AIC's Response to the
Proposed Consumer Data Protection Regime for Singapore

ABOUT THE ASIA INTERNET COALITION

The Asia Internet Coalition ("**AIC**") is an industry association founded by eBay, Google, Nokia, Skype and Yahoo! incorporated in Hong Kong. One of the objects of the AIC is to support and promote public policy and regulatory frameworks that facilitate the development of national digital industry markets in the Asia Pacific region.

The AIC welcomes the opportunity to comment on the questions posed and issues laid out in the Consultation Paper on the Proposed Consumer Data Protection Regime for Singapore (the "Consultation Paper"). For convenience, we addressed the questions raised in the Consultation Paper in the order they were presented:

Questions in relation to objectives and principles of proposed DP Framework:

Question 1: Do you have any views/comments on the impact of the proposed DP law on specific sectors? Do you have any suggestions on measures to mitigate this or any other anticipated impact?

Question 2: With reference to paragraph 3.8, do you have any views/comments on the concurrent application of the DP law with existing sectoral regulations?

By way of a general comment to the proposed DP Framework, we express our support for the twin objectives of the proposed DP Framework as stated in section 3.1(a) and (b). The achievement of both of these public objectives underlies the international instruments upon which most data protection regimes in the world are based.[1] Notably, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("OECD Guidelines"), the EU Data Protection Directive, and the APEC Privacy Framework expressly affirm the importance of maintaining information flows to sustain social and economic growth while protecting privacy.

We would also point out that both objectives are equally important and are not necessarily conflicting, as suggested by the statement in section 1.2 that "… a

[1] OECD /APEC/ EU - explain how these instruments recognize the free flow of information as critical to businesses

DP regime that seeks to create a *balance* between the need to protect individuals' personal data against an organization's need to obtain and process such data for legitimate and reasonable purposes."

In addition, we are heartened by MICA's acknowledgement of the need for balance between trends in Europe and US towards stricter, but often impractical, regulation with the need to keep business costs manageable. We also appreciate that strengthening Singapore's overall economic competitiveness and enhancing its status as a trusted hub for global data management is given equal priority status to ensuring appropriate safeguards for consumer data, and the recognition that, to achieve a positive economic impact, any legislation should facilitate data flow rather than impede it.

For the internet industry, key players have a track record of innovating to empower users to protect their own privacy. Very often, such features provide consumers with better protection than what consumers get in the off-line environment.

With the foregoing observations, we believe the adoption of a general baseline law to ensure a minimum standard of data protection, accompanying the existing sector-specific legislation is a positive step towards engendering consumer trust while providing flexibility.

There is a potential adverse impact upon internet intermediaries or online platforms such as access providers, search engines, hosting platforms, email providers, payment processors and social networks, to the extent that the same may be subject to third-party, secondary or indirect liability. These internet intermediaries play a vital role on the internet as powerful enablers of economic growth, innovation, creativity and expression. In the US alone, OECD data showed that internet intermediaries represented at least 1.4% of the total GDO value-added in 2008.

These benefits, however, will be at risk without safe harbors that protect internet intermediaries from liability for third-parties' actions. This is not a new idea. For example, telephone companies are not legally responsible for illegal activity discussed or planned over phone lines, and they do not have the legal responsibility to ensure that callers are not doing something illegal. Safe harbors have been recognized as foundational to the internet's success: the EU's eCommerce Directive and the US Communications Decency Act Section 30, and the Digital Millenium Copyright Act, all provide for safe harbors that provide limitations on liability of intermediaries for copyright infringement. We note that Singapore has already provided for safe harbours for intermediaries via Section 26 of the Electronic Transactions Act 2010, and it would be useful to ensure that the proposed DP law provides clarity that internet intermediaries are exempted from potential liability. The inclusion of a provision providing for a safe harbor that provides similar protection for internet intermediaries from DP law breaches by users will acknowledge the critical role of internet intermediaries to provide a platform for competition and innovation, and will furthermore strengthen Singapore's position as a trusted global hub for data.

Questions in relation to the definition of "personal data":

Question 3: Do you have any views/comments on the proposed definition of personal data outlined in paragraphs 3.9 to 3.11?

Question 4: With reference to paragraphs 3.15 to 3.16, do you have any views/comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views/comments on the proposed approach to the protection of the personal data of the deceased?

The Consultation Paper proposes that personal data be defined as follows:

"Personal Data" means information about an identified or identifiable individual; where "individual" means a natural person, whether living or deceased."

We agree with MICA's view that what constitutes personal data is context-specific and with continuous technological developments, would render efforts to populate a definitive list of personal data types unfeasible.

We note that the proposed definition of personal data is based upon that used in the OECD Guidelines[2]. Although a good starting point, the explanation provided in the Consultation Paper,[3] which adverts to the context-specific nature of information, gives an indication of the need to update the definition. Depending upon how it is implemented, defining personal data to broadly cover all information about an "identifiable individual" may disregard its context-specific nature and simply cover all information, regardless of whether the data controller can reasonably link the same with an individual.

We believe that personal data should be defined pragmatically, based upon the likelihood of identification. While it is helpful to have the DPC later publish guidelines giving examples of information that may constitute personal data, we propose to define personal data simply as "information that can be [certainly linked to an identified or identifiable individual". With that wording, context is taken into account, and considers information as personal data only when the data controller can certainly link the same to an individual. Accordingly, even though technology may exist that will allow someone to link the information to an individual, if the data controller is not in a position to certainly identify an individual using reasonable means, the information will not constitute "personal data".

[2] § 3.10
[3] § 3.12

It is important to note that uniqueness should *not* be associated with identifiability, as many companies employ de-identification techniques or assign random unique identifiers to data for the purpose of privacy protection. The data is still unique and research can be conducted that leads to innovative products and services, but it is not as likely to lead to a natural person.

- Other information stored with "personal data" should be treated as "personal data" *only* as long as that link is maintained. This also gives companies incentives to de-identify data.

- On the other hand, data that is neither associated with, combined with nor stored with any data that personally identifies a natural person, and is not itself individually indentifiable to a real person should not be considered personal data. Examples may include a unique number or de-identified number that cannot reasonably be associated with an individual.

- FINALLY, Information that has been anonymized should also not be considered personal data.

The distinction in 3.12 that "other types of information may be considered personal data only in specific contexts" fits nicely with the construct described above. Indeed, the acknowledgement that "what constitutes personal data is context specific" is in line with whether the data element identifies an individual, or simply could if combined with other personal elements. We strongly support this element being explicitly included in the definition suggested above.

We support the inclusion of all forms of personal data, both electronic and non-electronic as mentioned in section 3.13. Data collected and used for the same purposes should be treated equally.

The AIC suggests the proposed DP law should not cover deceased individuals. Certain rights (such as the rights of access and correction (mentioned in sections 3.68 to 3.73) are so intimately tied to the data subject that should only be exercised by the data subject itself. Moreover, it is entirely possible that a deceased person may not desire family members to access or see private information in the event of their demise. While we understand the potential privacy implications for family members, the underlying data should be, in practice protected even from family members, unless an individual has taken independent steps to ensure a family member can obtain access in an emergency.

Questions in relation to the organisations and activities covered by the DP law:

Question 5: Do you have any views/comments on the proposed organizations covered by the DP law?

Question 6: With reference to paragraphs 3.20 to 3.22, do you have any views/comments as to whether the DP law should extend to organizations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore? Do you have any suggestions as to how this DP law could be implemented if it should apply to such organizations?

We agree with the approach of applying a "light touch" baseline legislation that applies to all private sector organizations to ensure a minimum standard of DP across the private sector. We likewise agree with the pragmatic approach that limits the coverage of Singapore's DP law to all data collection and processing by organizations in Singapore, and not beyond its borders. Questions of governmental jurisdiction are often fact specific, but as a rule, consumers choose which legal entities they want to interact with, and their choices should be respected in that case by observing the facts surrounding the terms of service agreed to by that consumer. Therefore, jurisdiction should not necessarily nor automatically follow the user's location.

Given the pervasiveness of the Internet (which is global in nature), we echo MICA's view that there would be practical difficulties in enforcing the DP provisions on organizations located outside Singapore. Where consumers had agreed to a provider's terms of service (which may be subject to the laws of another jurisdiction), their personal data would already be subject to protection under the prevailing DP laws of that jurisdiction, if any.

Questions in relation to the general exclusions from the DP law:

Question 7. Do you have any views/comments on the proposed general exclusions from the DP law?

Question 8: With reference to paragraph 3.26, do you have any views/comments as to whether there should be exclusions for artistic and literary purposes under the DP Act? How should these exclusions be defined if exclusions for artistic and literary purposes should be provided for?

Question 9: Are there any other exclusions that should be catered for under the DP Act?

AIC does not have objections with the exclusions suggested in 3.24 – 3.27 and in particular, the exclusion for news activities, news archives and other editorial content With regard to the proposed data protection regime for Singapore, the AIC suggests broadening the definition of "news organization" as meaning any organization that engages in any news activity. There is often a public interest in personal information associated with public figures that is essential for quality news reporting. It is also reasonable to exclude business contact information as described in this section.

Also, the AIC suggests the DP consider exclusions for intermediaries hosting, caching, or acting as "mere conduits" of information posted online by users (also known as user generated content). With the advent of search engines, social media, social tagging, and user generated profiles with settings to make the data public or semi-public, the AIC suggests protections for this data be commensurate with the user's intent in posting the information. In other words, if the user is choosing to make the information public, the hosting, caching or conduit entity which is merely providing the publishing platform should not be liable for disclosure of the data.

Otherwise, as a general rule, exclusions should be minimized when the effect is to detract from global harmonization of DP rules.

Questions in relation to the general exclusions from the DP law:

Question 10: Do you have any views/comments on the proposed general rules under the DP law?

Question 11: With reference to paragraph 3.35, do you have any views/comments as to whether individuals should be deemed to have given consent for organizations to collect, use or disclose their personal data if they are notified and given reasonable time to opt out but do not?

Subject to the aforementioned qualification on the liability of intermediary service providers, we have no objection to the rule that an organization is responsible for personal data under its custody or control, including personal data that is not in the organization's custody but is under its control. The requirement of consent for collection, use or disclosure of personal data is well established.

However, although it may be reasonable to require that "an organization may not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure or personal data *beyond what is necessary* to provide the product or service,[4] it should be understood that this limitation should not preclude the possibility of improvements to the same products or services, which ideally will not trigger a separate consent requirement. It is important to note that the previous goal of enhancing innovation and the growth of commerce could be at odds with such an objective noted in 3.31. It is increasingly clear that using the data for research

[4] §3.31

and development for enhanced services, features, or entirely new products can be very much in the consumer interest. One consideration is to interject the concept that the use must be of current or expected overall value to the consumer, or provide a value that does not have a countervailing negative consequence for the user. This approach allows more experimentation for existing companies to innovate on behalf of their users.

We agree with MICA that the type of consent given could vary depending on the specific context of the collection, so there is no need to prescribe in detail the manner in which consent may be given in the DP Act. Consent obtained may be explicit or implied, depending on the circumstances.[5]

Regarding the possibility of adopting an "opt-out" approach, as adopted in jurisdictions such as British Columbia, suffice it to state that the same would not necessary result in a lower level of privacy protection or otherwise constitute an unreasonable burden upon consumers, particularly when privacy principles are faithfully implemented within a robust privacy program.

We support measures to provide individuals with control of personal data, such as the option to withdraw consent described in § 3.36. Many Internet players offer a variety of opt-out elements to their products and services. We consider opt-out to be an appropriate mechanism for cookie based ad networks or similar technologies because of how it fits in with a user's experience. User choices should be durable and revocable.

Questions in relation to the proposed rules on collection, use and disclosure of personal data:

Question 12: Do you have any views/comments on the proposed rules on collection, use and disclosure of personal data?

Question 13: Do you have any views/comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organizations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organization? Are there any other exceptions that should be provided?

Question 14: Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined at paragraphs 3.60 to 3.61?

For § 3.41, it might be more practical to disclose business contact information of a [customer care] team, as alternatives to an "officer" or "employee", this is especially important for businesses with millions of users.

[5] § 3.32

We also feel that § 3.44 should be expanded to include prospective employees and candidates of organizations.

The AIC would also like to take this opportunity to point out instances where internet businesses may need to collect or use data without consent here. There are several instances where data collection is necessary in the normal course of business for website operations. For example, to understand site traffic, improve site design, fraud detection, security defense, billing, determining which parts of a website are or are not being used, rendering a page in a format appropriate to the device and in the appropriate language, retrieving content data and delivering advertising that advertisers have paid us to deliver or comply with auditing requirements.

In § 3.49, it is mentioned that "the use or processing of such personal data by organizations must be reasonable and fulfill only the purposes for which the individual's consent was obtained", and that "unless consent is not required by the DP Act, fresh consent has to be obtained if the personal data collected is to be used for a different purpose other than the purposes for which the individual has been given consent." In this regard, the need for a fresh consent must not cover cases where the processing is for related purposes, particularly when necessary to enable improvement of products and services originally subject of the processing.

In line with the observation in § 3.38, we support the inclusion of an *accountability principle* that, beyond the appointment of one or more individuals responsible for ensuring compliance with the DP Act, will ensure that there will be internal mechanisms in place for demonstrating such compliance. The accountability principle should also require that organizations be transparent with their users regarding the collection, use and process of the collected personal data.

The AIC agrees Singapore should adopt a flexible approach to allow cross border data flows where similar principles have been adopted or are agreed to, such as the principles articulated in the OECD and APEC forums.

Questions in relation to the proposed rules on accuracy, protection and retention of personal data:

Question 14A: Do you have any views/comments on the proposed requirements for the accuracy, protection and retention of personal data outlines at paragraphs 3.6.2 to 3.6.7?

Question 15: With reference to paragraph 3.6.7, do you have any views/comments as to whether organizations should be required to specify the retention period when collecting personal data?

The data quality principle as described in § 3.63 and the security safeguards principle described in § 3.64 are long-standing DP principles which we fully support. As stated in § 3.65, appropriate security safeguards differ based on

sensitivity of data, nature of data and other factors and requires flexibility in choice, rather than a prescriptive or one-size-fits-all approach.

With respect to proposed notice of retention period at the point of collection, we agree with the observation that the appropriate retention period may differ according to context, and it may not be practicable for organizations to determine and specify a suitable retention period upfront.

Questions in relation to the proposed rules on access to and correction of personal data:

Question 16: Do you have any views/comments on the proposed rule on access to and correction of personal data?

We agree with the proposed approach especially that raised in para 3.73.

Specifically for the internet industry, correction/deletion of information proactively declared and submitted by the user about the user (such as data provided to open an email account, for instance) can occur within a reasonable period of time unless needed for anti-fraud purposes.

Selective deletion will not be possible in some circumstances (e.g., a user will be able to change his/her postal code but will not be able to leave this field blank)

Social networking profiles can be deleted within a reasonable period of time. Postings controlled by a web host may be deleted or anonymized, but posts controlled by others cannot be reasonably altered.

Questions in relation to the proposed penalty and enforcement regime:

Question 17: Do you have any views/comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?

Question 18: Do you have any views/comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views/comments on the criteria for breaches that would warrant financial penalties?

We believe that DP protections should be designed to prevent harm to individuals from wrongful collection or misuse of their personal information. Remedies to privacy infringements should be proportional to the likelihood and severity of the risk of harm.

The imposition of financial penalties by the DPC, by itself, is not objectionable but it must at all times be guided by proportionality and the “preventing harm”

principle[6]. There is further a danger that the amount of penalties collected by the DPC will later be viewed as a measure of the agency's performance, which may skew it towards needless or excessive imposition of penalties.

We note that according to § 4.6, "… the law will enable individuals to seek redress via civil proceedings in court". In our opinion, such a move would be a disproportionate response to any privacy concerns documented to date and would chill innovative and beneficial uses of data on widely-used websites. If a private right of action were the law of the land and a privacy violation were alleged, the sheer number of users on leading websites could result in hundreds or thousands of lawsuits. This threat could seriously discourage experimentation with data for beneficial features and functionality for consumers because one misstep could literally raise litigation costs to a point that threatens a business' viability.

We note also that according to § 4.9, where sectoral legislation exists, concurrent action under the DP law and the sectoral law is possible. This may allow overlapping actions and possibly conflicting decisions. Furthermore, this may result in the imposition of penalties by two regulators, resulting in an aggregate penalty that will no longer be proportional to the severity of the offense.

In addition, the AIC suggests that the DP regime would require the DPC or Appeals Board to give reasonably detailed grounds for decisions made, as well as to develop straightforward appeal processes.

Questions in relation to transitional arrangements:

Question 19: Do you have any suggestions on specific guidelines that the DPC should provide to help organizations achieve compliance with the DP law?

Joint industry initiatives to raise public awareness and consumer education on how they can protect their privacy would also contribute to achieving the aims of the DP law. This would support the proposed approach for a complaints-based rather than audit-based enforcement mechanism.

Considering the ongoing discussions on the proper definition of "personal data" it is appropriate for the DPC to continue to address this in guidelines. In particular, ***if not addressed in the DP law itself,*** the guidelines could consider a third category of data that is neither personal data nor data that is wholly anonymous – indirectly identifiable data. One model is the Austrian Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000) ("Austrian Law"), which considers data "only indirectly personal" for a controller, a processor or recipient of a transmission when "the Data relate to the subject in such a manner that the controller, processor or recipient of a

[6] APEC Privacy Framework, P. 14

transmission cannot establish the identity of the data subject by legal means". In other words, the identity of the individual can be retraced but not by legal means. Frequently, this class of data is used on an aggregate basis where the controller is not seeking to establish the identities of individuals. As the legal obligations should be proportional to the objective of the DP law, controllers should be subject to a different set of obligations corresponding to indirectly identifiable data. In this manner, data protection rules would not inhibit or unduly frustrate the advances that can be made through harnessing the power of aggregate data analysis.

The guidelines could also address process in relation to the adoption of appropriate security measures, recognizing the possibility of self-regulatory initiatives in lieu of a prescriptive approach.

Questions in relation to transitional arrangements:

Question 20: With reference to paragraphs 4.11 to 4.14, do you have any views/comments as to whether a one to two year "sunrise" period would be appropriate?

Question 21: With reference to paragraphs 4.15 to 4.19, do you have any views/comments on the proposed treatment of existing personal data?

Question 22: Are there certain organizations that may require different transitional arrangements.

A one year "sunrise" period should be sufficient, provided that the DP law raises no fundamental issues that would need to be addressed in regulations and/or guidelines, in which case additional time may be desirable.

The proposal in respect of existing personal data, whereby consent is deemed to have been given while requiring fresh consent for use of the same data for a new or different purpose, achieves a good balance between ensuring meaningful compliance with DP requirements and practical considerations.

Questions in relation to proposed National Do-Not-Call registry:

Question 23: Do you have any views/comments as to whether a National Do_Not-Call registry should be set up in Singapore?

The AIC has no objections to a DNC registry being set up. We note that the DNC should not include emails since emails already come under the jurisdiction of the Spam Control Act.

CONCLUSION

Thank you again for the opportunity to provide comments. We hope that our above comments are useful to you in your preparation of the bill.

Please do not hesitate to contact the AIC at director@asiainternetcoalition.org should you require further information on the contents of this submission.

Yours sincerely,

Dr. John Ure
Executive Director
Asia Internet Coalition