SINGAPORE PRESS HOLDINGS LTD

Submission to the Ministry of Information, Communications and the Arts on the Public Consultation on the Proposed Personal Data Protection Bill

30 April 2012

Contact Person:

Ginney Lim
General Counsel,
Executive Vice President
& Group Company Secretary
limmlg@sph.com.sg

TABLE OF CONTENTS

30 April 2012

Ministry of Information, Communications & the Arts

(via email MICA_DNC_Public_Consultation@mica.gov.sg)

Dear Sirs

PUBLIC CONSULTATION ON THE PROPOSED PERSONAL DATA PROTECTION BILL

A. INTRODUCTION

1.1 Following SPH's submissions on the Proposed Consumer Data Protection ("DP") Regime for Singapore on 25 October 2011 and Framework Details for the Establishment of a National Do-Not-Call ("DNC") Registry on 31 October 2011, we are pleased to submit our comments in response to the consultation paper ("Consultation Paper") on the Proposed Personal Data Protection Bill ("PDPA") issued by the Ministry of Information, Communications and the Arts ("MICA") on 19 March 2012.

1.2 As submitted in our earlier two responses, SPH would like to reiterate that there should be a balance struck between the need to protect consumers' personal data ("PD") and the value derived by organisations in collecting and using the data for their legitimate business objectives and purposes. In addition, SPH feels that the issue of compliance cost ought to be a key factor in the PDPA. Below are SPH's detailed comments and clarifications sought on the draft PDPA. Some of these comments were made in our two submissions during the earlier consultations and are repeated herein as SPH still holds the view that they are valid and should be taken into account.

B. SUMMARY OF COMMENTS

1.3 In broad terms, whilst SPH recognises that the PDPA may bring about greater accountability in the use of personal data, it is very concerned that the proposed PDPA does not strike a reasonable balance between the interests of data subjects and commercial organisations. Therefore compliance with the PDPA will result in very onerous obligations being imposed on commercial organisations. This leads to significant compliance burdens which are disproportionate relative to the concerns of data subjects, and also differ from other personal data regimes overseas.

1.4 SPH respectfully urges MICA to carefully re-consider the proposed PDPA framework and to more finely balance the rights of data subjects as well as the duties of organisations. SPH's primary concerns about the PDPA may be summarised as follows:

(a) Compliance requirements are onerous and insufficient flexibility for opting-out

Many of the obligations imposed by the PDPA will result in significant changes to business processes – eg. the need to disseminate corrections to third party recipients, the need to notify employees of collection, use or disclosure of their PD if "managing or terminating an employment relationship", etc. At the same time, the enforcement and penalty regime will mean that businesses will be

compelled to incur huge business costs to comply with the PDPA and also possibly maintain audit trails to place themselves in a position to defend assertions of breaches of the PDPA.

Further, the concept of "consent" under the PDPA, which is now subject to requirements of reasonableness and due notification of purposes, will apply to the obligations in Part IV of the PDPA (collection, use and disclosure) of personal data, but this concept does not appear to apply to the obligations imposed in Parts V and VI of the PDPA.

The requirements of Parts V and VI are no less onerous on organisations. As such, we would urge MICA to also allow for data subjects to opt-out of protections under these Parts of the PDPA so that there can be greater flexibility for data subjects and organisations to agree appropriate levels of protection of PD, given that the concept of consent is now subject to reasonableness requirements in any event.

(b) Remedies for breaches of the PDPA are too onerous and disproportionate

The proposed PDPA will introduce many layers of liability for breaches of the PDPA, specifically:

- Financial penalties of up to SGD 1 million
- Offences for certain wilful acts
- Personal liability of officers of organisations
- Rights of private action

Further, the availability of remedies at common law for breaches of obligations of confidence (depending of course on the facts) must also not be forgotten.

On top of this, the Data Protection Commission ("DPC") will have extensive powers of investigation, and further, whistle-blower protections have also been introduced in the PDPA (section 57).

The availability of such multi-layered remedies is comparatively rare in Singapore, and to date has been reserved for the most serious forms of improper conduct, such as corruption and money-laundering.

The nature of PDPA breaches appears to be hardly on the same footing. Hence it is puzzling why MICA has opted for such remedies for breaches of the PDPA. When comparing the remedies available under the PDPA, one notes they are more extensive than compared with those for breaches of obligations relating to PD under our existing sector specific laws.

Unlike data privacy regimes overseas, what is also conspicuously absent is any threshold of materiality before liability for breaches of the PDPA arises. Worse is that even if the DPC is of the view that a breach is trivial and that no punitive action should be taken against an organisation, rights of private action will mean that there may still be corporate exposure for breaches of the PDPA.

Given that the PDPA regime will be a new paradigm for the treatment of PD amongst organisations in Singapore, organisations and data subjects will need time to understand the requirements of the new regime. There will need to be room for norms to evolve from one where currently at law, the legal obligations relating to PD are very specific and well defined. The sunrise period will not be enough. Imposing an onerous multi-layered enforcement regime with personal liabilities attaching with too low a threshold may result in organisations having to undertake excessive steps to mitigate and manage corporate risk. At the same time, they will face practical difficulties in engaging compliance officers to undertake supervision of PDPA obligations.

SPH strongly urges MICA to calibrate the remedies available under the PDPA against other corporate regulatory compliance requirements and to balance the requirements of individuals and organisations more evenly. The penalties and remedies under the PDPA appear to be much more severe relative to other forms of corporate conduct which are subject to regulation (ie, outside the PDPA framework) and also privacy regimes overseas.

SPH also urges MICA to take a holistic view of some of its positions eg. there being no differentiated treatment of sensitive data and non-sensitive data, the inability to opt-out of the operation of certain provisions against the overall stringency of the enforcement regime.

1.5 As for the specific provisions of the PDPA, SPH's comments may be summarised as follows:

(a) "Data Intermediaries"

Section 4(3) should be clarified that an organisation should only be liable for PD that has been collected by it and not for PD collected by the intermediary.

(b) Interface between the PDPA and other Acts

The operation of section 4(7) should be clarified and further guidance on inconsistencies should be provided.

(c) Data Protection Officers

The personal liability of data protection officers appointed under Section 13(3) should be clarified. Offences which attract personal liability of officers and relevant defences (in particular Sections 50 and 51) should also be removed or reviewed.

(d) Intra-Group Sharing of Personal Data

SPH would like to appeal to MICA to re-consider excluding the consent requirement for intra-group sharing of PD as an integrated flow of information is necessary in many group business structures.

(e) Withdrawal of Consent

Clarity is sought on the meaning of “legal obligation” and “frustrate” under section 18(5).

In respect of Section 19 where an organisation had collected PD not under the circumstances or conditions in the Third Schedule, it should be clarified whether the organisation can still use or disclose the PD under Section 21, if the use or disclosure was for the purposes for which the PD was collected before the appointed day, even though these purposes may not fall under those in the Third Schedule.

Section 21 refers to “use” of PD but omits “disclose”. SPH is proposing that the word “disclose” be inserted. SPH is also of the view that Section 21(b) should be deleted as the situation is covered under Section 21(a).

(f) Access, Correction and Care of PD

The access and correction regimes in sections 23 & 24 are too onerous, and authentication of ownership issues may also arise in giving access to individuals and allowing them to correct PD. MICA should consider allowing for individuals to opt-out based on PDAP consent principles or further safeguards to prevent abuse.

Under Section 26, organisations should not be held culpable if inadvertent breaches or disclosures of PD were to occur.

(g) Guidelines, Comments, Penalties, etc.

Section 28(3) should stipulate that existing industry-specific guidelines should prevail over the guidelines issued under the PDPA and also for a guidance regime to be introduced so that organisations may seek advice on how statutes should interact.

SPH also believes that any financial penalty imposed should be based on clear provisions in the PDPA for specified and serious breaches. Sections 30 and 31 should be reviewed to only provide for financial penalties to be subject to more conditions, eg. for repeated offences, or when notice for compliance has been given and there was non-compliance or flagrant and deliberate breach of the PDPA.

In respect of complaint handling under Section 33, SPH is in favour of a more measured approach. The DPC should not take action on the first complaint. It should examine other factors such as the number of complaints and the potential for repeated breaches.

SPH also submits that the PDPA should incorporate a safe harbour regime in connection with section 35, which protects an organisation from liability if a contravention is inadvertent.

Further, as the offence and penalty framework is adequate deterrence, and individuals are already entitled under law to take civil action, it is not necessary to specifically provide that individuals may take private action against an organisation under Section 36, as this may encourage wasteful litigation.

(h) Do Not Call Registry

SPH seeks clarifications in respect of the definition "specified message" and calls for the same definition as used in the Spam Control Act to be applied. The definitions of "goods" and "services" should also be clarified under section 40.

With respect to section 41(3), as the word "goods" is defined, it would be clearer to replace the word "product" with "goods".

SPH does not agree that the DNC regime should include businesses and Section 44 should not allow them to opt out.

Section 47 requires an organisation to filter the numbers with DNC registry before sending out messages but a statement of the deadline by which the Commission has to revert and a maximum time frame should be provided for.

It should also be clarified that registering a number on the DNC should not constitute withdrawal of consent relating to other forms of PD within the meaning of Section 21.

The PDPA should also provide more clarity on the small quantity lookup service referenced in the consultation paper.

1.6 SPH's detailed comments follow.

C. DETAILED COMMENTS

A. Part I - Preliminary

2. Section 4(3) - Application of Act

2.1 Section 4(3) provides that the organisation is liable for PD processed by a data intermediary on its behalf.

2.2 However, some data intermediaries may themselves collect, use or disclose other PD relating to the same data subject, which may not have been provided by the organisation engaging the intermediary.

2.3 An example is where an organisation ("Instructing Organisation") uses a payment gateway and supplies it certain information. The payment gateway will itself collect credit card numbers which would constitute PD, but this may not necessarily be shared with the Instructing Organisation.

2.4 It is submitted that section 4(3) should be clarified to apply only in respect of PD which an organisation has provided the data intermediary, and not PD which the data intermediary collects on its own.

2.5 A further concern is that section 4(3) should also recognise some limitations on the liability of the Instructing Organisation for breaches of PDPA obligations by the data intermediary – for example, an Instructing Organisation should be regarded as having discharged its obligations under the PDPA if it can demonstrate that it has taken reasonable steps to ensure observance by the data intermediary of PDPA obligations applicable to the PD.

2.6 On a related front, to what extent would the data intermediary be regarded as an "agent" of the Instructing Organisation within the meaning of Section 51(2)? There must be some reasonable limitations along the lines stated above, and recognition that the Instructing Organisation does not have liability where the agent has exceeded its authority or acted on a frolic of its own.

2.7 Indeed, since there is already an established body of law relating to when a principal-agent relationship arises, and the liability of principals for the actions of their agents, section 51(2) is unnecessary and should be deleted. If it is to be included, then the section must be balanced off by recognising that it does not change any relevant legal principles (including defences) under the law of agency.

3. <u>Section 4(7) – Application of Act</u>

3.1 Section 4(7) provides that if there is any "inconsistency" between PDPA and any other written law, the other written law will prevail.

3.2 Section 4(7) uses the word "inconsistencies" but more clarity is needed as to what this will cover. For example, would an inconsistency arise only where both the PDPA and another written law address an identical subject matter in opposite ways?

3.3 How will section 4(7) apply for example where under section 47, Banking Act, the provision of customer consent will permit disclosure of customer information, but yet the consent regime in the PDPA is quite different in terms of its requirements?

3.4 SPH suggests that for section 4(7) to be meaningful, it should provide that where there are provisions in other written laws (including codes, guidelines, regulations and rules) that relate to the same subject matter as that covered in the PDPA, those other written laws should prevail, rather than providing that only in the event of "inconsistencies" will the other written laws prevail. Further, it should clarify that the enforcement regime of the PDPA will not apply where there are other relevant written laws dealing with the same subject matter.

3.5 It is also submitted that an informal guidance regime be introduced whereby organisations may seek clarification and guidance with the DPC on which laws ought to prevail, and that immunities be provided to organisations complying with such guidance.

B. Part III – General Rules with respect to Protection of Personal Data

4. <u>Section 13(3) & 13(6) – Compliance with Act</u>

4.1 Section 13 requires that an organisation must appoint one or more "individuals" to ensure that the organisation complies with the PDPA. However, an organisation is not thereby relieved of its obligations under the PDPA.

4.2 Section 13(3) provides that an organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA ("DP Officer"). However, the PDPA does not provide any guidance on whether such individual must be an employee of the organisation or whether the role may be outsourced to an independent third party. SPH would like to seek clarification on this point.

4.3 A further issue is that the PDPA is not clear as to the extent to which these individuals will have personal liability for breaches under the PDPA.

4.4 Section 13(6) merely states that the designation of an individual by an organisation shall not relieve the organisation of any of its obligations under the PDPA. However, it is also noted that under Section 50, "officers" of a body corporate (which is broadly defined to mean "any director, partner, member of the committee of management, chief executive, manager, secretary or other similar officer of the body corporate and includes any person purporting to act in any such capacity") may be personally liable if they are found to have committed an offence under the PDPA knowingly or further, and unusually, where there was "neglect" on the part of the officer.

4.5 Would the DP Officer designated under Section 13(3) be treated as an officer within the meaning of Section 50? The defence available to employees under section 51(3) does not apply to any employee who "was in a position to make or influence a decision regarding that act or conduct" (Section 51(4)), and it would seem that a DP Officer, would in a majority of cases, fall within this exclusion. If so, as a practical matter, it will be difficult to engage any person who would be willing to undertake such a role, since there would be a high risk of personal prosecution.

4.6 This concern is compounded because it is rare that corporate officers are subject to personal prosecution for negligence in relation to corporate acts in Singapore.

4.7 For example, under Section 157(1) read with Section 157(3) of the Companies Act, only a director (and not officers in general) is subject to personal prosecution where he has failed to act "honestly and use reasonable diligence" (and this imposes a higher standard of care than mere negligence). The punishment for such offences is a maximum fine of $5,000 or imprisonment for up to 12 months.

4.8 Under the Penal Code, persons are at risk of prosecution for negligence only in very specific circumstances (see eg Part XIV)[1]. The closest analogy may perhaps be drawn with section 336, where an offence is created where a person "does any act so … negligently as to endanger human life or the personal safety of others", but even so, it is punishable "with imprisonment for a term which may extend to 3 months, or with fine which may extend to $1,500, or with both".

[1] "Negligent act likely to spread infection of any disease dangerous to life" (section 269), "Negligent conduct with respect to any poisonous substance" (section 284), "Negligent conduct with respect to any fire or combustible matter" (section 285), "Negligent conduct with respect to any explosive substance" (section 286), "Negligent conduct with respect to any machinery in the possession or under the charge of the offender" (section 287), "Negligence in pulling down or repairing buildings" (section 288), "Negligence with respect to any animal" (section 289).

4.9 SPH questions whether against the existing statutory framework, breaches of the PDPA should be treated as being of such severity that they merit the creation of a new offence attracting personal liability of officers for mere "neglect".

4.10 Further, the offence under the PDPA attracts "a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding $1,000 for every day or part thereof during which the offence continues after conviction". This is a far more severe punishment than for the existing offences relating to negligence discussed above.

4.11 SPH submits that introducing such personal liability for officers for PDPA offences is disproportionate and this concept should be removed from the PDPA. The severe financial penalties which may be imposed will already ensure that organisations will take their PDPA obligations seriously. Further, it is open to organisations to dismiss or take other disciplinary steps against employees who have exposed the organisation to such prosecution without the need to further legislate for this.

4.12 Sections 50 and 51 will otherwise deter employees from accepting the additional duties of a compliance officer and in addition, organisations will have difficulty persuading directors to join their boards if directors were to be subject to personal liability.

C. Part IV – Collection, Use and Disclosure of Personal Data

5. <u>Section 15 – Consent required</u>

5.1 Paragraph 2.35 of the Consultation Paper clarifies that MICA does not intend to provide exclusions from all or part of the PDPA for the sharing of data among related organisations.

5.2 SPH understands that not all feedback and inputs can be accepted and consolidated under the PDPA. However, we hope that the MICA will take into consideration that many organisations already have massive amounts of data and information flowing between their subsidiaries, affiliates, divisions, departments and business units.

5.3 SPH would like to appeal to MICA to re-consider and provide that no consent is required for such sharing of PD amongst related corporations. It is a reality that businesses are organised as groups with distinct subsidiaries which often share common corporate resources – eg. human resource functions may be centrally handled at a group level by the main corporate entity. Such integration is organic and necessary as businesses face stiffer competition and an ever-changing and challenging environment. Hence, to require consent for integrated flow of information and PD would retard integration that is so vital for survival and the prosperity of Singapore's economy.

5.4 Rather than dismiss the concept outright, MICA can perhaps consider a more calibrated response, eg. allow sharing amongst designated related corporations (within the meaning of section 6 of the Companies Act) or where the entities are located in Singapore.

6. <u>Section 18(5) – Withdrawal of consent</u>

6.1 Section 18(5) stipulates that an individual may not withdraw consent if withdrawing consent would frustrate the performance of a legal obligation.

6.2 SPH would like to seek clarity on two points:

(a) The definition of "legal obligation" in the section should explicitly cover legal obligations under laws, codes, regulations, etc, as well as contractual obligations so that it is very clear that organisations may meaningfully rely on this provision.

(b) The term "frustrate" lacks sufficient clarity within the context of this section. As a legal concept, "frustration" at contract law for example may not extend to deliberate acts of one party to the agreement – though of course the law offers remedies against a party who "repudiates" his obligations by not intending to be bound by them. MICA may perhaps consider either clarifying the meaning of the term "frustrate" or using a different term.

7. Section 19 – Collection, use and disclosure without consent

7.1 Section 19 provides that the Third, Fourth and Fifth Schedules set out the circumstances and conditions under which no consent is required for the collection, use or disclosure of PD respectively. This extends to before the appointed date. However, it is not clear whether an organisation which had collected PD not under the circumstances or conditions in the Third Schedule, can still use or disclose the PD under Section 21, if the use or disclosure was for the purposes for which the PD was collected before the appointed day, and even though these purposes may not fall under those in the Third Schedule. SPH would like to seek clarification on this point.

8. Section 21 – Personal Data Collected Before the Appointed Date

8.1 Under Section 21, an organisation may still "use" PD if PD was collected before the appointed date for the purposes for which PD was collected unless (i) consent is withdrawn in accordance with Section 18; or (ii) before or after the appointed date, the individual indicates to the organisation that he does not consent to the use of the PD.

8.2 In this regard, SPH has the following concerns:

(a) In Section 21(a), the word "use" could be interpreted to mean that an organisation can only use but cannot disclose the PD even if the PD was collected before the appointed date. SPH submits that the word "disclose" should be inserted. This is to reflect more accurately the situation whereby the organisation may have also been using and disclosing the PD before the appointed date. It is also noted that in other parts of the PDPA, where applicable, the word "disclose" is also mentioned with the word "use". Hence, Section 21 should apply to both "use and disclosure" of PD before the appointed date.

(b) Section 21(b) refers to, *inter alia*, the individual indicating to the organisation that he does not consent to the use of PD before or after the appointed date. This appears to be the same as Section 21(a) which refers to consent being withdrawn in accordance with Section 18. If there is a subtle difference between indicating to the organisation and withdrawing consent under Section 18, SPH submits that this will only cause confusion in implementation and compliance, and that Section 21(b) should therefore be deleted in its entirety.

8.3 Section 21 also specifically states that withdrawal of consent should be done in accordance with Section 18. It is submitted that the PDPA should also be clarified to

explicitly state that the mere registration of a number on the Do Not Call ("DNC") register will not amount to withdrawal under Section 21, until the individual submits a withdrawal of the consent within the meaning of Section 21. It should be noted that whilst MICA appears to take the position that it does not wish to adopt an exception to the DNC for existing relationships, if the consent was previously provided in relation to other types of PD in addition to the telephone number, the registration of a number on the DNC register should not constitute a withdrawal of consent in relation to other types of PD.

D. Part V – Access to and Correction of Personal Data

9. Section 23 – Access to Personal Data, Section 24 – Right to Request Correction of Personal Data

9.1 SPH is of the view that Section 23(1) is too prescriptive and will be unnecessarily burdensome on organisations, particularly the obligation to provide an individual with information about the ways in which the PD has been and is being used by the organisation. This information probably includes names of the individuals and organisations to whom the PD has been disclosed. It will be impractical, if not impossible, for organisations to keep track and a record, of the names of the individuals to whom the PD has been disclosed, particularly if the disclosure was done in the course of its business activities and shared with employees or persons within the group of related companies, or with their out-sourced organisations and employees or agents.

9.2 Another issue is the authentication of the ownership of PD before access is given or correction is allowed to be done. SPH recommends that where authentication cannot reasonably be carried out, organisations should have the right to deny access or reject any request for correction by a consumer. In addition, the PDPA should also provide for a mechanism to deter frivolous or vexatious requests from individuals.

9.3 We note that in the Hong Kong Personal Data (Privacy) Ordinance ("PDPO") and the UK Data Protection Act ("UK DPA"), procedural steps have been implemented to ensure that data access requests are not too onerous for organisations to comply with.

9.4 Under the PDPO, certain situations are provided for in which the organisation may refuse to comply with a data access request:

(a) where the organisation 'is not supplied with such information as the [organization] may reasonably require in order to satisfy the [organisation] as to the identity of the requestor;'[2]

(b) where the request is not in writing in the English or Chinese language, the organization is not supplied with such information as the organisation may 'reasonably require to locate the personal data to which the request relates', and the request follows two or more similar requests made by the individual who is the data subject in respect of personal data to which the request makes, and 'it is

[2] Section 20(1)(a)(i) PDPO.

unreasonable in all the circumstances for the data user to comply with the request; [3]

(c) where the commissioner has specified that the access request should be made in a particular form, and the request has not been made according to that form.[4]

9.5 Under the UK DPA, an organisation is not obliged to supply any information in response to an access request unless the request is made in writing and such fee as he may require has been paid.[5] Furthermore, an organisation is 'not obliged' to comply with the access request unless he is supplied with further information, where the organisation 'reasonably' requires such further information in order to satisfy himself as to the identity of the person making the access request and to locate the information which that person seeks, and has informed him of this requirement.[6]

9.6 Thus, in these countries, access rights of individuals are prefaced with procedural requirements. It is submitted that MICA should consider the implementation of similar procedural steps in PDPA as such procedural steps would aid in restraining frivolous requests, and provide organisations with the right to refuse access to PD on certain grounds. This in turn will ease the burden of compliance. For example, in the UK, the duty to supply information to the individual is subject to the principles of proportionality, or the individual agreeing otherwise.

9.7 In addition, we note that the PDPO provides for adequate deterrent for individuals to make frivolous or vexatious requests. There is a provision for punishment of individuals who provide false or misleading information to organisations in a data access request.[7]

9.8 Finally, it is important that any access or correction rights of an individual to his or her PD, should not unduly burden the organisation, such as disrupting its business operations and causing administrative burden or additional costs. For example, under the UK DPA, the obligation to provide the data subject with a copy of the personal data being processed need not be complied with if the supply of such a copy would involve disproportionate effort or is not possible,[8] or the data subject agrees otherwise.[9]

9.9 We believe that the UK DPA approach strikes an appropriate balance between the interests of individuals and organisations. Our PDPA should likewise provide for an option to 'opt-out' of the access and correction rights. Since the concept of consent in relation to collection, use and disclosure under the PDPA is subject to the principles of proportionality and there is also a right for consent to be withdrawn, the individual's

---

3 Section 20(3) PDPO.

4 Section 20(3)(e) PDPO.

5 Section 7(2) UK PDPA.

6 Section 7(3) UK PDPA.

7 Section 64(2) PDPO.

8 Section 8(2)(a) UK PDPA.

9 Section 8(2)(b) UK PDPA.

interests would still be served if this right of consent can be extended to non-access of PD.

E. Part VI – Care of Personal Data

10. Section 26 – Protection of Personal Data

10.1 SPH agrees that it is important for organisations to ensure the security of the PD.

10.2 However, MICA should be cognisant of the fact that despite the greatest of effort and will, the most secure information technology system may be breached. High-profile examples of such breaches have found their way in the newspapers, notable amongst them being the Wikileaks. Hence, SPH would advocate that organisations should not be held culpable or punished if such inadvertent breaches or disclosures of PD were to occur.

10.3 The PDPA should also adopt a safe harbour framework that protects organisations from liability if the violation was made inadvertently and the organisation can demonstrate that they had written procedures and policies in place to monitor and prevent unauthorised collection, use and disclosure of PD. This is also considered in the next section.

F. Part VII – Enforcement of Part III to Part VI

11. Section 28(3) – Guidelines on Enforcement

11.1 Section 28(3) states that where the guidelines would apply to an industry or a sector of industry that is subject to the regulation and control of another regulatory authority, the DPC shall, in preparing those guidelines, consult with that regulatory authority.

11.2 SPH welcomes this consultative approach adopted by the PDPA. However, the PDPA does not spell out the consequences of what follows if such a consultation did not take place and the guidelines turn out to be at odds with the regulations of the regulatory authority. For instance, the current voluntary Code of Ethics put out by the Contact Centre Association of Singapore, with its comprehensive list of guidelines and the establishment of DNC lists in organisations, also adequately allows individuals who do not wish to have unsolicited telemarketing calls an avenue to object to it. Section 4(7) talks about other written laws prevailing over the PDPA. It is not too clear whether the same principle applies to guidelines. Hence as earlier suggested, SPH submits that an informal guidance regime be introduced whereby organisations may seek clarification and guidance from the DPC.

11.3 In this context, we would also bring to MICA's attention that the HK PDPO provides for such a consultative framework in greater detail. Under the PDPO, the commissioner's duties and functions include assisting bodies representing organisations to 'prepare codes of practice for guidance in complying with the provisions' of the PDPO, 'in particular the data protection principles'[10]. The commissioner also has an express duty to 'examine any proposed legislation that the commissioner considers may affect the privacy of individuals…and report the results of the examination to the person proposing the legislation'[11].

[10] Section 8(1)(b) PDPO

[11] Section 8(1)(d) PDPO

11.4 Similarly under the UK DPA, the commissioner has a general duty to 'give advice' to persons on 'good practice' in relation to the UK DPA. The UK DPA also provides for the commissioner to, 'with the consent of the organisation, assess any processing of the personal data for following of good practice'[12].

11.5 As seen above, the duties of the commissioner in relation to providing advice or codes of practice under these legislations are more specific and explicit than currently provided for under the PDPA. It is suggested that greater clarity in the express scope of the DPC's duties, particularly in the provision of advice or drafting codes of practice, would be a great aid to organisations in complying with the PDPA.

11.6 It is also suggested that the PDPA should introduce an option of voluntary evaluation, where the DPC may provide guidance on PDPA compliance and immunities against prosecution where the company has acted in accordance with the guidance of the DPC. Combined with the provision of clear codes of practice, these would be good methods of ameliorating the harshness of enforcement regime for contravention of the PDPA.

12. Section 30 – Power to review and Section 31(2)(d) – Power to give directions

12.1 Section 31(2)(d) stipulates a maximum financial penalty of S$1 million for a breach of the PDPA. In SPH's view, this is too high. SPH advocates that any financial penalty should be imposed only for repeated offences, when notice for compliance has been given and there was flagrant and deliberate breach of the PDPA.

12.2 SPH would also like to suggest that the DPC be given the powers to review or reconsider the corrective measures that an organisation may have taken and for the framework to allow an organisation to submit a request for reconsideration or review ("Reconsideration Request") where the organisation feels aggrieved by any act, direction or decision of the DPC. In this way, it ensures that the enforcement process is flexible and fluid, and that there is an avenue for the DPC to address concerns that the corrective measures are unnecessary, burdensome or unduly broad.

12.3 We would also submit that the PDPA should mirror the checks and balances on enforcement found in other privacy acts.

12.4 For example, under the UK DPA, prior to the imposition of a monetary penalty, the commissioner serves an 'enforcement notice' on the organisation[13] specifying such steps that must be taken by the organisation to rectify any contravention of the data protection principles[14]. Furthermore, a test is built into the statute to ensure that an enforcement notice is only served where the commissioner considers that 'the contravention has caused or is likely to cause any person damage or distress'[15].

---

12 Section 51(7) UK PDPA

13 Section 40 UK PDPA

14 Section 40(1) UK PDPA

15 Section 40(2) UK PDPA

12.5 Further, monetary penalties are only imposed if the commissioner is satisfied that[16]:

(a) there has been a 'serious contravention' of the data protection principles;

(b) the contravention was of the kind likely to cause substantial damage or substantial distress; and

(c) the contravention was deliberate; or

(d) the organisation knew or ought to have known that there was a risk that the contravention would occur and that the contravention would be of a kind likely to cause substantial damage or substantial distress but failed to take reasonable steps to prevent the contravention.

12.6 In addition to the above, the organisation has also been conferred express rights of appeal against the commissioner's decisions[17]. Similar provisions are found in the Hong Kong PDPO[18].

12.7 We note that section 31 of the PDPA empowers the DPC to give directions to organisations in the event of non-compliance. However, it is submitted that there is ambiguity in the current language with regard to how the DPC will arrive at the decision that the organisation is not compliant and fix the appropriate penalty. SPH believes that MICA should consider implementing express procedural steps to allow for greater transparency in the regime. It is also suggested that MICA consider inserting express thresholds, such as the test under the UK DPA, which must be met prior to the imposition of the financial penalty.

13. Section 33 – Power to Investigate or Conduct Inquiry

13.1 In addition to the comments above on the enforcement regime, in assessing a complaint, the DPC should also consider factors such as the number of complaints and the potential for repeated offences.

13.2 SPH suggests that there should also be a provision that if an organisation which is subject to investigative or enforcement action by the DPC, but which is also regulated by another regulatory body, the organisation may request or submit to the DPC that its actions are to be more appropriately investigated by that regulatory body.

14. Section 35 – Offences and Penalties

14.1 SPH feels that as a deterrent, there should be a corresponding provision in the PDPA to punish individuals who make frivolous and vexatious complaints against organisations. Otherwise, organisations may end up having to defend its actions to the DPC very often, and incur unnecessary costs and time in doing so.

---

16 Section 55A UK PDPA

17 Section 55B(5) UK PDPA

18 Section 50 PDPO

14.2 As mentioned before in paragraph 10.3, the PDPA should also have a safe harbour provision that protects organisations from liability if the violation of the PDPA was made inadvertently. Incorporating this provision will relieve organisations that have genuine reasons for inadvertence, of the strenuous consequences of a breach of the law.

15. Section 36 – Right of Private Action

15.1 We note that Section 36 confers on individuals a right of private action.

15.2 As in our earlier submission, SPH does not agree that the PDPA should provide that individuals may separately seek redress via civil proceedings in court. It is submitted that there is no need to provide for such a right. At law, the law of confidence already provides remedies for unauthorised disclosures of confidential information, and further, in relation to the PDPA, the DPC can impose financial penalties and prosecute offences.

15.3 If, on top of this framework, private individuals have a right of private action, there is potential for the floodgates of litigation to be opened, bringing about the risk of significant resource drains and also increasing the cost of compliance. Corporations may be faced with the prospect of having to settle frivolous and vexatious claims before they go to court to minimise business disruption (and bearing in mind also the prospect of criminal prosecutions), but may in turn become victims of "extortion" and encourage further litigation.

15.4 In this regard, we would also highlight that the statutory right of private action does not appear as such in the data protection legislations of major countries, including UK, Hong Kong and Australia.

15.5 For example, in the UK, there are limits to claims for compensation, eg. the data controller had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned. Distress is only claimable where the individual has suffered damage or there was processing for special purposes. In Hong Kong, a claim for compensation must relate, whether in whole or in part, to personal data of which that individual is the data subject, and further, it is a defence to show that such care as in all the circumstances was reasonably required to avoid the contravention concerned, or in any case the contravention concerned occurred because the personal data concerned was inaccurate, the data accurately recorded data received or obtained by the data user concerned from the data subject or a third party.

15.6 Clearly, therefore, there is no established norm that there must be a private right of action for privacy-related breaches as such, and hence we urge MICA not to provide such a right of action, particularly given that the PDPA will be a new regime.

15.7 If indeed MICA feels otherwise, then there should be a corresponding provision in the PDPA to punish individuals who make frivolous and vexatious complaints against organisations – much like there are groundless threat actions in various intellectual property statutes in Singapore to deter groundless claims of infringement, otherwise private individuals will feel little pressure not to "try their luck" with litigation.

15.8 There should also be a limitation period within which complaints may be brought by individuals against the organisation for alleged contraventions of the law – this should also be short, say no later than 1 year after the breach (as in Hong Kong in respect of the limited rights to seek compensation), having regard to the huge amounts of audit trails

that corporations may need to maintain to defend against any potential complaints which may surface in the future.

G. Part IX – Do-Not-Call Register

16. Section 40 – Interpretation of this Part

16.1 Section 40 is the interpretation section for Part IX on Do-Not-Call ("DNC") Register. Although the PDPA uses the term "specified message", the scope of this term tracks closely the definition of a "commercial electronic message" in the Spam Control Act but with a significant difference – in the latter, a commercial electronic message is one where the **primary purpose** of the message is the offer of goods or services or to advertise or promote the same.

16.2 Under the PDPA, as long as "**the purpose, or one of the purposes**" of the message is the offer of goods or services or to advertise or promote the same, it would constitute a "specified message".

16.3 The Spam Control Act definition is less stringent in that it will permit for incidental marketing messages, and it would appear there was a conscious decision on the part of the Singapore Government to allow for this. Even though our Spam Control Act appears to have been based on the Australian Spam Act, we adopted the "primary purpose" definition. We note also that Hansard discussions on the Spam Control Bill emphasised balancing the needs of consumers and businesses, and the need for a light touch approach, so that the burden placed on businesses would not be so onerous. Indeed SPH would argue that similar considerations should apply to the PDPA and that the definition of "specified message" should apply the "primary purpose" test, and there is no logical distinction why the Spam Control Act and PDPA definitions should differ on this point.

16.4 On a related note, the Tenth Schedule provides that if the sole purpose of a message is to conduct market research or market survey, such message is excluded from the meaning of a "specified message". This suggests a market research/survey message which contains one or more marketing elements will not be considered as a specified message if the sole purpose is for market research/survey. If SPH's suggestions in the preceding paragraph are adopted, this will obviate the need for such complexity in the statutory language of the PDPA. Alternatively if MICA insists otherwise, then SPH would like to propose that the PDPA specifically states that all market research and survey will not be considered as specified messages even if contains some marketing elements.

16.5 Section 40 also defines "goods" and "services". "Goods" means personal property, residential property as well as vouchers specifically. The word "vouchers" is not defined and it begs the question of why it is singled out in the definition and why it is not considered as "personal property". SPH would like to seek clarification on the significance of "voucher" in the definition of "goods".

16.6 The definition of "services" includes financial services, repairing residential property to club membership and time share. The use of the word "includes" instead of "means" seems to tell us that services can cover more than those listed in the definition. This creates an ambiguity and seems out of sync with the other definition terms, except for "voice call" which also uses the word "includes" and not "means". SPH submits that it will

be clearer and less confusing if "includes" is changed to "means" for both definitions and if necessary, both definitions should be extended to cover the full scope.

17. Section 41(3) – Meaning of "specified message"

17.1 While Section 40 defines "goods", Section 41(3) uses the word "product" instead of "goods", whereas other provisions in the same section mentions "goods" instead. This causes some confusion and SPH seeks clarification whether "product" has the same meaning as "goods" and if so, perhaps the term "goods" should be used instead.

17.2 The language of sections 41(3) and 41(4) also needs to be re-examined. It should not be the case that a person who knowingly allows his product or service to be advertised or promoted should be deemed to also have authorised the sending by the sender of any message that advertises or promotes that person's product or service. The threshold for such liability is set too low, and surely the person must at least knowingly allow the sending of specified messages before he should be deemed to have so authorised?

17.3 In any event, section 41(4) suggests that it is only where a person takes "reasonable steps" to stop the sending of any message referred to in that subsection would he be relieved of liability under section 41(3) – but this assumes that the person will in fact have control of the sender.

17.4 This is not invariably the case – for example, if a newspaper delivery service sends specified messages advertising home delivery services for SPH's newspapers, SPH should not have liability for these specified messages unless it had specifically authorised the sender to issue such messages on its behalf. We can also envisage situations where say magazines or books from SPH's publishing arms are purchased by end retailers through wholesalers and the specified messages are sent by the end retailers. SPH may not have any contractual privity with such retailers and would not be in a position to take the reasonable steps referred to in section 41(4), yet the language of sections 41(3) and (4) may be broad enough to impose liability on SPH.

17.5 Given these practical concerns, SPH would request that MICA considers removing sections 41(3) and (4), and leave such matters to ordinary rules of evidence and proof in any prosecution. It is also submitted there will not be in fact a need to trace upwards as seems to be the effect of sections 41(3) and 41(4), as the primary party sending the specified messages will always be identifiable, and prosecution of that party will already achieve the objectives of deterring specified messages being made without consent.

18. Section 44 – Application

18.1 SPH understands that the DNC regime (as with the PDPA) is intended to focus on protecting individuals. Allowing business numbers to be put on the DNC register appears to be incongruent with this objective. As such, SPH believes that Singapore should follow the regime in the United States of America which does not permit businesses to place their phone numbers on the DNC register. Besides, SPH believes that businesses in Singapore should have adequate resources and avenues to prevent or reduce unsolicited marketing messages. To include business numbers on the DNC register is likely to hinder business-to-business vibrancy and should not be recommended in Singapore's fairly young and developing business environment.

18.2 We understand that in the UK, the DNC concept is provided for by the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Privacy and Electronic Communications (EC Directive) Regulations (Amendment) 2004 ('2004 Amendments'). While businesses are able to place their numbers on the DNC List, the numbers are not retained indefinitely. An email reminder is sent to the business on a yearly basis, thus providing businesses with the opportunity to reconsider their decision regularly, thus balancing both the need for business vibrancy and restrictions on unwanted telemarketing calls.[19]

18.3 SPH would also like to suggest setting an expiry period of two years for each number registered. Setting an expiry date would give individuals a chance to re-consider their original decision to opt out. If left alone, it is likely that most of us would not remember or bother to deactivate our registration from the DNC register. Giving the chance for re-consideration helps businesses to expand their base of potential clients as consumer preferences shift and new products and services emerge.

19. Section 47 - Duty to Check Register

19.1 This Section requires an organisation to filter the numbers with the DNC Registry before sending out messages. However, there is no provision stating the deadline by which the DPC is to revert with confirmation or otherwise. SPH requests that such a provision be included.

H. Part X – General

20. Section 50 – Offences by bodies corporate, etc, Section 51 – Liability of Principals, Agents, Employers and Employees

20.1 For reasons raised in our discussion above on Section 13, SPH would recommend that relevant portions of Section 50 and Section 51 be deleted accordingly.

21. Small-quantity Number Lookup Service

Paragraph 2.174 of the consultation paper (page 40) states that MICA will include a small quantity number lookup service as one of the features of the DNC Registry.

SPH feels that it remains unclear what this small quantity number lookup service entails. In MICA's earlier consultation paper, it was clarified that this service was for organisations with small scale marketing operations such as small & medium enterprises for a nominal fee or for free. SPH would like to suggest that the PDPA should provide for this clearly.

D. CONCLUSION

SPH would like to thank MICA for the opportunity to participate in the public consultation exercise for the draft PDPA bill. We hope MICA will look into our feedback and the issues raised and address them accordingly.

As raised in this submission, the language of the PDPA still needs some clarification. It would be useful if the PDPA itself can contain illustrations or scenarios under certain sections to demonstrate the scope and application of those sections. On top of that,

[19] Regulation 2(4) of the 2004 Amendments

guidelines and practice directions would also be welcome. Most importantly, SPH requests that MICA reviews the enforcement framework to have more balance between the interests of individuals and organisations.

Please do not hesitate to contact the undersigned (email: limmlg@sph.com.sg) if you have any queries or require any clarification.

Yours faithfully

Ginney Lim May Ling (Ms)
General Counsel,
Executive Vice President,
Corporate Communications &
Group Company Secretary