Public Consultation on the

Draft Personal Data Protection (Amendment) Bill

28 May 2020

Contact Person: Dr. Rex Yeap
[Redacted]

This is a response to the 'Public Consultation on the Draft Personal Data Protection (Amendment) Bill.' [1]

Section A: Summary of Major Points

This is a summary of the sections within the public consultation document that I have responded to:

- **PART I: INTRODUCTION** -> "7a. …to amend the PDPA to incorporate relevant recommendations of the Public Sector Data Security Review Committee (PSDSRC)"
- **PART II: STRENGTHENING ACCOUNTABILITY** -> "Accountability principle"
- **PART II: STRENGTHENING ACCOUNTABILITY** -> "18. MCI/PDPC also intends to prescribe in Regulations categories of personal data"
- **PART III: ENABLING MEANINGFUL CONSENT** -> "41. Revisions will also be made to the research exception"
- **PART IV: INCREASING CONSUMER AUTONOMY** -> "Data Portability Obligation"
- **PART IV: INCREASING CONSUMER AUTONOMY** -> "47… b) The technical and process details"
- **PART VI: OTHERS** -> "Prohibitions to providing access"

Section B: Statement of interest

I am one of the pioneer batch (2014) of trainers and practitioners for the "WSQ Fundamentals of the Personal Data Protection Act" programme and is still active as of today.

Section C: Comments

C1. Response to "PART I: INTRODUCTION" -> "7a. …to amend the PDPA to incorporate relevant recommendations of the Public Sector Data Security Review Committee (PSDSRC)"

I have previously reviewed and cited the publicly available information relating to the recommendations of the PSDSRC and I feel that this is a positive development to make the PDPA more robust.

C2. Response to “PART II: STRENGTHENING ACCOUNTABILITY” -> “Accountability principle”

Version 1 and Version 2 of the “WSQ Fundamentals of the Personal Data Protection Act” programme was made available in 2014 and 2016 respectively. It is timely for the Commission to update the courseware to officially replace the Openness obligation with the Accountability obligation with updated examples.

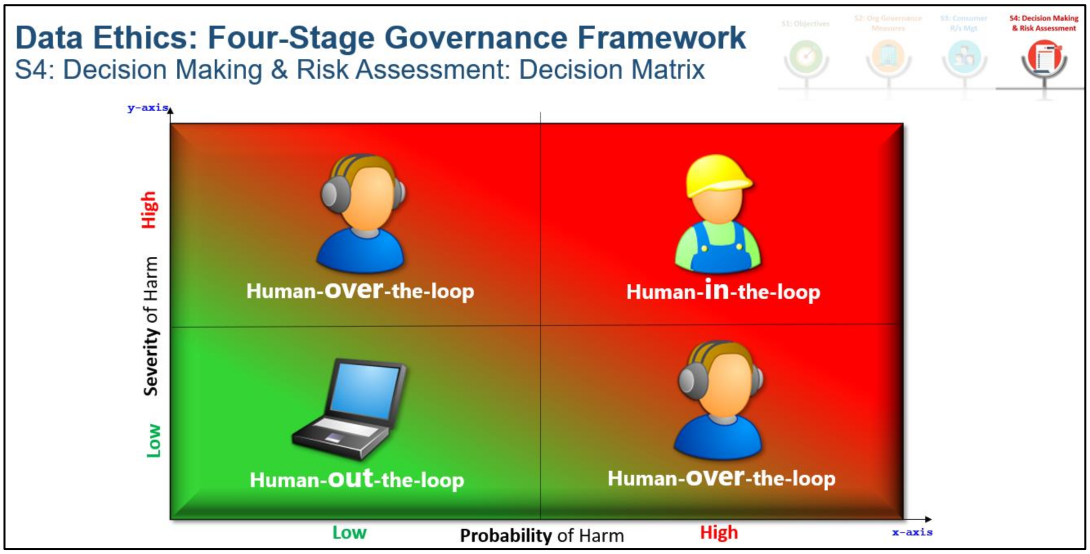
C3. Response to “PART II: STRENGTHENING ACCOUNTABILITY” -> “18. MCI/PDPC also intends to prescribe in Regulations categories of personal data”

Categorisation of personal data is most welcome as it takes into consideration various types of sensitive personal data which was further elaborated in the PDP Digest 2019 [3].

PDPC may also wish to review the Data Breach Management Plan (CARE model), and determine if further updates are required or necessary.

C4. Response to “PART III: ENABLING MEANINGFUL CONSENT” -> “41. Revisions will also be made to the research exception”

MCI/PDPC may also wish to take into consideration Data Ethics. The 4-stage Governance Framework [4] may apply to many data-driven and Artificial Intelligence systems. Recently, when I saw the use of safe distancing robo-ambassador in one of Bishan-Ang Mo Kio park [5], I was reminded of the Decision Making & Risk Assessment under the 4-stage Governance Framework [6] (Figure 1).



Data Ethics: Four-Stage Governance Framework

S4: Decision Making & Risk Assessment: Decision Matrix

Figure 1. Decision Matrix in the “Decision Making & Risk Assessment”

C5. Response to “PART IV: INCREASING CONSUMER AUTONOMY” -> “Data Portability Obligation”

Similar to my response in C2, I hope that Version 3 of the “WSQ Fundamentals of the Personal Data Protection Act” programme to be updated (soon) to include this obligation with examples. It might be helpful if the Commission can review all the past enforcement cases (or incidents from the three volumes of the PDP Digest) to identify scenarios that are relevant to the Data Portability obligation; and the extent of a violation of the Data Portability obligation (suppose it was in existent since 2014).

C6. Response to “PART IV: INCREASING CONSUMER AUTONOMY” -> “47… b) The technical and process details”

During the last year "Public Consultation on Review of the PDPA – Proposed Data Portability & Data Innovation Provisions" [7], there was a question: "*What are your views on the proposed binding codes of practices that set out specific requirements and standards for the porting of data in specific clusters or sectors?*" Having reviewed the text in the current public consultation focusing on the security/technical aspects on the porting of data, it is unclear to me if the stance is still the same last year, ie. "*Security of data: minimum standards to ensure the protection of data during transmission and the integrity and security of participating systems.*”

If yes, then I am repeating my concerns here:

(a) Some organisations may consider that a minimum standard for hashing is the use of MD5 and we have seen in the case of “FEI FAH MEDICAL MANUFACTURING PTE. LTD.” Case Number: DP-1409-A145 where the Commission noted that "*Although the passwords were encoded, they had been encoded using an MD5 message-digest algorithm, a commonly used cryptographic hash function, which could be easily attacked with password tables by any motivated individual.*” Instead, a more appropriate stance might be to use a standard that the industry deemed to **reasonably secure** which in the case of Fei Fah Manufacturing, that could be the use of the cryptographic hash function SHA256 [8].

(b) In another case involving P&N Holdings Pte. Ltd [9], the organization attempted to provide a secure means of hosting documents by using a "robots exclusion protocol" [10] which was supposed to '*hide documents from Google's search engine crawler*' [9, pp183]. As stated by its editors, '*the Organisation's approach towards protecting the documents in the VO System through the use of "/robots.txt" was not sufficient and evinced an incorrect or inadequate understanding of the security measure which they chose to implement'* [9, pp185]. Notably, the editors stated that '*Each organisation should adopt* ***security arrangements that are reasonable and appropriate*** *in the circumstances...*' [9, pp186]. Therefore, it is my opinion that adhering to "minimum standards" would be a mistake, a mistake such that if any future organization are in a similar situation like what happened to Fei Fah Manufacturing or P&N Holdings, may claim that 'minimum standards' was what expected of them in the security of personal data.

(c) Specific to the transfer of the ported data, organizations may wish to consider the use of public-key cryptography where each organization has a pair of private and public keys, of which its public key is known to all other organizations to facilitate a highly secure transfer of ported data [11]. Where necessary, a multi-signature approach to the private key management may be implemented so that there are multi-key holders [12].

C7. Response to "PART VI: OTHERS" -> "Preservation of personal data requested pursuant to access and porting requests"

There are too many incidents regarding individuals request to CCTV footage under the Access and Correction obligations and due to organisations misunderstanding of the obligation and thus failed to preserve the video footage and consequently causing grief to the requester, the "requirement for organisations to preserve personal data requested pursuant to an access request (or a copy)…" is very welcome.

It is expected that even with this requirement, there will be organisations that are ignorant of not just this requirement but also the Access and Correction obligation and I hope that the Commission will direct the company to send their DPO(s) or relevant staff for a formal PDPA training, or re-training – similar to the enforcement decision [13], ie. "*For all employees of the Respondent handling personal data to attend a training course on the obligations under the PDPA…*"

C7. Response to "PART VI: OTHERS" -> "Prohibitions to providing access"

I quote this text from section 74 "*From PDPC's experience, this has resulted in implementation issues for organisations providing access to personal data… The amendment will allow organisations to provide access to such data, regardless of whether providing access could (i) reveal personal data about another individual, or (ii) reveal the identity of an individual who has provided personal data about another individual and that individual does not consent to the disclosure of his/her identity.*"

I am surprised by this proposed amendment because the masking can always be applied to various media, be it text, image, video, or audio formats. While I am aware that such masking effort for formats such as audio and video involved a lot more effort compared to text, it is still doable. Furthermore, under the Access and Correction obligation, an organization can impose a reasonable fee – many would deem the inclusion of any cost involving masking to be reasonable. Therefore, I do not understand the absolute need for this amendment.

If the amendment goes through, there could be future scenarios where the unmasked footage of one or more individual(s) that result in unintended consequences – social, moral, ethical, legal, or political.

I might be a lone voice in this matter but I still hope that the Commission will reconsider the amendment in its current form.

<u>Section D: Conclusion</u>

I thank the MCI/PDPC for conducting this public consultation and hope that the inputs are constructive.

References

[1] PDPC, (2020). **Public Consultation on the Draft Personal Data Protection (Amendment) Bill**. Personal Data Protection Commission.

[2] Smart Nation, (2019). **Completion of public sector data security review: To secure and protect citizens’ data.:** https://www.smartnation.gov.sg/whats-new/press-releases/completion-of-public-sector-data-security-review--to-secure-and-protect-citizens-data#sthash.Cjh7y6q1.dpuf (Last access on 27 May 2020)

[3] PDPC, (2019) **Personal Data Protection Digest 2019.** https://www.pdpc.gov.sg/news-and-events/announcements/2019/07/pdp-digest-2019-now-available (Last access on 27 May 2020)

[4] PDPC, (2020), **Model AI Governance Framework**, 2nd Edition, https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework (Last access on 27 May 2020)

[5] CNA, (2020), **Meet the robot dog promoting safe distancing in Singapore's parks**, https://www.channelnewsasia.com/news/singapore/meet-the-robot-dog-promoting-safe-distancing-in-singapore-s-12716544 (Last access on 28 May 2020)

[6] Yeap, R. 2020. **Data Ethics: Four-Stage Governance Framework & Decision Matrix**, IP Blockchain, A220846607F940ED2BC1BDED2FE23B34C2401D09FD12A08B74B1ACD0BCE0F64F, 2020-05-28.

[7] PDPC, (2019). **Public Consultation on Review of the PDPA – Proposed Data Portability & Data Innovation Provisions**. Personal Data Protection Commission.

[8] Gilbert Henri, Helena Handschuh (2003). **Security Analysis of SHA-256 and Sisters**. Selected Areas in Cryptography, pp175–193

[9] Yeong Z.K., Alfred D., Chen S.A., Aw Jansen (2017). **Personal Data Protection Digest**, Academy Publishing, pp 182-189.

[10] Sverre H. Huseby (2004). **Innocent Code: A Security Wake-Up Call for Web Programmers**. John Wiley & Sons. pp. 91–92.

[11] Ferguson, Niels; Schneier, Bruce (2003). **Practical Cryptography**, Wiley. ISBN 0-471-22357-3.

[12] Bellare M, Neven G (2006). **Identity-Based Multi-signatures from RSA**. Topics in Cryptology – CT-RSA. Lecture Notes in Computer Science. 4377. pp. 145–162.

[13] PDPC, (2016), **[2016] SGPDPC 4**.