PUBLIC CONSULTATION ON PROPOSED REGULATIONS ON THE

PERSONAL DATA PROTECTION ACT 2012 IN SINGAPORE

- A RESPONSE FROM THE ASIA INTERNET COALITION

19 MAR 2013

The Asia Internet Coalition (AIC) is an industry association with a membership of eBay, Facebook, Google, Skype and Yahoo! Inc. As its mission, the AIC seeks to promote the understanding of Internet policy issues in the Asia-Pacific Region.

Nominated contact person
Prof. John Ure
Executive Director of the Asia Internet Coalition
director@asiainternetcoalition.org

Comments on the Proposed Regulations on Personal Data Protection in Singapore

We thank the Personal Data Protection Commission (the Commission) for the opportunity to comment on the proposed regulations under the Personal Data Protection Act (PDPA), and after a thorough review, would request the changes and clarifications discussed herein.

SUMMARY OF MAJOR POINTS

1. General

1.1 – *Data shared with a service provider (Data Processor) represents a "use" and not a "disclosure," and thus should be subject to separate requirements under the PDPA.*

2. Access Requests

2.1 – *Information previously provided, publicly available or readily accessible need not be included in a Subject Access Request (SAR);*

2.2 – *Where personal information has been "disclosed," the obligation to send corrected data should be optional.*

3. International Transfers

3.1 – *We encourage the Commission to recognise existing accountability models to facilitate international data transfers.*

4. Proxies for Data Subjects

4.1 – *There should be a single person responsible for personal data, and the Commission should require family members or heirs to obtain a court order so that entities are able to recognise the individual charged with that responsibility.*

We provide our reasoning below.

COMMENTS

1 GENERAL Comments

In order to provide context for our discussion, we must first clarify the term "disclosure."

1.1. Data shared with a service provider (Data Processor) represents a "use" and not a "disclosure," and thus should be subject to separate requirements under the PDPA.

The proposed regulations should distinguish between a "disclosure" of personal data, in which the data moves from one Data Controller to another, and the original Data Controller no longer makes decisions about the data, and a "use" of personal data by a service provider, in which an entity retains its role as a Data Controller but enables another entity (a "Data Processor") to process the data consistent with the Data Controller's policies.

Maintaining this distinction is important not only to promoting meaningful transparency for individuals whose data is transferred to a new Data Controller, but also to reducing unnecessary burdens for smaller entities that collect personal data. Specifically, while a large company might handle certain back-end processing tasks – such as operating a web server or maintaining a database system – internally, smaller companies typically contract out these tasks. Treating service provider relationships like these as "disclosures" would add burdens for smaller entities and lead to consumer disclosures that are not meaningful.

Data Disclosure

Companies that handle personal data sometimes share data with other entities, a process known as "disclosure." Where a company shares information with a third party who will determine its own purposes of use for personal information, the third party is acting as a Data Controller. Given that the company who has shared the information will lose control over the purpose of use on shared data, such sharing should be considered a "disclosure" and not a "use".

Data Use

In contrast, companies may share information with service providers (Data Processors) – entities that perform tasks on behalf of, and under the instruction of, that company (Data Controller). Where data is shared with such Data Processors, it is done under agreements that contractually bind the Data Processor to process data only as permitted and instructed by the Data Controller. The Data Processor makes no decisions related to the purpose of use for personal information. In such circumstances, the sharing of data should be considered a "use" and not a "disclosure."

This distinction is supported by privacy laws in other countries, such as Canada[1]. We ask the Commission to recognise this distinction and fine-tune classifications in the Regulations to clarify the obligations around "disclosures" – sharing with a third party for that third party's own purposes – separately from "uses." This distinction is necessary so that organisations are not unnecessarily burdened with requirements that do not accurately reflect their roles in the data collection, use and disclosure process. Regulation is thus applied in a proportionate manner.

Accordingly, the PDPA should have separate requirements for dealing with sharing/transfers that would be classified as a "use" versus sharing/transfers that would be classified as a "disclosure."

2 Comments on ADMINISTRATION OF REQUESTS FOR ACCESS TO AND CORRECTION OF PERSONAL DATA

In response to the Commission's Question: "Do you have any views / comments on the proposed manner in which an individual may make an access or correction request or the proposed positions relating to how organisations are to respond to such requests?" we observe:

2.1. Information previously provided, publicly available or readily accessible need not be included in a Subject Access Request (SAR).

For example, with respect to Section 21(1)(b), information about the ways personal information is used or disclosed are already provided to individuals in a Privacy Notice, per the Notification Obligation under Section 20 of the PDPA. Consequently, to require such information be again included in a Subject Access Request (SAR) is redundant. The inclusion of such information would increase the costs of responding to a request, and potentially contribute to delays in responses, benefiting neither the individual nor the entity. Similarly, personal data that is publicly available or readily accessible to the user – such as by viewing his or her account information through an automated tool -- should not be required to be included in a SAR response.

Consequently, we would seek clarification on the necessity of duplicating information in a SAR, and permit entities to respond to SARs in ways that can reduce costs for individuals and entities alike (e.g.: provide references to previously provided account information/agreements; etc.).

2.2. Where personal information has been "disclosed," the obligation to send corrected data should be optional.

Section 22(2)(b) requires an entity to "send the corrected personal data to every other organisation to which the personal data was disclosed." As we described in Section 1.1, the scope of this requirement should be limited to sharing with a third party for that third party's own purposes – a "disclosure." Even with that limitation, to 'waterfall' corrections to such third parties potentially puts the privacy of the individual at risk, and could well be contrary to the wishes of an individual. For example, an individual may

[1] "Transfer" is a use by the organisation. It is not to be confused with a disclosure. When an organisation transfers personal information for processing, it can only be used for the purposes for which the information was originally collected. http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_e.asp

wish to maintain a relationship with the original entity, and provide his updated/corrected contact information (phone, email, etc.) for such purposes. However, this same individual may not necessarily wish to maintain a relationship with the third parties to whom his data was disclosed. Indeed, in addition to creating a compliance burden on the entity, requiring a continued flow of updated data relating to an individual would in many cases be contrary to the intentions of the individual. Specifically, if an individual authorised information about himself to be sent to a third party on one occasion, it could undermine his privacy expectations for subsequent updates to his personal data to be communicated to any third party that received it in the past. A more rational approach would be to understand that, if this individual desired further contact with such third parties, he could contact those entities himself. In protecting the privacy of individuals, access should only be granted to individuals who can be authenticated to prevent the accidental sharing of personal data with third parties.

Furthermore, where personal information has been "disclosed," to a third party, the data is no longer in the control of the original entity, so there is no mechanism to enforce compliance by a third party. The best the original entity can do is inform a third party of the change – again which the individual may not desire.

Thus we request that the correction requirements apply only to a company and its service providers, where said company can exercise a measure of control over the data operations necessary to perform the corrections. Accordingly, informing third parties to whom personal information has been "disclosed," should be optional.

3 Comments on TRANSFER OF PERSONAL DATA OUTSIDE SINGAPORE

In response to the Commission's Questions:

- Question 1: "Do you have any views / comments on other means of ensuring the protection of personal data transferred out of Singapore?"
- Question 2: "Do you have any views / comments on the proposed requirements for contractual clauses and binding corporate rules to protect personal data transferred out of Singapore?"

we observe:

3.1 We encourage the Commission to recognise existing accountability models to facilitate international data transfers

We appreciate the Commission's recognition of the complexities involved in cross-border data flows and the allowance of flexible mechanisms for facilitating international data transfers. Interoperability with existing privacy regulatory mechanisms is critical to ensuring that businesses and individuals in Singapore can avail themselves of the resources of the global economy, while also promoting the privacy goals embodied in the PDPA. In this respect there remains a lack of clarity whether the PDPA would apply to foreign entities who may offshore data to Singapore for processing and how, if so, the PDPA could be enforced extraterritorially.

In relation to binding corporate rules, we would like to highlight that it would be difficult to apply the requirements stated in Section 7.12 (in particular sections 7.12(a) and 7.12(b) to companies which operate in a multi-tenanted cloud based environment. In such situations, companies would be storing the personal data collected in the "cloud", where it would be onerous to pinpoint the location of a piece of personal data at any one point in time to the level of specificity that the Commission requires. We request the Commission to consider not imposing such specific requirements, which may have the unintended effect of hindering the development of cloud technologies, but rather focus on the principles data protection in administering the PDPA.

Building on flexible mechanisms, we would encourage the Commission to direct obligations on the entity engaging in the processing through an 'accountability' style programme that is contemplated in both OECD and Canadian frameworks. The Commission should also take into consideration the Asia Pacific Economic Cooperation ("APEC") Cross Border Privacy Rules system (CBPR). We would encourage the Commission to recognise that cross border transfers of data between companies that have been self-certified before an accredited accountability agents under the APEC CBPR will be deemed compliant with PDPA as well. Another possible option would be for Commission to specifically allow or implement US-EU Safe Harbour type processes in relation to the transfer of data outside of Singapore.

Accountable organisations have programmes in place to protect the privacy of information no matter where (or to what jurisdiction) that data flows, and stand ready to demonstrate and account to regulators what those protections are, and how they are put into practice within the entity. An accountability-based privacy regime provides a flexible balance between the law and individual organisations responsibility for determining how best to meet those standards in practice. This approach is one of the leading and most promising tracks to enhance the goal of interoperability (mutual respect) between privacy regimes in different regions and is a major feature of emerging modern legal frameworks on privacy.

Further, the significant investments entities are asked to make to give meaning to this principle should be recognised and incentivised. Building comprehensive privacy programmes, assigning dedicated personnel to look after privacy matters, and creating documentation around these programmes is characteristic of an organisation seeking to comply with the law. As such, we recommend the Commission consider incentivising good practice in this area by introducing compensatory benefits for entities enacting such programmes. Other jurisdictions have considered such incentives in the form of either a statutory presumption of compliance with the law (*see, eg.* Art.38 of the Draft Colombian Privacy Regulation: Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales) or a reduction in penalties for those with programmes in place (as in Spain: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal).

4 Comments on INDIVIDUALS WHO MAY ACT FOR OTHERS UNDER THE PDPA

In response to the Commission's Questions:

- Question 1, "Do you have any views / comments on the areas for which individuals may act for other individuals under the PDPA that should be prescribed?"
- Question 2: "Do you have any views / comments on the extent to which minors should be able to exercise rights and powers conferred on them under the PDPA?"

- Question 3: "In particular, do you have any views on the minimum age below which individuals should not exercise their own rights and powers under the PDPA?"
- Question 4: "Do you have any views / comments on the proposed priority list in relation to individuals that may act for deceased individuals?"
- Question 5: "In particular, do you have any views on the appropriate priority list and/or whether priority should be given equally to all relatives (or to relatives within certain categories such as spouse and children, parents and siblings, etc) for the purposes of the PDPA?"

we observe:

4.1 There should be a single person responsible for personal data, and the Commission should require family members or heirs to obtain a court order so that entities are able to recognise the individual charged with that responsibility.

With respect to assuming control of data of the deceased, where no such personal representative has been specified in the deceased's will, the Commission should require family members or heirs to obtain a court order to access the personal data protected under the PDPA. To do otherwise invites conflict. For example, suppose there is a familial conflict over care of the deceased's estate. One family member may abuse his position to obtain information against the will of another family member entrusted with care. How should an entity respond to such competing, or contradictory requests? In complying with the errant request, has a company unwittingly made an unauthorised disclosure and violated the PDPA?

Accordingly, in the absence of a will, rather than introducing a priority list of nearest relatives to a deceased individual only an order from a Judge should be valid to allow another individual to act as an individual's data representative. Alternatively, the Commission could establish processes to protect entities acting in good faith that have received conflicting data processing requests.

With respect to minors, assigning control based on "understands the nature of right" is too arbitrary. Either the parent or the minor should be in control – not both. To do otherwise invites conflict. For example, suppose a parent puts a minor's phone number on the DNC list, but the minor has opted into marketing communications. Whose 'consent' will control in such a situation? If a message is sent to that minor, has a company unwittingly violated the PDPA? In addition to creating confusion, this conflict could in fact undermine the privacy interests of the minor, if for example it allowed the parent of a 17-year-old to gain access to or direct handling of the personal data of the 17-year-old.

Accordingly, a specific age threshold of 13 years should be established to indicate when a minor becomes responsible for the control of his own personal information. This minimum age would be consistent with data protection frameworks that protect the personal data of children around the world and with the data protection practices of many global companies which collect, use and disclose personal data of individuals under the age of 18 as part of their business models. Alternatively, the Commission should establish processes to protect entities acting in good faith who have received conflicting data processing requests. In general, the Commission should also take care that its regulations would not inadvertently prevent those below the minimum age from accessing the Internet nor should the regulations impose overly onerous age verification requirements on online intermediaries/platforms.

CONCLUSION

AIC expresses thanks for the willingness of the Commission to listen to views and comments from stakeholders.

We suggest that the recognition of the distinction between data "disclosures" and "uses" – and hence Data Controllers and Processors – be classified in order to improve and make more specific the clarification of data record management requirements for individual entities of different natures.

In regards to access rights; since information about the ways personal information is used or disclosed are already provided to individuals in a Privacy Notice (*Section 21(1)(b)*), we seek clarification on the necessity of duplicating information in a SAR. This also applies to personal data that is publicly available or readily accessible to the user as we propose that including such information would lead to an increase in cost and potential delays, benefitting neither the individual nor the entity. Additionally, we suggest that the scope of the requirement for entities to send corrected personal data to relevant organisations as per Section 22(2)(b), be classified as optional and should only apply to a company and its service providers of which they hold a measure of data control. We feel that 'waterfall' corrections to third parties could potentially put the privacy of the individual at risk, and could well be contrary to the wishes of an individual.

For the international transfer of personal data, we encourage the Commission to recognise an 'accountability' style framework whereby the entity engaging in the processing should have programmes in place to protect the privacy of information regardless of jurisdiction destination. To complement the framework, we recommend incentives to compensate entities for their investments made to build and adhere to good practice. At the same time, we request that the Commission also recognises and reconsiders the potential impact on the development of cloud technologies that may subsist due to binding corporate rules on organisations which operate in a multi-tenanted cloud based environment, namely Section 7.12.

Referring to proxies for data subjects; we suggest that court orders for access to a deceased individuals' personal data protected under the PDPA be required in the case that no appointed representative is specified. With respect to minors, our view is that only one party – either minor or parent – be in control, and that a specific age threshold of 13 years be established to determine when control should be made a responsibility of the individual. Finally, we encourage the Commission to bear in mind and set up processes for the protection of entities acting in good faith who have violated the PDPA due to conflicting data processing requests.

We respectfully request that the Proposed Regulations be reevaluated in light of the comments presented here and we thank you again for taking the time to engage industry. If requested, we would very much like to meet in person so that we can discuss these issues in greater detail.

In the meantime, should you have any further queries please do not hesitate to contact director@asiainternetcoalition.org for any further information on the contents of this submission.