ASIA
INTERNET
COALITION

8 April 2019

To
Mr Tan Kiat How
Commissioner
Personal Data Protection Commission
10 Pasir Panjang Road,
#03-01 Mapletree Business City, Singapore 117438

Subject: Industry Submission and Recommendations on the Discussion Paper on Data Portability

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the Personal Data Protection Commission (PDPC) and the Competition and Consumer Commission of Singapore (CCCS) for the opportunity to submit comments on the Discussion Paper on Data Portability. AIC is an industry association comprised of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. Our current members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Oath), and Booking.com.

We commend the government's efforts on developing the Discussion Paper, with an aim to discuss the impact and benefits of a data portability requirement for business innovation, market competition and consumers. The issue of data portability and data flows is at a unique crossroad between data protection and competition regulations and should not be considered in isolation. Both perspectives should be taken into consideration when implementing a data portability requirement and determining the optimal approach to reaping maximum benefits from such a requirement while keeping costs manageable.

Such efforts and dialogue are critical, particularly at a time when cross-border trade and data security has taken a center stage in a new global development. As responsible stakeholders in the developmental progress, we appreciate the ability to participate in this discussion and the opportunity to provide input into the policy-making process. As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request PDPC and CCCS to consider, which could be a useful feedback for future consultations to determine an optimal approach to implementing a data portability requirement that will reap maximum benefits from data portability.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Importantly, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions and help shape the dialogue around effective data portability framework in Singapore.

Sincerely,

Paine

Jeff Paine
Managing Director

Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

1. What is data portability?

a. The PDPC's discussion paper defines data portability as: "allow[ing] individuals to obtain and re-use their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability" (citing the UK's ICO).

b. Fundamental to the above definition is the scope of data to be covered by a data portability requirement. The PDPC's discussion paper rightfully emphasizes the need for clarity in determining what types of data will be subject to a portability requirement. Clarity will be essential to enable businesses, regardless of size and expertise, to appropriately develop portability mechanisms.

- The PDPC suggests that a portability requirement will be "most beneficial" if its scope "extends beyond classical personal data – i.e. information about an individual, including data generated from his activity – to data that is provided by him, for example, emails, photographs and documents."

c. In addition, it is essential to clarify: (1) whether such data portability will be imposed as a mandatory regulatory requirement; (2) if yes, which sectors/organizations it will apply to; and (3) how it will need to be implemented – what will be the mechanisms/processes chosen by PCPC to ensure such data portability.

While in principle we support data portability and acknowledge the benefits it brings to consumers and businesses (covered in more detail below), we believe the Discussion Paper does not provide sufficient details to carry out a thorough assessment of actual benefits vs. the costs of implementation of such data portability requirement. As such, we recommend that PDPC:

i. Analyses and clarifies the objectives it is trying to achieve with this requirement and, in particular, the concerns it is trying to address (is there a market failure from competition law perspectives? Or consumer protection angle?);

ii. Whether such concerns can be addressed without introduction of mandatory data portability requirements:

- by working with the industry and developing industry best practices, voluntary regional or international standards and code of conducts;
- allowing the industry to use commercially negotiated terms and conditions offering customers tools and methods to move their data; easy contract termination provisions and pay as you go pricing – which would help addressing any potential "lock-in" concerns;

iii. We believe that mandated data portability, tied to a specific process or standard may threaten innovation and contractual freedom, which in turn may adversely impact market development and harm consumers. Hence, we believe a thorough assessment is necessary before any such requirements are introduced.

Furthermore, we would like to provide a few specific comments around data portability assessed in the Discussion Paper. In general, we support data portability that covers personal data as well as information that individuals directly provided to a service. However, for reasons discussed below (in *Challenges*), we do not support portability (whether mandatory or not) requirements that extend beyond data provided by the individual, such as "observed" or "inferred" data, which could include some types of data generated from the individual's activity.

2. Benefits of data portability

a. As noted in the discussion paper, data portability does indeed provide a number of potential benefits to consumers and businesses. Portability can:

- Enable user control over their personal data and autonomy in their activities in digitally-enhanced sectors.
- Promote competition in digitally-enabled services through reduced switching costs.
- Enhance innovation and support economic growth by improving access to data within and across sectors.

b. The PDPC's discussion paper thoroughly covers the variety of potential positive impacts from data portability, if done properly. Suffice it to say that we look forward to working with the PDPC to find the best methods helping to unlock these benefits and address concerns mentioned in Section 1 above through close industry cooperation.

3. Challenges of data portability

For all its benefits, it is important to recognize that data portability can present challenges, including in the following contexts:

a. Data Protection

Data portability requirements with broad scopes can implicate the privacy interests of individuals other than the one making a request. This is particularly true in the social networking space. The degree of portability of information that relates to the "social graph" can raise particular privacy concerns.

- A user's "social graph" is the intricate map of the connections between the information they provide to a service, their interactions with other users on that service, and their interactions with the service itself. It could include information that is shared with or belongs to friends or third parties (including photos, group memberships, contact information, event participation, and more).
- Data portability tools that allow users to migrate their complete social graph or portions that relate to the information or activities of their connections could adversely implicate the privacy interests of other users whose social graphs overlap and interconnect.

Data portability requirements must account for the risk posed by bad actors who might seek to obtain individuals' information through deceptive or unfair practices. There should also be protections in place for organizations when they respond to requests: it should be established that the request to port data can only be triggered by the data owner and organizations should not be required to conduct investigations into the legitimacy of the request.

As the PDPC's paper rightly highlights, individuals must have information concerning the track record, reputation and data management and protection practices of the data recipient to ensure that their personal data is not being received by entities that might misuse it.

b. Data security

Data portability can pose a number of cybersecurity challenges, *even if implemented correctly*.

- Specifically, portability tools can increase attack surface by enlarging the number of sources for attackers to siphon user data; further, if the mechanism by which data is ported (typically an API) is not implemented securely, unauthorized parties could use it to access data under the guise of portability requests.

- It is axiomatic (https://cyber.harvard.edu/interop/pdfs/interop-breaking-barriers.pdf) in system design that the risk of inadvertent disclosure or data leakage through vulnerabilities increases when there are more ways to access data.

- Making independently designed systems interoperable at scale (https://stratechery.com/2018/open-closed-and-privacy/) means that there are more ways to access data — and not just for the intended parties. Further, the greater the volume of data and variation in its original source, the greater the privacy and security risks to users and services.

- The greater the scope of data covered, the greater the risk to users — especially if social graph data is included.

c. Intellectual property

- If a data portability requirement is scoped too broadly, it could cover information that implicates the IP or business interests of a compliant organization. For example, inferred or observed data (even generated from individuals or their activity) could include proprietary information that is used to provide or improve services. Requiring companies to make such information available for portability may thus compromise their intellectual property rights, because of its proprietary nature.

- Increasing the scope of portable data to cover observed, inferred, or proprietary information could also expose analytic information containing valuable insights generated by a service — insights that could eventually lead to innovative new features or more efficient operation. Inadvertent or intentional access to these insights could allow some companies to duplicate the features of others, reducing the incentive of companies to innovate.

d. Proportionality

- As with many other regulations, data portability requirements might be more burdensome for smaller service providers than for larger providers. Smaller providers may have less capacity to efficiently process portability requests, and less ability to implement portability mechanisms securely. Thus, any portability requirement must take into consideration the varying capacities among organizations and provide for reasonable exceptions (discussed below).

4. Getting data portability right

a. We encourage the PDPC to consider flexible data portability rules that enable individuals to port the data they provide to a service in a structured, machine-readable format either through a downloadable or, where technically feasible, machine-to-machine mechanism.

b. To realize the variety of pro-consumer, competition, and innovation benefits of data portability, data portability rules must be designed and implemented in a manner that are privacy-protective and incentivize covered organizations to develop innovative means of enabling portability.

The PDPC discussion paper identified a number of means through which the above goals might be achieved. The same are listed below with further comments:

- ***Standards***

  - Standardized means of transferring data between services are essential for scalable, secure forms of data portability. Industry-developed standards can help ensure transfers are privacy-protective and secure, enable implementation regardless of organizational size and expertise, and reduce compliance costs. However, mandated standards would risk locking-in innovation and development of new standards. Hence, we believe PDPC should encourage development of voluntary, market driven, international or regional best practices rather than mandatory standards.

  - The discussion paper rightly notes that “there are no internationally defined or developed standards to address data portability.”

  The PDPC could however, consider further the work of the Data Transfer Project (DTP) in developing such best practices guidelines.

  Google, Facebook, Microsoft, and Twitter have partnered on the Data Transfer Project to develop best practices and industry standards around such direct data portability solutions. DTP is an open source initiative dedicated to developing technical tools that will enable consumers to securely port their data directly from one service to another, without needing to download and re-upload it. Also refer to: https://datatransferproject.dev/.

- ***Accreditation***

  One means of addressing concerns over data security and privacy in the context of data portability requests could be a system of accreditation or certification, potentially against a code of conduct developed by industry in consultation with relevant stakeholders.

- Individuals will need information about the nature and recipients of data transfers and assurances that their information will remain protected and secure to feel confident in making data portability requests.

  As the PDPC notes, "information extends beyond the nature of the new product or service that they are acquiring or transparency over how their data will be utilized by the data recipient. Equally pertinent is information concerning the track record, reputation and data management and protection practices of the data recipient."

- Data portability rules should encourage industry and government to partner to develop mechanisms to ensure individuals are informed about potential data recipients, to guard against bad actors who might have subpar data protection practices or seek to obtain personal data under false pretenses. As mentioned above, we do not support accreditation as a mandate to be applied across the board to all organizations.

c. Portability rules should also account and provide for:

- ***Exceptions***

  Data portability requirements should provide exceptions so that organizations are not compelled to take actions that: 1) are technically infeasible; 2) compromise the privacy or security of personal information for other individuals; 3) disclose trade secrets or proprietary information; 4) interfere with law enforcement, judicial proceedings, investigations, or efforts to guard against, detect, or investigate malicious, unlawful, or fraudulent activity or enforce contracts; or 5) violate laws or the rights and freedoms of other individuals.

- ***Limitations on liability***

  - While, we are encouraged by the PDPC paper's discussion of liability: "There should also be clarity on the limits of liability for the data recipient. The porting organization cannot be expected to vet all data recipients, so it should be exempted against any claims for damage from any misuse of data by data recipients. The same goes for data breaches suffered by individuals if the data is under their own care. The porting organization should also not be held liable against any claims relating to the accuracy and quality of the ported data unless it was demonstrated that the data was corrupted while under the care of the organization."

  - Portability requirements should limit liability for those organizations that port data pursuant to a user request in a manner that is appropriately privacy-protective and secure. This limitation on liability could be contingent on a requirement for reasonable vetting and oversight of data recipients, consistent with the spirit and purpose of data portability.

- ***Scalability***

  - Portability requirements should be scalable, rather than target organizations based on size. Individuals may well wish to port the data they provide from smaller services to larger services, or from smaller services to other small services. A portability requirement that leaves out services below a certain size would limit the value of portability for users.

  - Instead, a better formulation is one that is scalable to smaller companies and encourages them to take advantage of industry standards.

- ***Ongoing work***

  - Any new data portability requirement should account for and encourage the work already being done in industry, such as the Data Transfer Project described above.

End of Submission