ASIA PACIFIC CARRIERS' COALITION
(Incorporated in the Republic of Singapore)

Singapore PDPC Public Consultation on Approaches to Managing Personal Data in the Digital Economy

By The
Asia Pacific Carriers' Coalition

3 October 2017

Asia Pacific Carriers' Coalition
c/o Rajah & Tann Singapore LLP
9 Battery Road #25-01
Singapore 049910
T: +65 6535 3600
F: +65 6225 0747
Email: secretary@asiapacificcarriers.org

TABLE OF CONTENTS

A. STATEMENT OF INTEREST

The Asia Pacific Carriers' Coalition is grateful for the opportunity to provide input to the Personal Data Protection Commission's consultation on possible reforms to the Personal Data Protection Act of 2012.

The Asia Pacific Carriers' Coalition is an industry association of global and regional telecommunications carriers operating in the Asia Pacific region, formed to work with governments, National Regulatory Authorities and users, to advocate open market policies and best practice regulatory frameworks to promote competition and efficient investment in telecommunications markets.

B. COMMENTS

Members of the Asia Pacific Carriers' Coalition (APCC) only provide services to the enterprise customer and are fully committed to protecting the privacy and security of their enterprise customers' personal data. We recognize that establishing a trusted environment for consumers across the digital ecosystem is crucial to the success of the market.

The APCC supports the consistent, flexible approach of the Personal Data Protection Act of 2012 (PDPA or "the Act") and its schedules, as this framework balances robust protections for the privacy of individuals with the possibility to use data in ways that benefit society. APCC members recognize that valuable insights can be gained from data when responsible companies use proper safeguards. Our companies have strong policies and procedures in place governing the responsible collection and use of personal data.

Comments of the APCC which respond to the specific topics of consultation appear below.

1) Notification of Purpose as a basis for processing data

The Personal Data Protection Commission (PDPC) indicates that consent is currently the primary basis for the processing of personal data in the PDPA, and that it may be necessary to create a separate basis for processing data in circumstances in which it is difficult to obtain the consent of individuals whose data is collected. The APCC supports this approach. Such challenges for a consent regime may be present in the context of Smart Cities, the use of unmanned aerial vehicles (drones), or in retail centers that employ WiFi hotspots, for example.

In these situations, it is good practice to provide individuals with the capacity to opt out of data collection or to contact the organization collecting the data, where feasible. The Act might clarify that organizations should offer individuals a persistent mechanism to opt out of certain uses and disclosures of their data to the greatest extent possible.

The PDPC's proposal to place conditions on the collection and use of data through "Notification of Purpose" is appropriate. The PDPC proposes that this method be used when collection or use is not expected to have an adverse impact on individuals.

In discussing the concept of "Notification of Purpose" the PDPC proposes a risk and impact assessment is to be undertaken. We agree with this in principal and recommend that such an assessment should be phased to firstly consider if there is a risk, and if so, secondly complete an assessment. If the requirement is absolute, i.e. an impact assessment is required in all cases, even where there is no risk, this poses companies with an administrative burden to ensure compliance with the market's position as compared to other markets where they operate. This could breed a risk whereby compliance becomes an administrative form filling process, moving the focus away from practically and operationally having and enforcing suitably high standards of protection. Where there is deemed to be risk, an assessment should follow and we

suggest that this includes an evaluation of the benefit to the public or the organization in using the data, taking into account any potential negative impacts on individuals or risks involved.

Therefore a 'notification of purpose' approach as proposed is pragmatic and reasonable where it is not possible to obtain consent and there is no risk to the individual. This approach is also reflected in the European Union Privacy Regime. To that end we believe that the Act could also incorporate some of the safeguards adopted by the European Union in GDPR) for further processing of data, by allowing for collection and use of personal data without consent where pseudonymisation is employed or where the organization adheres to a code of conduct that establishes an industry good practice.

2) Legal or Business Purpose

The APCC welcomes a reform to the PDPA which would allow for the collection, use or disclosure of personal data without consent where it is necessary for a legal or business purpose. While the Second, Third, and Fourth Schedules to the Act provide for a variety of purposes for which data may be collected, used, and disclosed without consent, certain legitimate purposes are not clearly included in the schedules. Some scenarios that can be highlighted as legitimate without consent cases include: maintaining the security of communications networks, sharing information among organizations and with authorities to prevent and respond to cybersecurity threats, and improving an organization's products and services. Some of these purposes may be achieved by using de-identified data; some require the use of pseudonymised or personal data. It would be helpful for the PDPC to provide indicative guidance as to the types of legal or business purposes that do not require consent.

The PDPC's proposal that collection, use and disclosure of personal information for a legal or business purpose take place when it is not desirable or appropriate to obtain consent and when the benefits outweigh the risk of harm to individuals is also appropriate. The PDPC might recognize pseudonymisation or other methods to safeguard the privacy of individuals as good practices that reduce the risk to individuals and render a certain collection or use of data as legitimate by the data controller / "data intermediary" (in the sense of the EU data processor).

The PDPC might also recognize that certain types of marketing of a company's products and services, such as first-party marketing, can be legitimate purposes for using personal data absent the prior consent of the individual. Providing individuals with a chance to opt out of this use of their data achieves a proper balance between the interests of the individual and the business, as the GDPR recognizes.

3) Proposed data breach notification framework

The APCC supports the codification of a data breach notification framework in Singapore. We offer comments on the PDPC's specific proposals, as well as additional considerations to take into account when drafting such a framework.

(a) Risk of impact or harm to affected individuals

APCC supports the inclusion of a harm trigger as a precursor to the requirement to notify. APCC suggest that the appropriate precursor to notifying the regulator may be suitably different to the precursor to notifying affected individuals, whereby the harm trigger in the latter should be identified as a higher risk of harm than the former. Here too we believe that the EU GPDR constitutes good practice in this area, requiring notification to the regulator where a personal data breach is *"likely to result in a risk to the rights and freedoms of natural persons*" (Articles 33-34). There may be breaches of personal data that pose a very low risk of harm to individuals – including, for example, improper access to personal data by employees of

an organization – and the notification of these types of harm would cause unnecessary alarm for individuals and may result in notice fatigue.

Another sample to consider: "Where data is sent in error to the wrong recipient via email, this is immediately identified and the recipient promptly deletes the data, there is no misuse of the data and no harm whatsoever".

In order to further the goals of providing appropriate notice and creating clear and predictable rules for business organizations, the PDPC should include the following elements in the definition of a breach of personal data:

- A clear delineation of the personal data that is subject to breach notification requirements. This generally consists of an individual's name or other clear identifier in combination with information whose acquisition creates the risk that identity theft or other fraud will occur (e.g. financial account number, national identification number, home address). Were the PDPC to use the Act's current definition of "personal data," an organization might have to notify individuals of the breach of information that merely reveals the existence of a customer relationship with the organization.

- Clarification that the requirement to notify applies when there is a precursor of risk, or high risk, due to personal data being acquired, disclosed, lost, or destroyed.

- An exception to notification requirements for the good faith acquisition of data by the employee of an organization.

The APCC submits the following definition of a personal data breach for the PDPC's consideration:

> *"Personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of unencrypted and unredacted personal data transmitted, stored or otherwise processed, which causes or the organization reasonably believes has caused or will cause identity theft or other fraud to any individual.*
>
> *Good faith acquisition of personal information by an employee or agent of an organization for the purposes of the organization is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the organization or subject to further unauthorized disclosure.*

(b) Significant scale of breach

The APCC respectfully submit for your consideration that the level of risk could be the legal test that determines whether notification is required, with the scale of the breach being one of a number of criteria taken into account when determining said level of risk.

The APCC considers it good practice to take scale into account when quantifying the impact on individuals, however finds that the proposal to notify the PDPC and individuals where 500 or more individuals are affected to be inappropriate in and of itself.

If the position set out in the proposal proceeds to legal effect, further clarity is required regarding the connection between the risk of harm threshold and the scale of the breach. Should they be applied independently or together? If applied together how would it work in practice? Would there be a "lead criteria"? The potential for 499 records to be breached that may cause a risk of harm to the data subjects and there to be no requirement to report the breach sounds dangerous.

In coming to this position, we acknowledge the complexity of data security and that a breach could occur in many ways and at many levels, with vary levels of risk and potential impact; thus defining a number that triggers notification is problematic and once defined it could place too much emphasis on a singular measure, which in isolation could have the effect of being arbitrary.

With the market's place in a digital ecosystem of increasingly global interactions the recommended approach can allow focus of resource in areas where protection could be strengthened, or in the event of a breach it can be dealt with more efficiently.

There is a concern held that notifications in absence of an assessment of risk can be administratively burdensome on the time of the PDPC and those companies doing the notifying, and our joint resources are best utilized to increase protection and accountability where risk exists. This is particularly true for companies with global operations where the approach in the market has to be treated as an exception to globally defined standards, processes and policies; and in the context of increasing speed of technological development.

(c) Concurrent application with other laws and security breach notification rules

The APCC welcomes the proposal of PDPC to permit companies to fulfil their duties under any new data breach notification framework by complying with existing, sector-specific requirements. This reduces the cost of compliance so that the organization may focus on investigating the cause of any breaches and implementing robust security measures. Indeed companies should not be subjected unnecessarily to cumulative or inconsistent burdens. For the sake of efficiency and proportionality, market providers should not have to abide by different requirements depending on the services they provide.

We would like to clarify in case the conditions will run concurrent with existing sectorial breach reporting obligations but that they won't necessarily mirror them, this is similar to the breach reporting obligation under GDPR/E-Privacy.

(d) Obligations of the data intermediary

The APCC considers that separate requirements for a "data intermediary" or party who manages personal data for another organization are generally unnecessary, as the organization that is ultimately responsible for the personal data will generally impose such requirements on its affiliates through contractual provisions. As is the case with the GDPR approach the Data controller would want to know if a "Data Intermediary" or "Data Processor" had suffered a breach of their data. If there is no clear reporting requirement, then the Data controller & Data intermediary (or data processor) will be put under an onerous task of checking the contract terms to ascertain if there had been bound to a breach reporting obligation. That will no longer be necessary if there is a specific requirement under the law. This will also streamline processes around the Globe.

(e) Exclusions and exemptions from breach notification

The APCC suggests that the duty to provide notification of a data breach apply generally to parties who are in a position to detect, prevent, and remedy such a breach. Thus, the exemption of a public agency, an organization acting on behalf of a public agency, or other types of organizations from this requirement would appear contrary to the goals of securing personal data and allowing others to take the necessary steps to protect themselves from harm if the data has been accessed improperly.

(f) Provisions surrounding notification

The APCC supports the proposal to delay notification to individuals if a law enforcement agency determines that such notice will impede a criminal or civil investigation or national security. The framework might specify that notice be made after the law enforcement agency determines that notification will no longer impede the investigation or jeopardize national security.

(g) Encryption of data

The APCC advises the PDPC to incentivize the use of encryption for personal data in any breach notification framework. This may be done in the definition of a breach of personal data, by establishing that unauthorized acquisition of data that has security measures in place, an example of which would be data that has been encrypted does not constitute a breach unless the decryption key has also been obtained. Alternatively, the framework may provide that breach notification is not required if the data acquired has been encrypted and the decryption key has not been obtained. This ensures against over-notification of individuals and authorities, which may lead to notice fatigue, and it encourages organizations to implement good security practices.

(h) Time frame for notification

The investigation and information-gathering that an organization must undertake in the event of a breach in order to assess the type of data that has been accessed and the risk of harm to individuals is complex, and it may require considerable time and resources. The immediate priority should be to investigate a breach and take appropriate action to limit loss or damage. Short notification requirements may lead to a misappropriation of resources that are better devoted to thoroughly investigating a suspected breach and remedying it to prevent further harm. It can also be counterproductive to provide hasty notice to authorities and individuals, particularly if an organization determines that no breach has occurred and must then notify these parties a second time. The APCC therefore questions whether or not it can provide any meaningful information within 72 hours and therefore proposes to notify PDPC as soon as is practicable, the same standard as to be applied with its customers.

The APCC also considers important that any timeframe for notification begin after the *determination* that a breach has occurred. This furthers the goal of providing quick and accurate information about an actual breach and its impact.

(i) Method of notification

The APCC supports a flexible approach for providing notice of a breach to both the PDPC and affected individuals where a direct relationship with the individual exists/data controller. Particularly where individual customers are concerned, an organization should be permitted to contact them via the method through which transactions are normally carried out (e.g. through electronic mail, via a prominent notice on the organization's Web site, through post, or a combination of these).

When providing services to large multinational retail customers or wholesale customers, business providers are typically at least one step removed from the individual using the "end service". Enterprise service providers do not have the capability to identify those end-users, who are either the employees of our enterprise customers or the end-users of our wholesale customers. The entity with the ability to identify the individual(s) who may be affected by a data breach is therefore not the upstream business provider providing network access but the retail provider that has the billing relationship with the end user/individual. Against this background, enterprise service providers obligations should be limited to

notifying their "downstream customer" (subscriber) and not the individual. And this logic also applies to the notification/reporting obligation that applies to data controller and not the data intermediary.

C. CONCLUDING REMARKS

Thank you for the opportunity to provide input to the Personal Data Protection Commission. Should you require additional information, or if we may be of assistance during this process, please do not hesitate to contact the APCC.