Faculty of Arts & Social Sciences
National University of Singapore
Blk AS6, #03-41
11 Computing Drive
Singapore 117416

19 Sep 2017

Personal Data Protection Commission
460 Alexandra Road
#10-02 PSA Building
Singapore 119963
corporate@pdpc.gov.sg

Dear Sir/Madam,

Re: NM4203 Response to the Public Consultation for Approaches to Managing Personal Data in the Digital Economy

We thank the Personal Data Privacy Commission (PDPC) for this opportunity to participate in the policymaking process of Singapore with this open consultation on the Approaches to Managing Personal Data in the Digital Economy.

We thank the Personal Data Privacy Commission (PDPC) for this opportunity to participate in the policymaking process of Singapore with this open consultation on the Approaches to Managing Personal Data in the Digital Economy.

As current students of InfoComm Policy (NM4203) in the Communications and New Media (CNM) department of the National University of Singapore (NUS), we examined the approaches proposed towards personal data as put forth by the PDPC as part of our class study. As such, we make the following observations and recommendations on the review of the Personal Data Protection Act (PDPA):

- **Question 1: Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?**

We agree that the PDPA should provide for Notification of Purpose as a basis for the collection, use, and disclosure of personal data without consent. We make the observation that the Notification of Purpose is often (1) not noticeable e.g. poorly-lit and hidden signages in public areas, or (2) written in legal language/language which is not accessible to the layperson/only in one language (English). We recommend that the Notification of Purpose should be made explicit to the individual, and should be highlighted in plain language rather than legal language, and where possible should be highlighted in our national languages.

- **Question 2: Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?**

We agree that the proposed Notification of Purpose approach be taken, and be subject to the proposed conditions, such as situations where it is impractical or practically impossible for an organisation to obtain consent, AND where it is not expected to have any adverse impact on the individual. We recommend that there be circumstances where Notification of Purpose be excluded, such as in times of national crisis (e.g. declaration of war), medical emergencies (e.g. SARS or similar outbreaks) or natural disasters (e.g. earthquake, tsunami etc).

- **Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?**

We agree that legal interests of an organisation should be regarded as a basis for collecting, using and disclosing personal data without consent and notification. If the personal data collected could serve as incriminating evidence, consent and notification should not be deemed necessary. In fact, we note that

the act of obtaining consent or giving prior notification might hinder investigative processes (e.g. embezzlement investigations)

However, we would strongly recommend that the collection of personal data on the basis of business purposes should require **notification** as well as the party's **consent**. Generally, the collection of personal data for marketing purposes does not necessarily benefit the public (e.g studying of consumer preferences.) As such, members of the public should have the right to know what their personal data is being used for, and also the right to keep it confidential. For instance, where personal data is collected by businesses to improve their product/services (e.g. improvement of public transport services via analysis of passenger travel patterns), consent and notification should still be mandatory.

- **Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?**

We find that the proposed conditions could be specified in greater detail - the phrases "not desirable or appropriate" and "benefits to the public" appear vague and could be misappropriated by organizations to invoke this provision for extraneous reasons.

One suggestion to improve on the stated conditions is that organizations should be able to justify in writing, and declare for the record why obtaining consent was inappropriate or undesirable. This would introduce a system for accountability into this provision.

An additional condition that could be that the Legal and Business Purpose approach cannot be used to circumvent the earlier requirements for notification as outlined in 3.8.

- **Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?**

In section 4.4, it is mentioned that Article 33 would be enforced 'unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons'. We feel that the term 'rights and freedoms' is too vague and would require a more comprehensive definition for that. Furthermore, 'rights and freedoms' of each individual is very subjective (e.g. not causing any emotional, physical or financial harm).

With regards to the proposed number of affected individuals (i.e. 500 or more) in 'signalling' the presence of a systematic issue, we feel that a definitive number is not enough. Instead, PDPC should also use a percentage of the total data breached in measurement. For instance, when **30% or < 500 (whichever is lower)** of data has been accessed by an unauthorised party, PDPC should do further investigation and provide guidance in implementing the appropriate remedial actions.

- **Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?**

We agree with the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations. In all situations where the breach notification requirements are met or notifications are required by written law or sectoral regulations, the PDPC should be notified.

- **Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements?**

We agree with the rationale behind the need for exceptions and exemptions from breach notifications. There is a need to ensure that notification provisions are applied only in appropriate situations. However, in other circumstances, adherence to another overarching written law that prohibits notification would be

necessary. In that case, it is crucial to clarify which laws overrides/supplants the notification provision laws to prevent ambiguity.

The two proposed exceptions to the requirement to notify affected individuals are apt. However, the technological protection exception may not be fair in all circumstances. 'A reasonable standard' of encryption is not made clear to the layman and it would require individuals to trust entities that it is in fact secure. Moreover, the industry standards for encryption are constantly evolving, and may not be consistent throughout the region. We suggest that even in the case where data is highly encrypted, a breach notification should still be sent out to the individuals affected. This can include a message to reassure the individual that the entity has taken the necessary steps to secure the data and while the system has been breached, their personal data is still secure.

The Commissioner, along with the approval of the Minister, has the right to exempt organisations from the breach notification requirements in this proposed guidelines. However, we recommend that clarification can be given to the language used. For example, terms such as 'exceptional circumstances' and 'situations where notification may not be desirable' can be clarified to improve understanding from individuals and corporations on what specific situations may cause these exceptions to arise.

- **Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?**

We find the language "as soon as practicable" vague. Assuming the presence of risk of impact or harm, we suggest that organizations notify all affected individuals within 24 hours from the knowledge of the breach, so that precautionary measures may be taken. Organizations need only specify the occurrence of a breach without providing extensive details with regards to the breach. Organizations are required to follow up with the affected individuals with details of the full investigation, preferably within 40 days.

PDPC should be notified of the breach as soon as affected individuals are notified. Organizations are required to provide PDPC with relevant information as soon as practicable, within 72 hours from the knowledge about the breach, including weekends and public holidays if applicable.

We thank you once again for the opportunity to participate in this consultation process. We would be happy to discuss any of the above feedback with you.

Yours sincerely,
Class of NM4203 (AY2017/2018)

1. Lim May-Ann (lecturer) mayann@nus.edu.sg
2. Martijn Alexander ter Meulen E0215852@u.nus.edu
3. Gabriel Lim Min Kang A0124904@u.nus.edu
4. Chiang Hai Xuan haixuan.chiang@u.nus.edu
5. Carissa Liong Yuan Ting carissa.liong@u.nus.edu
6. Nisha Suresh Bhojwani nisha.bhojwani@u.nus.edu
7. Yu Han Huang e0216207@u.nus.edu
8. Lim Zeng Hou limzenghou@u.nus.edu
9. Nora Atiqa Adha a0130396@u.nu.edu
10. Yap Fang Qi Jolene a0113715@u.nus.edu
11. Lim Yen Han a0116094@u.nus.edu
12. Luo Junyang a0125131@u.nus.edu