Social login (Section II. 5.4. of the Final Report)

- **Competition Concern:** By mandatorily requiring app developers to display app stores' social login option, this conduct allows app stores to use their positions and give preferential treatment to their own services.
- **The DMCH's Direction:** Businesses that provide app stores of a certain size or larger shall not require developers using the application stores to use, to offer, or to interoperate with their identification services.

CIPL believes that the DMCH's direction should provide users with a true list of options to choose from by taking into account considerations, such as convenience, privacy, or security. In doing so, users will have the freedom to choose whether or not to use the app store's ancillary services or those provided by alternative services. Otherwise, individuals would be confronted with limited options that may not necessarily fit with their expectations, including privacy and security expectations. CIPL also wants to highlight that the policy direction should be made not only based on the questionnaire survey to developers consumers, but also should be surveyed to determine the right balance.