M1'S RESPONSE TO MCI'S AND PDPC'S PUBLIC CONSULTATION ON THE DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL, INCLUDING RELATED AMENDMNETS TO THE SPAM CONTROL ACT

This paper is prepared in response to MCI's and PDPC's Public Consultation document dated 14 May 2020 and represents M1's views on the subject matter. Unless otherwise noted, M1 makes no representation or warranty, expressed or implied, as to the accuracy of the information and data contained in this paper nor the suitability of the said information or data for any particular purpose otherwise than as stated above. M1 or any party associated with this paper or its content assumes no liability for any loss or damage resulting from the use or misuse of any information contained herein or any errors or omissions and shall not be held responsible for the validity of the information contained in any reference noted herein nor the misuse of information nor any adverse effects from use of any stated materials presented herein or the reliance thereon.

Introduction

1. M1 is Singapore's most vibrant and dynamic communications company, providing mobile and fixed services to over 2 million customers. With a continual focus on network quality, customer service, value and innovation, M1 links anyone and anything; anytime, anywhere.

M1's view on the Proposed Amendments to the PDPA

2. M1 supports the development of a proportionate and stable regulatory environment as it will catalyse a sustainable and growing info-communications industry where long term planning and decisions can be undertaken.

3. M1 welcomes the opportunity to submit our comments to MCI/PDPC's public consultation on the proposed amendments to the Personal Data Protection Act ("**PDPA**"). We believe that it is timely to review the PDPA to ensure that the regulatory environment keeps pace with the evolving technological and business landscape, while providing for effective protection of personal data in the Digital Economy.

4. M1's specific comments on the PDP (Amendment) Bill Consultation are set out in the following sections.

PART II: STRENGTHENING ACCOUNTABILITY

Accountability principle

1. M1 has no objection to MCI/PDPC's proposal to insert the words "AND ACCOUNTABILITY FOR" in Part III of the Personal Data Protection Act 2012 ("PDPA").

Mandatory data breach notification requirement

Notification Criteria

2. M1 supports MCI/PDPC's proposal to introduce a mandatory data breach notification requirement under the PDPA. We have no objection to MCI/PDPC's proposal to prescribe in Regulations categories of personal data, which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals. However, we would suggest that MCI/PDPC conduct another round of consultation with the industry to determine the appropriate categories of personal data that will be considered likely to result in significant harm to the individuals.

Assessment and notification timeframes

3. We note that the proposed obligation of the Data Intermediary's ("DI") is to notify the organisation without undue delay from the time it has credible grounds to believe that a data breach has occurred. However, it remains unclear on where the responsibility should lie in the event that the DI has not reported the data breach incident to the organisation in a timely manner for further investigation. In such a situation, we wish to seek MCI/PDPC's confirmation that enforcement actions would only be taken against the DI, given that the organisation would be unaware of such a data breach incident if it was not reported.

4. We also note the requirement for organisation to (i) notify all affected individuals on or after notifying PDPC; and (ii) not notify any affected individual if instructed by law enforcement agencies or PDPC, or during exceptional circumstances. We wish to clarify whether any notification to affected individuals is therefore subject to PDPC's approval or should be certain period of time after PDPC is notified.

5. With respect to draft section 26D(5), we note the exclusion for "…any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual". We propose to delete the word "technological" to give organisations greater flexibility to design and implement measures that will render it unlikely that such breach will result in significant harm to individuals.

Removal of exclusions for organisations acting on behalf of public agencies

6. M1 has no objection to MCI/PDPC's proposal to remove the exclusion for organisations that act on behalf of a public agency in relation to the collection, use or disclosure of personal data.

Offences relating to egregious mishandling of personal data

7. M1 has no objection to MCI/PDPC's proposal to introduce the following new offences under the PDPA to hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation or a public agency:

i. Knowing or reckless unauthorised disclosure of personal data;

ii. Knowing or reckless unauthorised use of personal data for a wrongful gain or a wrongful loss to any person; and

iii. Knowing or reckless unauthorised re-identification of anonymised data.

PART III: ENABLING MEANINGFUL CONSENT

Enhanced framework for collection, use and disclosure of personal data

8. M1 supports MCI/PDPC's proposal to expand deemed consent under section 15 of the PDPA to include:-

   i. Deemed consent by contractual necessity;

   ii. Deemed consent by notification.

9. M1 also agrees with MCI/PDPC's proposal to introduce two new exceptions to the consent requirement:-

   i. Legitimate interests exception;

   ii. Business improvement exception.

10. Lastly, M1 has no objection to MCI/PDPC's proposal to revise the research exception to permit organisations' use and disclosure of personal data without consent for research purposes. However, there remains ambiguity over the assessment of several key factors proposed by MCI/PDPC, such as how does the organisation determine that the benefit to the public (or any section thereof) outweighs any likely residual adverse effect to the individual. To this end, we would request that MCI/PDPC provides more guidance to help organisations better understand how to implement the enhanced framework in a practical manner.

PART IV: INCREASING CONSUMER AUTONOMY

Data Portability Obligation

11. M1 supports MCI/PDPC's proposal to introduce a new data portability obligation. We agree that this is beneficial to consumers as it eases the transition between different service providers, and also lead to new and increased collaborations among organisations across industry sectors.

12. However, MCI/PDPC would understand the implementation of Data Portability obligation will not be a straightforward matter, and there are many issues which require further deliberation (e.g. data format, charges, security, liabilities etc.). We note that PDPC will work with the industry and relevant sector regulators to develop the requirements to be prescribed in the Regulations. As such, we will provide our specific comments on the different requirements of the Data Portability Obligation during the relevant consultation.

Improved controls for unsolicited commercial messages

13. M1 supports MCI/PDPC's proposal to make the following amendments to address the issue of spam messages in Singapore:-

i. For the Spam Control Act ("**SCA**") to cover commercial text messages sent to instant messaging ("**IM**") accounts and in bulk;

ii. To introduce the prohibition of the sending of specific messages to telephone numbers obtained through the use of dictionary attacks and address harvesting software under the Do Not Call ("**DNC**") Provisions;

iii. To introduce obligation and liability on third-party checkers; and

iv. To incorporate the Personal Data Protection (Exemption from Section 43) Order 2013 into the DNC Provisions.

PART V: STRENGTHENING EFFECTIVENESS OF ENFORCEMENT

Enforcement of DNC Provisions under administrative regime

14. M1 has no objection to MCI/PDPC's proposal for PDPC to enforce certain DNC Provisions under the same administrative regime as the DP Provisions. However, we would ask MCI/PDPC to provide more clarity on the specific DNC Provisions that will be enforced under the same administrative regime as the DP Provisions.

Increased financial penalty cap

15. M1 notes that MCI/PDPC has proposed to increase the maximum financial penalty to (i) up to 10% of an organisation's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher. We are very concerned over MCI/PDPC's proposal, as it is overly punitive for data breaches. Furthermore, we note that some organisations may be already subject to various penalties across multiple regulatory frameworks (e.g. a cybersecurity incident leading to a data breach). Such organisations should not be unfairly penalised under various regulatory frameworks for the same incident that occurred.

16. In view of the above, we would urge MCI/PDPC to review the proposed financial penalty cap. Also, we are of the view that there should not be any imposition of double penalties under different regulatory frameworks for the same incident.

Require attendance

17. M1 has no objection to MCI/PDPC's proposal to introduce an offence for a person's failure to comply with an order to appear before PDPC/an inspector and provide his/her statement(s) in relation to an investigation under section 50 of the PDPA.

Statutory undertakings

18. M1 has no objection to MCI/PDPC's proposal to include statutory undertakings under the PDPA.

Referrals to mediation

19. M1 note that MCI/PDPC' has proposed to amend section 27 of the PDPA to provide PDPC with the power to (i) establish or approve one or more mediation schemes; and (ii) direct complainants to resolve disputes via mediation. However, there is lack of information on how PDPC intends to implement the proposal in a fair and practical manner. For example, PDPC will need to establish a clear process (e.g. the relevant criteria for escalation (including whether there is an exception for frivolous and vexatious complaints), scope of issues, and the party responsible to cover the costs of mediation, whether the agreed outcome of mediation will be legally binding on the parties etc.) for individuals to seek PDPC's assistance on a complaint or dispute under the

PDPA. We trust that MCI/PDPC will be conducting further consultations with the industry to determine the appropriate process for such mediation referrals.

PART VI: OTHERS

Preservation of personal data requested pursuant to access and porting requests

20. M1 has no objections to MCI/PDPC's proposal to introduce a requirement for organisations to preserve personal data requested pursuant to an access request (or a copy) for a prescribed period of (a) at least 30 calendar days after rejection of the request, or (b) until the individual has exhausted his/her right to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal, whichever is later. However, we wish to clarify whether organisations will be able to charge such individuals for reasonable costs incurred to preserve personal data requested.

Prohibitions to providing access

21. M1 has no objections to MCI/PDPC's proposal to amend section 21 of the PDPA to reduce the scope of prohibitions to access in relation to user provided and user activity data.

Excluding "derived personal data" from Correction and Data Portability Obligations

22. M1 is supportive of MCI/PDPC's proposal to exclude "derived personal data" from Correction and Data Portability Obligations. However, we wish to seek for clarification on the rationale behind requiring organisations to provide individuals with access to derived personal data, and/or with information about the ways in which the derived personal data has been or may have been used or disclosed by the organisation within a year before the date of the request. As mentioned by MCI/PDPC in paragraph 49 of the Consultation document, "derived personal data" is commercially sensitive information that may foster business innovation and investments by organisations. In allowing individuals to access such "derived personal data", there is a risk that such insights may be retrieved and leaked to competitor organisations, resulting in a loss of competitive advantage for the organisation who had developed these insights.

Revised exceptions to Consent Obligation

23. M1 has no objections to MCI/PDPC's proposal to streamline and consolidate the exceptions to consent, and to simplify how organisations may collect, use and disclose personal data without consent.