BAKER & MCKENZIE.WONG & LEOW

Baker & McKenzie. Wong & Leow
(Reg. No. 200010145R)

8 Marina Boulevard #05-01
Marina Bay Financial Centre Tower 1
Singapore 018981

Tel: +65 6338 1888
Fax: +65 6337 5100
www.bakermckenzie.com

30 April 2012

By email:
MICA_DP_Bill_Consultation@mica.gov.sg

Ministry of Information, Communications and the Arts

Dear Sirs

Public Consultation on the Proposed Personal Data Protection Bill

We refer to the public consultation paper on the proposed personal data protection bill issued by the Ministry of Information, Communication and the Arts on 19 March 2012.

We have been keenly following the development of the framework for the proposed data protection law and the national do-not-call registry, and we are pleased to set out under cover of this letter our comments on the proposed personal data protection bill.

We thank you for giving us the opportunity to provide feedback on the proposed personal data protection bill, and we hope that our input would prove useful.

Please do not hesitate to contact the undersigned should any clarification be required.

Yours faithfully,

See Khiang Koh
Senior Associate
+65 6434 2651
see.khiang.koh@bakermckenzie.com

Encl

TABLE OF CONTENTS

1. SUMMARY OF MAJOR POINTS

1.1 In the next section, we have set out our concerns on the following areas of the proposed Personal Data Protection Act ("**PDPA**"), based on the draft bill annexed to the consultation paper ("**Consultation Paper**") issued by the Ministry of Information, Communications and the Arts ("**MICA**") on 19 March 2012:

(a) Proposed application of the proposed PDPA to data with a Singapore link;

(b) Interface between "data intermediary" and "data controller";

(c) Clarity as to what constitutes "use" of personal data;

(d) Whether implied consent constitutes valid consent;

(e) Restrictions on use of existing personal data;

(f) Exclusion for managing or terminating an employment relationship;

(g) Definition of "specified message" for the purposes of the national do-not-call ("**DNC**") registry;

(h) Interaction between the proposed PDPA and the *Spam Control Act*; and

(i) Consent as a defence to breach of duty to check register.

1.2 We have also set out our comments on other minor drafting issues in the proposed PDPA for your kind consideration.

2. COMMENTS

2.1 Given that this is already the third stage of the public consultation process, we do not intend to reopen any of the issues for which a policy position has already been established, or undertake an exhaustive review the proposed PDPA. However, we wish to set out our concerns regarding the following areas of the proposed PDPA, in the hope that these concerns may be addressed prior to the enactment of the proposed PDPA.

<u>Proposed application of the proposed PDPA to data with a Singapore link</u>

2.2 In the Consultation Paper, MICA suggested that the ambit of the proposed PDPA would be extended to organisations that are not physically in Singapore, to the extent that they are engaged in the collection, use or disclosure of personal data within Singapore. This is reflected in the drafting of the proposed PDPA in section 5(2)(a)(ii) and sub-paragraph (i) of sections 5(2)(b) to 5(2)(e) (as well as sub-paragraph (ii) to the extent that it refers to section 5(2)(a)(ii)).

2.3 It appears logical that personal data collected, used or disclosed within Singapore would constitute data with a "Singapore link", and therefore arguably defensible that the organisation responsible for such collection, use or disclosure should be required to comply with the proposed PDPA. However, it is submitted that practical difficulties may arise in the absence of further guidance regarding what constitutes collection, use or disclosure within Singapore.

2.4 In particular, it is not clear to us why the location of the personal data at the time of collection (i.e. the factor set out in section 5(2)(a)(ii)) should determine whether the requirements of the

proposed PDPA would apply. For example, would an organisation in, say, the U.S. collecting personal data from residents in the U.S. through a website that is not available to residents from other countries (including Singapore) be required to comply with the proposed PDPA merely because the server hosting the personal data collected is located in Singapore? Conversely, would an organisation in Singapore collecting personal data from individuals outside of Singapore online fall outside of the ambit of the proposed PDPA, if the server storing the personal data collected is located outside of Singapore?

2.5 Equally, if the current drafting of the proposed PDPA is to be maintained, further clarity regarding what constitutes "use" and "disclosure" of personal data in Singapore would be required. We note that these factors are pegged to the location in which the activity takes place, as opposed to the location of the personal data in the case of collection. In that sense, it appears likely that the organisation concerned would need to have some sort of presence in Singapore, whether through a local subsidiary or a local data intermediary.

2.6 Further, the application of section 5(2)(a)(i) (i.e. personal data is collected from an individual who is physically present in Singapore at the time of collection) is likely to give rise to even greater difficulties. The only explanation for this provision in the Consultation Paper is found in the following sentence, which appears immediately after the proposal to extend the application of the proposed PDPA to foreign organisations engaging in the collection, use and disclosure of personal data in Singapore: '*For example, overseas organisations engaged in data collection activities online and collection of personal data from a person in Singapore will be covered under the PDPA.*'

2.7 With due respect, we would submit that the two factors are in fact quite distinct, and that the physical location of an individual within Singapore at the time of data collection does not constitute a reasonable nexus to Singapore. This can be illustrated with the following hypothetical scenarios:

(a) An individual normally residing in Singapore is on vacation, and while abroad, he accesses the website of a local company to purchase some items, and submits his personal data during the checkout process. Assuming that this data is collected and stored on a server located outside of Singapore, it appears (see above) that this data does not have a Singapore link and the local company does not have to comply with the proposed PDPA in respect of this data.

(b) An individual normally residing in Australia is passing through Singapore, and while in transit at Changi Airport, she accesses the website of a company in Australia to purchase some items, and submits her personal data during the checkout process. It would appear that this data does have a Singapore link, and that the relevant Australian company would thereby be subject to the requirements of the PDPA.

2.8 We hope that the examples given above serve to illustrate that a literal reading of sections 5(2)(a)(i) and 5(2)(a)(ii) may potentially lead to unintended consequences. This is particularly important since sub-paragraph (ii) of sections 5(2)(b) to 5(2)(e) refer back to section 5(2)(a) (i.e. an organisation collecting personal data falling within section 5(2)(a) would be required to comply with all relevant requirements in the proposed PDPA).

2.9 The application of these provisions would also impose unnecessary administrative overheads on both local as well as foreign organisations, since they would have to assess whether the proposed PDPA would apply in respect of certain personal data in their custody or control on the basis of:

(a) the location of personal data at the time of collection;

(b) the location of the data subject at the time of collection; or

(c) the location in which the use or disclosure of the personal data takes place.

2.10 In summary, while we understand the rationale for extending the ambit of the proposed PDPA to foreign organisations insofar as they deal in personal data with a Singapore link, we are of the view that the current drafting of section 5(2) is apt to confuse, and may lead to illogical outcomes. We would recommend that all relevant organisations based in Singapore are subject to the proposed PDPA, regardless whether the personal data is collected from an individual physically in Singapore, and whether the personal data is used or disclosed in Singapore. This would be similar to the position under the Model Data Protection Code for the Private Sector ("**Model Code**").

2.11 Foreign organisations should be subject to the proposed PDPA only if:

(a) they are dealing with personal data from individuals that are resident or domiciled in Singapore; or

(b) the relevant processing activity actually takes place in Singapore.

The location of the personal data and the data subject at the time of collection is somewhat arbitrary and should not form the basis for determining whether the proposed PDPA applies.

Interface between "data intermediary" and "data controller"

2.12 The Consultation Paper has introduced the concept of a "data intermediary", being an organisation which processes personal data on behalf of another organisation. Data intermediaries are essentially exempt from complying with the relevant provisions in the proposed PDPA, except for section 26 on the protection of personal data through reasonable security arrangements.

2.13 We support the approach described in the foregoing paragraph, and note that the relationship between organisations and data intermediaries under the proposed PDPA is similar to the relationship between data controllers and data processors in many other jurisdictions with established data protection regimes (e.g. under the EU data protection framework). However, the fact that the distinction between organisations and data intermediaries under the proposed PDPA is not pegged to "control" may potentially give rise to certain issues.

2.14 For example, while a data intermediary (e.g. a call centre) may be processing certain personal data (e.g. telephone numbers of prospective clients) on behalf of another organisation, the data intermediary will likely be the data controller in respect of other personal data in its possession (e.g. information on its own employees). This is not an issue under the proposed PDPA to the extent that the exemption mentioned only applies in respect of '*personal data processed by the data intermediary on behalf of another organisation pursuant to a contract which is evidenced or made in writing.*' Our only comment in this regard is that the rationale for the inclusion of the contract requirement is not immediately apparent, unless the proposed PDPA intends to regulate certain aspects of such agreement.

2.15 More pertinently, it should be recognised that in certain cases a data intermediary may well have some measure of control over the purposes for which the personal data is processed, or the means by which such processing takes place. Such a data intermediary would be more

accurately considered a joint data controller[1], and we would suggest that the exemption mentioned above should not apply to such a data intermediary. In the event that MICA is minded to give effect to this recommendation but does not wish to make substantive amendments to the existing definition of a data intermediary, it may wish to consider adding the following proviso to section 4(2) of the proposed PDPA: '*... pursuant to a contract which is evidenced or made in writing, to the extent that the data intermediary does not determine the purposes for which the personal data is processed, and the means by which such processing takes place*.'

Clarity as to what constitutes "use" of personal data

2.16 Part IV of the proposed PDPA essentially seeks to impose a legal requirement on relevant organisations to obtain consent from individuals for the collection, use and disclosure of their personal data. Putting aside the question of what type of consent is required for the time being, we note that there is no definition in the proposed PDPA as to what would constitute the collection, use and disclosure of personal data, for which consent must be sought.

2.17 In this regard, while we accept that the activities denoted by the words "collection" and "disclosure" are tolerably clear such that no definition may be required, we are of the view that the word "use" would benefit from further elucidation. For example, it may be argued that the mere storage or transmission of personal data would not, in the normal usage of the term, constitute "use" of the personal data. Does this imply that no consent is required if a relevant organisation in Singapore is merely transmitting personal data to another entity overseas?

2.18 The situation is further complicated by the use of the phrase "processing" of personal data in the proposed PDPA. Processing, in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, including the following list of operations set out in section 2:

(a) recording;

(b) holding;

(c) organisation, adaptation or alteration;

(d) retrieval;

(e) combination;

(f) transmission; or

(g) erasure or destruction.

2.19 Interestingly, the word "processing" is only used in section 4 in defining the scope of the proposed PDPA. Thus, for example, the proposed PDPA does not apply to a public agency or an organisation acting as its agent in the processing of personal data. As previously mentioned, a data intermediary is not required to comply with the relevant provisions of the proposed PDPA to the extent that it is processing personal data on behalf of another

[1] See for example the opinion of the Article 29 Working Party on the role of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) in processing personal data on behalf of financial institutions (01935/06/EN WP128), as well as the Article 29 Working Party's subsequent opinion on the concepts of "controller" and "processor" (00264/10/EN WP 169).

organisation. Conversely, an organisation is required to comply with the proposed PDPA in respect of personal data processed on its behalf by a data intermediary.

2.20 It is not clear how the terms mentioned above relate to each other. Does the collection or disclosure of personal data constitute the processing of personal data? If not, does that imply that an organisation that is merely collecting or disclosing personal data on behalf of another would not be considered a data intermediary, and would thus be subject to the relevant provisions in the proposed PDPA?

2.21 Further, would the use of personal data constitute processing of the personal data (or *vice versa*)? It would appear from the slides presented during the industry sharing session conducted on 30 March 2012 that the word "use" is intended to encompass the "processing" of personal data. However, we would suggest that a better approach may be to:

(a) clarify that the processing of personal data encompasses the collection, use and disclosure of personal data, and

(b) use the term "processing" of personal data rather than "use" of personal data, to the extent possible.

We are of the view that beside enhancing the clarity of the proposed PDPA, such an approach would also be more consistent with the convention adopted in other jurisdictions with an established data protection tradition.

Whether implied consent constitutes valid consent

2.22 Once the proposed PDPA takes effect after the sunrise period, the collection, use or disclosure of personal data will be illegal unless:

(a) the individual concerned gives, or is deemed to give, his/her consent to the organisation; or

(b) the collection, use or disclosure of personal data without consent is authorised under the proposed PDPA or other applicable laws.

Unlike ordinary consent under the proposed PDPA, "deemed consent" under section 17 does not depend on the organisation providing the individual with specific notification regarding the purposes for which the personal data will be processed (per section 22(3)(a)). It is arguable that the interests of the individual are protected by the other safeguards that are in place (e.g. in order for the deeming provision to apply, the individual must voluntarily provide the personal data to the organisation and this must be reasonable).

2.23 While we express our support for the inclusion of the deemed consent route and acknowledge that the proposed PDPA should not be overly-prescriptive on the manner in which consent may be given, we would like to seek confirmation on whether implied consent can constitute valid consent under the proposed PDPA. In this regard, we note that paragraphs 2.49 and 2.50 of the Consultation Paper discusses whether failure to opt out should be held to constitute deemed consent, and MICA opined that '*consent should generally not be deemed when individuals are notified of an organisation's intent to collect, use or disclose their personal data, but do not object within a reasonable timeframe.*'

2.24 While we do not disagree with this position, we note that deemed consent is unlikely to be applicable in the first place given that we are more likely to be dealing with a situation where the organisation can collect the personal data without the individual's involvement, rather

than one where the individual voluntarily provides it to the organisation. We are of the view that the more pertinent question in this case is whether the inaction of the individual can be held to constitute implied consent, and whether such implied consent can constitute valid consent under the proposed PDPA.

2.25 We note that MICA does recognise in paragraph 2.50 of the Consultation Paper that '*there may be instances where consent may be implied through an individual's action or inaction*' and that there is no requirement for consent to the collection, use or disclosure of personal data to be "explicit" (unlike consent for an organisation to contact an individual on the DNC register under section 47(3)(b)). Nevertheless, we would recommend that this is made clear in the proposed PDPA by the addition of the words "whether express or implied" after the word "consent" in section 16(1)(b).

2.26 The significance of such clarity extends beyond situations where there is a failure to opt out. For instance, most websites collect a fair amount of personal data from users, in certain cases without the users actively submitting such information to the website (e.g. through the use of cookies or web beacons). The collection, use and disclosure of such personal data is typically regulated through the privacy policy of the relevant website, which would generally describe the information-gathering practices of the website and the purposes for which such information may be processed. In most cases, the user's acceptance of such privacy policy is implied by the mere fact that the user continues to visit or use the website after being notified of the privacy policy. We trust it is not MICA's intention that the common practice described above should be outlawed under the proposed PDPA, since it is often impractical for explicit consent to be sought from all users.

Restrictions on use of existing personal data

2.27 In paragraph 2.139 of the Consultation Paper, MICA sets out its proposal for the treatment of existing personal data in the possession of relevant organisations before the "appointed day" (i.e. when the relevant restrictions in the proposed PDPA kick in). MICA proposes that organisations should be allowed to continue using such personal data for reasonable existing purposes, taking into account the nature of the organisation's business. There is no need to obtain fresh consent from the individuals concerned unless the organisation intends to use the personal data for a new purpose, or for purposes beyond what would be considered reasonable.

2.28 We are of the view that the above proposal is eminently reasonable, and strikes the right balance in reducing the compliance cost imposed on organisations and fulfilling the consumer protection objectives of the proposed PDPA. However, we note that the proposal does not appear to be fully reflected in the drafting of the proposed PDPA. The relevant part of section 21 of the proposed PDPA merely states:

> '*Notwithstanding the other sections in this Part, an organisation may use personal data collected before the appointed day for the purposes for which the personal data was collected…*'

2.29 We would recommend that it should be clarified in section 21 that the purposes for which the personal data was collected should be reasonable (section 20(a) does not appear to apply given the opening words of section 21). Otherwise, the organisation would arguably have *carte blanche* in processing the personal data inconsistently with the proposed PDPA, simply because it had been processing the personal data that way prior to the appointed day. While this may be considered implicit in the drafting, it may also bear repeating that the organisation would have to comply with the relevant provisions of the PDPA (including seeking consent

from the individual) to the extent that it wishes to use existing personal data for other purposes or for purposes beyond what would be considered reasonable.

2.30 Likewise, it may be worth clarifying that the obligations in the other Parts of the proposed PDPA would apply to existing personal data. As such, the organisation should provide individuals with the opportunity to access and correct their personal data, whether such personal data is collected before or after the appointed day. The organisation should ensure that existing personal data remains accurate and secure existing personal data with reasonable security measures. Finally, the organisation should destroy or anonymise existing personal data once retention is no longer required for the purposes for which the existing personal data was collected, or for legal or business purposes.

Exclusion for managing or terminating an employment relationship

2.31 The Third Schedule of the proposed PDPA contains an exclusion in respect of the collection of personal data by an organisation for the purpose of managing or terminating an employment relationship between the organisation and its employees. No consent from the individual employee is required in respect of such collection provided that:

(a) the collection is reasonable for that purpose set out above; and

(b) the organisation has notified the employee of that purpose and the business contact of its designated representative in accordance with section 22(4).

2.32 Our first observation is that the exclusion only appears in the Third Schedule of the proposed PDPA (on collection of personal data without consent), and not the Fourth Schedule (on use of personal data without consent) or the Fifth Schedule (on disclosure of personal data without consent). It is not clear if there is any reason for the absence of the exclusion in the Fourth Schedule and the Fifth Schedule, but we note that this appears to be inconsistent with section 22(4), which suggests that the exclusion should apply towards the collection, use and disclosure of the employee's personal data. This is also acknowledged in paragraph 2.69 of the Consultation Paper, where MICA stated:

> '*Organisations may still collect, use or disclose personal data without consent (but with notification) for the purposes of managing or terminating an employment relationship.*'

2.33 It is also not clear how the notification requirement mentioned above would apply in practice, given the potential overlap between this exclusion and other exclusions. For example, personal data may be collected, used or disclosed without consent of the employee to the extent that the data is necessary for "evaluative purposes", which includes the purpose of determining the suitability of the employee for:

(a) promotion or continuance in employment or office; or

(b) removal from employment or office.

Where the employee is allegedly guilty of misconduct, the organisation may also potentially seek to rely on the exclusion for personal data collected, used or disclosed for investigations (i.e. relating to breach of the employment contract) or proceedings.

2.34 Given the potential overlap, we would recommend that the notification requirement should be applied consistently. For example, it is merely a matter of semantics whether personal data was collected for terminating an employment relationship or for assessing whether an

employee should be removed from employment. If section 22(4) applies in the former case, it should similarly apply in the latter. We would therefore suggest that the notification requirement in section 22(4) should apply to all organisations in respect of the collection, use or disclosure of their employees' personal data, regardless whether the collection, use or disclosure takes place (a) with the employees' consent, or (b) without the employees' consent under one of the exclusions in the proposed PDPA.

Definition of "specified message" for the purposes of the DNC registry

2.35 From a consumer's perspective, one of the key components of the proposed PDPA is the establishment of a national DNC registry. This long-awaited feature of the proposed PDPA seeks to give consumers the right to opt out of receiving marketing calls and other communications sent using a telephone number, by registering the telephone number on the DNC registers that will be implemented pursuant to the proposed PDPA.

2.36 The DNC framework in the proposed PDPA applies in respect of a "specified message", which is defined in section 41. We note that the definition appears to be adapted from the definition of a "commercial electronic message" under the *Spam Control Act*, but contains a number of significant differences. In particular, an electronic message will only be deemed to be of a commercial nature under the *Spam Control Act* if the "primary purpose" of the message is one of the specified purposes, but a message will constitute a specified message under the proposed PDPA if "one of the purposes" of the message is one of the specified purposes.

2.37 While we acknowledge there is no compelling reason why the two definitions should be synchronised, we are of the view that it would be preferable if the drafting in the *Spam Control Act* is adopted at least in relation to this aspect of the definition of a specified message. Under the proposed PDPA, an organisation is not prohibited from sending its customers (even those registered on the applicable DNC register) a message that is non-commercial in nature (e.g. an order confirmation or a notice informing its customers of a change in its address). It would be unduly restrictive and contrary to existing business practices if the prohibition would kick in simply because the organisation includes a hyperlink to its website (which is likely to contain information regarding its products or services) or an unobtrusive marketing banner in the message, particularly since the communication would not constitute "spam" under the *Spam Control Act*.

Interaction between the proposed PDPA and the *Spam Control Act*

2.38 Similarly, while we acknowledge that the DNC framework and the framework in the *Spam Control Act* are intended to regulate different subject matter, there is no doubt that there is a significant overlap between the two regimes. In this regard, we would recommend that inconsistencies between the two regimes should be minimised to the extent possible in order to lower the compliance costs for businesses subject to requirements under both statutes.

2.39 For example, the Consultation Paper clarifies that the DNC framework in the proposed PDPA would apply to messages that are sent to a telephone number via a mobile data connection, such as instant messaging services like WhatsApp or iMessage. The Consultation Paper also clarifies that the DNC framework in the proposed PDPA would not, at this point in time, apply to messages that are not addressed to a telephone number, such as messages sent via cell broadcast. This exclusion would presumably also apply to messages pushed to a mobile device based on geo-location data, and other location-based services. We note, however, that these clarifications are not clearly reflected in the current drafting of the proposed PDPA, and would recommend that further guidance be issued if the current drafting is to be maintained.

Separately, the Government should also consider whether the ambit of the *Spam Control Act* should be clarified accordingly (e.g. whether spim should likewise be covered).

2.40 Another potential area of difficulty arises from the requirement for explicit consent before an organisation can send a specified message to an individual through a telephone number registered on the DNC registry. The *Spam Control Act* does not impose a requirement for the consent to be explicit, which implies that organisations currently sending marketing communications to their users without complying with the requirements in the Second Schedule (as the message is not "unsolicited") based on implied consent would need to obtain fresh consent if they wish to continue contacting such users without filtering out telephone numbers registered on the DNC registry.

2.41 Similarly, the interaction between an unsubscribe request under the *Spam Control Act* and the explicit consent requirement under the proposed PDPA needs to be considered. In this regard, we agree with the position set out in paragraph 4.6 of the consultation paper on the proposed framework for the DNC registry released by MICA on 31 October 2011. An individual sending an unsubscribe request to an organisation should never be deemed to be withdrawing explicit consent given for the organisation to send marketing communications to him/her on a telephone number listed on the DNC registry. Quite apart from the differences in the scope of the two statutes, we note that such an individual would likely not have given explicit consent to the organisation, since the unsubscribe requirements in the *Spam Control Act* only applies to "unsolicited" commercial electronic messages sent in bulk. Put another way, if consent for marketing communications to be sent to a telephone number registered on the DNC register needs to be explicit consent, the withdrawal of consent should be explicit as well.

Consent as a defence to breach of duty to check register

2.42 Our final substantive comment relates to the drafting of section 47(3)(b), which provides that explicit consent of the individual operates as a "defence" to the offence set out in section 47(1) (i.e. the prohibition against the sending of a specified message to a telephone number listed on the DNC registry). While this drafting achieves the result intended by MICA in practice, we would prefer as a matter of principle that the sending of a specified message to a telephone number with the explicit consent of the individual is carved out from the scope of section 47(1), such that no offence would be committed in the first place.

2.43 As a matter of principle, the current drafting in the proposed PDPA suggests that organisations have a duty to filter the entire list of telephone numbers they intend to send specified messages to against the DNC registers, regardless whether they have the explicit consent of the individuals concerned for such contact to be made. We trust that it is not MICA's intention to impose such an unnecessary administrative burden on organisations, and that the duty to check the DNC registers does not arise where the individuals concerned have provided explicit consent to the organisation.

Other minor drafting comments

2.44 We have set out some other minor comments on the drafting of the proposed PDPA below. We trust that these suggestions are self-explanatory but would be happy to provide a detailed exposition of the reasons behind each of them if required.

(a) The new definition of "personal data" in the proposed PDPA includes data about an individual who can be identified from that data and '*other information to which the organisation is likely to have access.*' We would suggest for the avoidance of doubt

that the quoted portion should read '*other information to which the organisation has or is likely to have access.*' This would be more consistent with the definition of "personal data" in the Model Code, from which this definition was derived.

(b) There is an exclusion in the Third Schedule that applies to personal data included in a document or record produced in the course, and for the purposes, of the individual employment, business or profession. We are not sure why this exclusion should be subject to the notification requirement in section 22(4), since the collection of such personal data is presumably not restricted to collection by employers.

(c) There is an exclusion in the Third Schedule that applies to personal data disclosed without consent under the Fifth Schedule. We are not sure why this exclusion should be "subject to" paragraph 3 of the Third Schedule, since that provision technically expands (rather than restricts) the operation of this exclusion.

(d) There are various exclusions in the Third, Fourth and Fifth Schedules that apply to personal data available to the public from a "prescribed source", which term is not defined in the proposed PDPA. We note that MICA wishes to retain the flexibility to update the list of prescribed sources (e.g. telephone directories) over time, and assume that further guidance regarding what constitutes a "prescribed source" will be issued after the proposed PDPA is enacted.

(e) There are various exclusions in the Third, Fourth and Fifth Schedules that apply to the collection, use or disclosure of personal data for "prescribed evaluative purposes". Given that "evaluative purpose" is already defined in the proposed PDPA, it is not clear whether the addition of the word "prescribed" implies that not all evaluative purposes will qualify for the relevant exclusion. This is especially confusing since the Sixth and Seventh Schedules contain exclusions for '*opinion data kept solely for an evaluative purpose.*' We would suggest that the word "prescribed" in the above exclusions is deleted for clarity.

(f) There are various exclusions in the Third, Fourth, Fifth and Sixth Schedules that apply to the collection, use or disclosure of personal data for the purposes of an "investigation". This is defined in the proposed PDPA to include an investigation relating to '*a breach of an agreement*'. We would suggest that this should be broadened to include investigations into possible breaches of documents which do not necessarily constitute a legal agreement, such as, in the case of employees, company policies or employee handbooks.

3. CONCLUSION

3.1 We hope that the above comments would prove useful to MICA in undertaking further review of the proposed PDPA.

3.2 Please note that the above comments represents the author's personal opinion, and do not reflect the position adopted by the firm's clients. Likewise, responsibility for any error remains with the author.