Public Consultation on Review of the PDPA – Proposed Data Portability & Data Innovation Provisions

1st July 2019

Contact Person: Dr. Rex Yeap

This is a response (version 1.1) to the 'Public Consultation on Review of the PDPA – Proposed Data Portability & Data Innovation Provisions.' [1]

Q1. What are your views on the impact of data portability, specifically on consumers, market and economy?

Response: Part II of the document has clearly summarized what as well as the positive impact of data portability for the consumers, market and the economy. I look forward to this 10th data protection obligations within data protection provisions of the PDPA.

Q2. What are your views on the proposed Data Portability Obligation, specifically –

a) scope of organisations covered; and

b) scope of data covered?

Response: I would like to suggest that the individual be notified before (at least 30 days in advance) and after (within 3 days) the porting of data from one organization to another.

Q3. What are your views on the proposed exceptions to the Data Portability Obligation, specifically –

a) the proposed exception relating to commercial confidential information that could harm the competitive position of the organisation, to strike a balance between consumer interests and preserving the incentive for first movers' business innovation; and

b) the proposed exception for "derived data"?

Response for Q3(a): If this exception is granted, some organisations may deliberately use the exception to deny any request, rendering this obligation ineffective.

Response for Q3(b): This make sense because much of the 'derived data' would be deemed as an IP of the organization which invest in resources for the generation of such 'derived data' of which many of the techniques involved are most probably proprietary and some may even be patented. An example of one such patent application is US20190041984 titled *System and method for detecting invisible human emotion in a retail environment* [2].

Q4. What are your views on the proposed requirements for handling data portability requests?

Response: No comment.

Q5. What are your views on the proposed powers for PDPC to review an organisation's refusal to port data, failure to port data within a reasonable time, and fees for porting data?

Response: I strongly support the proposed powers for PDPC to review an organisation's refusal to port data, failure to port data within a reasonable time, and fees for porting data.

Q6. 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?

Response: Paragraph 2.49(d) states that "Security of data: minimum standards to ensure the protection of data during transmission and the integrity and security of participating systems." I am concerned with the "minimum standards" statement.

(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 [6].

(b) In another case involving P&N Holdings Pte. Ltd [4], the organization attempted to provide a secure means of hosting documents by using a "robots exclusion protocol" [5] which was supposed to '*hide documents from Google's search engine crawler*' [4, 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*' [4, pp185]. It is notable that the editors stated that '*Each organisation should adopt **security arrangements that are reasonable and appropriate** in the circumstances...*' [4, 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 [7]. Where necessary, a multi-signature approach to the private key management may be implemented so that there are multi key holders [8].

Q7. What are your views on the proposed approach for organisations to use personal data for the specified businesses innovation purposes, without the requirement to notify and seek consent to use the personal data for these purposes?

Response: Business innovation are can also be deemed to be the IP of an organization which would have typically invested much resources – this has been elaborated in my response to Q3(b).

On the requirement to seek consent first before use, I do not see this as practical.

However, it would certainly be good if organization could broadly indicate how our personal data would be use in their business innovation.

Q8. What are your views on the proposed definition of "derived data"?

Response: I have stated my views on 'derived data' in my Q3(b) response and I would like to cite another patent CN106570474B titled *Micro expression recognition method based on 3d convolution neural network* with micro-expression as a novel form of derived data.

Q9. What are your views on the proposal for the Access, Correction and proposed Data Portability Obligations not to apply to derived personal data?

Response: No strong view on this.

Conclusion

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

References

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

[2] Lee Kang, Zheng Pu (2019). "**System and method for detecting invisible human emotion in a retail environment**", Nuralogix, United States Patent Application Number US20190041984.

[3] PDPC (2016). "**FEI FAH MEDICAL MANUFACTURING PTE. LTD. (UEN No. 199800455H)**", Case Number: DP-1409-A145.

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

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

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

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

[8] 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.

[9] Lu Guanming, Yang Cheng, Yan Jingjie (2016). "**Micro expression recognition method based on 3d convolution neural network**", National Intellectual Property Administration, Granted Patent Number CN106570474B.