THE LAW SOCIETY OF SINGAPORE'S COMMENTS ON THE PERSONAL DATA PROTECTION COMMISSION (PDPC)'S PUBLIC CONSULTATION PAPER FOR MANAGING UNSOLICITED MESSAGES & PROVISION OF GUIDANCE TO SUPPORT INNOVATION IN THE DIGITAL ECONOMY

Executive summary

Question 1:

i. We support the joining of the DNC provisions of the PDPA and Spam Control provisions in a New Act, for a more comprehensive form of protection for individuals, subject to our views on the need for clarity on definitions, nuances and penalties.

ii. We also propose that enforcement powers be given to the PDPC to ensure that the New Act will have "bite". Administrative enforcement action should be taken only in respect of the worst offenders.

Question 2:

i. We support the proposal to extend the Spam Control Provisions to include IM identifiers.

ii. However, we propose that there be a national register for IM identifiers, instead of the de-centralised approach suggested by PDPC, so as to safeguard the interests and the privacy of consumers and the public.

Question 3:

i. We do not support the proposed reduction of the period for effecting withdrawal of consent to 10 business days.

ii. We propose that the period to effect a withdrawal of consent request remain at 30 business days.

Question 4:

i. We support the amendment to prohibit the use of dictionary attack and address harvesting software for sending of commercial messages to all telephone numbers, IM identifiers and email addresses.

ii. However, there may be some overlap with the Computer Misuse and Cybersecurity Act (CMCA). There needs to be some rationalising of the two Acts in order to ensure consistency.

iii. We are also of the view that the amendment ought to be targeted at the mischief of harvesting *public* data and not in respect of an organisation's use of address harvesting software on data it owns.

Question 5:

i. We are of the view that the B2B marketing messages exception should be still maintained in the DNC Provisions.

ii. We are of the view that it is important to properly define and specify how the B2B marketing message exception is to apply. This can be coupled with guidelines and guidance for companies and individuals alike.

Question 6:

i. While we are happy to leave the enforcement regime for the PDPC to decide, we are of the view that regardless of the type of enforcement regime implemented, the PDPC should nonetheless ensure the defendant retains his or her existing rights under the criminal enforcement regime, such as the right to be heard.

ii. We have also considered the practical implementation and process of such an administrative regime and propose that the penalties must have a deterrent effect and that there be sentencing guidelines.

Question 7:

i. We support this amendment as it would prevent third party checkers from hiding behind a "shield" of excluding liability.

Question 8:

i. We do not support the proposed prohibition as it might not be the most cost-efficient solution. Whether an organisation wants to check with the DNCR directly or with a third-party reseller should be left to market forces, which are the forces which started the resale in the first place.
ii. Further, an added prohibition would require a further need for enforcement, thereby potentially taking up more of PDPC's current resources.
iii. We propose a provision to the effect that: if it is pleaded that an organisation has obtained results of telephone numbers from a third-party database and/or resold results, such process of verification would not be a valid defence against liability for contravention of the DNC provisions.

Question 9:

i. We do not support this provision as it would shift the burden of proof onto the individual to defend himself or herself.
ii. Also, it is unfair to unsuspecting individuals whose devices are hacked as they would not even know about it until he or she is put on notice and investigated.
iii. We think that the PDPC should prove its case against an individual without the deeming provision being introduced to skip this step.

Question 10:

i. We do not support the proposed EPG framework as we have concerns that the criteria of "complex or novel", "cannot be addressed by PDPC's general guidance and existing published resources" and "does not amount to a request for legal advice" are difficult to apply in practice.
ii. It is also equivocal whether the EPG would be legally binding.
iii. Lastly, the EPG may never be exhaustive enough as every case will have its own unique facts.

Feedback On Exceptions to Consent

We propose that the current exception for consent for use of personal data for research purposes (Third Schedule, paragraph 1(i) read with Paragraph 2; and Fourth Schedule, paragraph 1(q) read with paragraph 4), (collectively, the "**Research Exception**") be refined as there are issues as to the scope / applicability of the Research Exception, and as to the difficulty of applying the Research Exception.

We also provided feedback on reforming the exception as it relates to disclosures to public agencies in the public interest, and proposed amendments to make it easier for organizations to apply the exception.

Issue 1: Scope of Research Exception

We propose either a definition of research which carves out "service improvement" type uses of personal data from "research" under the PDPA, or, alternatively, to classify all uses of data in this spectrum as research purposes.

Issue 2: Criteria for the Research Exception

We propose reforming the Research Exception along the following lines:

a. Organisations should be entitled to conduct research for internal business purposes (including research and development) if certain specified conditions are met ("the framework").

b. The organization must have a policy in place that establishes the framework, which also specifies the operational and legal measures to be put in place to support the research and what to do in the event of a data breach or a breach / abuse of any research.

c. Where external research collaboration is required, the collaborating parties are to ensure that there are appropriate agreements and policies in place for such collaborations.

d. The Research Exception could disclose to data subjects, under access obligations, research usage except where confidential and proprietary information would be revealed, and provide a limited right for the data subject to have his / her personal data withdrawn from research.

The Exception for Disclosures to Public Agencies

The current exception from consent depends on the ability to prove that the disclosure is both necessary and in the public interest. Neither is necessarily capable of proof by an organization seeking to rely on the exception. Our proposal is to allow organisations to simply establish that a disclosure is reasonable in the public interest and to allow organisations to deem it so if the request was issued from a public agency through an official channel.

PART II: REVIEW OF DNC PROVISIONS AND THE SCA

PUBLIC CONSULTATION PAPER

Question No.	Comments
Question 1 What are your views on the proposed scope and applicability of the DNC Provisions and the Spam Control Provisions?	i. We welcome the initiative proposed by the PDPC. ii. A common theme in both the DNC Provisions of the PDPA and the Spam Control Act is the need to protect individuals against communications that can easily be sent in bulk and cause nuisance or harassment. By joining these statutory Acts together, a more comprehensive form of protection for individuals can be achieved. iii. It is also a step towards greater recognition of the privacy of the individual from receiving unsolicited messages. However, this should also be balanced with the need to maintain a business environment where legitimate marketing activities may still be carried out unimpeded. iv. There are two considerations that we put forward for the New Act. v. First, we note that the proposed DNC Provisions would apply to unsolicited "marketing text messages" whereas the proposed Spam Control Provisions would apply to unsolicited "commercial text messages". We propose that these definitions should be made consistent, and be properly defined in the New Act. vi. On the earlier point, this is to ensure that the protective measures afforded to the individual are consistently applied to the various instances and mediums of communication. vii. On the second point, there are many different types of commercial text messages, and these may not encompass typical marketing text messages. A proposition to do business may not be the same as a marketing message for the business itself. It is these nuances that need to be resolved in coming up with the New Act. viii. Second, in a case where there are exact overlaps

Question No.	Comments
	between the DNC Provisions and the Spam Control Provisions, it is unclear how the New Act would apply to these, and the penalties that would be afforded against an organisation that infringes both in a single act. Would the penalties be compounded or would they be additional and separate? There is an obvious need to avoid a case of double-penalties for essentially the same act or transaction. Instead, a sensible penalty should be imposed that would befit the transgression of both provisions. ix. Apart from our comments on the scope and applicability of the New Act above, we are also of the view that there needs to be careful consideration of how the New Act is to be enforced. The Spam Control Provisions only provide for private civil action, and there is no provision for regulatory action to be taken. Given the time and costs involved in private civil action, it is unlikely any recipient of a non-compliant message would commence action. In the present climate, most of these errant companies therefore get away scot-free. x. Accordingly, we propose that there be enforcement powers given to the PDPC to ensure that the companies comply with both the Spam Control Provisions and the DNC Provisions in the New Act. This would give the New Act the "bite" it needs to ensure compliance. In order to control the amount of enforcement cases to be handled by the PDPC, we can suggest that the New Act provides for administrative enforcement action to be taken only in respect of the worst offenders, ie based on the number of messages being sent.
Question 2 What are your views on including commercial text messages sent using IM identifiers under the Spam Control Provisions?	i. We support the proposal to extend the Spam Control Provisions to include IM identifiers. ii. This has perhaps been a long-awaited update to keep abreast of the latest trends and developments in technology. iii. At present, neither email addresses nor IM identifiers are covered under the DNC Registry. For instance, an instant message sent on Facebook is

Question No.	Comments
	not covered under the DNC Registry because a Facebook account is not linked to a Singapore telephone number. iv. It is therefore not uncommon to find errant companies turning to sending out messages via IM instead of the previous mode of communication by way of email or SMS-es in order to circumvent the Spam Control Provisions and DNC Provisions. v. However, we do wish to propose that there be a national register for IM identifiers, instead of the de-centralised approach as PDPC suggested at paragraph 3.13 of its consultation paper. vi. Although we recognise that there are likely to be certain operational difficulties in maintaining a national register, this may be outweighed by the difficulties companies in Singapore may face in seeking to comply. A de-centralised system would mean that companies would not have a common reference point to determine an individual's consent or preference, and they will have to seek individual consent accordingly. Not only is this costly and impractical, it may defeat the entire purpose since the individuals themselves would have to inform each and every organisation of their consent (since there is no centralised system). vii. We believe that it is easier for companies to have a common register against which to check rather than having many fragmented, organisation-specific registers. viii. Ultimately, while we recognise the issues with the increased costs for maintaining a national register, we believe it is far more important to safeguard the interests and the privacy of consumers and the public. ix. There is also the issue of territorial scope of the DNC Provisions and Spam Control Provisions. Presumably, there must be a nexus between email addresses/IM identifiers and Singapore in order for the email addresses/IM identifiers to be protected under the New Act. At present, under the DNC Provisions, telephone numbers can be identified as belonging to Singaporeans by the +65 prefix. However, if we have a national register for email

Question No.	Comments
	addresses/IM identifiers, one of the issues we will have to tackle is to ensure that only people with a nexus to Singapore can register. We do not want a situation where the PDPC has to regulate messages which are sent between individuals with no connection to Singapore. x. In order to address this issue, we propose that the DNC Registry be expanded to allow individuals to register their email addresses and IM identifiers (at least the main ones). This would serve the overall purpose of (a) ensuring that protection is afforded to such telephone numbers, email addresses and IM identifiers with sufficient nexus to Singapore (b) ensuring consistency of protection across these modes of communication; and (c) ensuring that there is a centralised system upon which companies may check for individuals' consent / preference.
Question 3 What are your views on the proposed reduction of the period for effecting withdrawal of consent to 10 business days, in line with the period to effect an unsubscribe request under the Spam Control Provisions?	i. The proposed reduction of the period for effecting withdrawal of consent to 10 business days is undesirable. It is less than half of the current prescribed period of 30 business days (see regulation 17 of the PDP Regulations) and is too tight a timeline for organisations to effect a withdrawal of consent. ii. We propose that the period to effect a withdrawal of consent request remain at 30 business days.
Question 4 What are your views on prohibiting the use of dictionary attack and address harvesting software for sending of commercial messages to all telephone numbers, IM identifiers and email addresses?	i. We support the amendment to prohibit the use of dictionary attack and address harvesting software for sending of commercial messages to all telephone numbers, IM identifiers and email addresses. ii. However, it must be noted that there may be some overlap with the Computer Misuse and Cybersecurity Act (CMCA) as it already criminalises circulating data that was mined. In this regard, there needs to be some rationalising of the two Acts in order to ensure consistency. iii. There are also concerns that the amendment may

Question No.	Comments
	affect an organisation's own address harvesting software on data it currently owns. This may inhibit the types of business activities it may carry out especially in respect of large databases it owns. We therefore propose that the amendment ought to be targeted at the mischief of harvesting *public* data and not in respect of an organisation's use of address harvesting software on data it owns.
Question 5 Should B2B marketing messages be subject to the requirements under the DNC Provisions, in alignment with the coverage under the Spam Control Provisions?	iv. There is room for adjusting the exception for B2B marketing messages. However, we are of the view that B2B marketing messages exception should be still maintained in the DNC Provisions. v. The B2B marketing messages exception plays an important role for communications across and amongst businesses. Without it, there is a danger that much of these communications would be hindered, impeded and restrained. This would make for an unconducive business environment where communication is the key to networking and for carrying out various business functions and operations. vi. A simple example may illustrate the issue. If a businessman was looking to find a partner to join in a business venture, and obtained a Singapore telephone number through a common contact, he would have to check the DNC Registry in order to reach out to this other person. If he had to do the same for each and every other person he wants to do business with, this would make for a very stifling and unconducive business environment. vii. We do, however, recognise that there may be difficulties drawing lines between a "business purposes" and "personal purposes" in terms of applying the B2B marketing message exception. In this regard, there may be some uncertainty when an organisation sends out a message as to whether it can rely on a B2B marketing message exception. viii. In our view, the answer to it is to properly define and to specify how the B2B marketing message exception is to apply. This can be coupled with guidelines and guidance for companies and individuals alike.

Question No.	Comments
	ix. For the reasons above, we do not think that the B2B marketing exception should be removed from the DNC Provisions.
Question 6: What are your views on the proposal for the DNC Provisions to be enforced under an administrative regime?	i. We are happy to leave the enforcement regime for the PDPC to decide. However, we are of the view that regardless of the type of regime implemented for enforcement of the DNC Provisions, the PDPC should nonetheless ensure the defendant retains his or her existing rights under the criminal enforcement regime, such as the right to be heard. ii. In deliberating on a response to this question, we also consider the actual implementation of such an administrative regime if it is so adopted and wonder how the process would be. If, for instance, there is a fixed schedule of financial penalties, these should be large enough to have a deterrent effect and so an optimal price point may have to be identified depending on the breach. In addition, if the Registrar ought to be deciding how much penalty to impose in each case, we suggest that coming up with and publishing sentencing guidelines would be helpful. A common theme in both the DNC Provisions of the PDPA and the Spam Control Act is the need to protect individuals against communications that can easily be sent in bulk and cause nuisance or harassment. By joining these statutory Acts together, a more comprehensive form of protection for individuals can be achieved. iii. We welcome a further collaboration between the Law Society of Singapore and the PDPC in preparing such guidelines and supporting the PDPC in this endeavour.
Question 7: What are your views on the proposed obligation to communicate accurate DNCR results, and liability on third-party checkers for any infringements of the DNC Provisions resulting from inaccurate information they provided?	We support this amendment. Third party checkers might otherwise hide behind a "shield" of excluding liability.

Question No.	Comments
Question 8: What are your views on the proposed prohibition of resale of results of telephone numbers checked with the DNCR?	i. We are of the view that a prohibition might not be the most cost-efficient manner to prohibit or at least deter reliance on results which have been resold. Whether an organisation wants to check with the DNCR directly or with a third-party reseller should be left to market forces. After all, market forces are the reason why such a resale started in the first place. ii. Further, if another prohibition (which is considered an offence) is carved out, there would be further need for enforcement of such a matter, potentially taking up more of PDPC's current resources. iii. We propose instead that rather than banning the resale of telephone numbers checked with the DNCR, perhaps it may be provided for instead that if it is pleaded that an organisation has obtained results of telephone numbers from a third-party database and/or resold results, such process of verification would not be a valid defence against liability for contravention of the DNC provisions.

Question No.	Comments
Question 9: What are your views on the proposed deeming provision?	iv. We do understand where the benefit of doing so could be from the perspective of efficiency in enforcement. v. However, we do not support this provision as ultimately, it would shift the burden of proof onto the individual to defend himself or herself. To illustrate a potentially adverse situation, consider if an individual was not the one to have actually sent the unsolicited marketing message as his or her phone was stolen. It would be difficult for such an individual to prove his or her innocence. The next question could then be: what exactly would be sufficient to rebut the deemed liability? vi. Another potentially challenging situation would be when an individual's device is hacked (without him or her being aware, which tends to be the case given the advent in technology which has made these attacks less obvious). The individual being targeted and made the scapegoat in such a case may not even know about it until he or she is being put on notice and is investigated. vii. We note that under section 36(3) of the PDPA, if a specified message is sent and at the relevant time the device was "controlled by a person without the knowledge of the owners or authorized users", the owner or authorized user shall be presumed not to have sent the message unless the contrary is proved. viii. Unless section 36(3) covers the scenarios above, we are therefore of the view that although the proposed deeming provision does have its merits, it may be more onerous on the individual being investigated, which may not necessarily be a fair balance given the challenges in an individual being able to put up a good defence. Hence, we think that the PDPC should prove its case against an individual without the deeming provision being introduced to skip this step.

PART III: ENHANCED PRACTICAL GUIDANCE

PUBLIC CONSULTATION PAPER

Question No.	Comments
Question 10 What are your views on the proposed Enhanced Practical Guidance framework?	i. The PDPC will assess requests for Enhanced Practical Guidance using the following criteria set out at paragraph 6.2 of its consultation paper: a. the query relates to a **complex or novel compliance issue** for which there is currently no clear position for treatment under the PDPA; b. the query **cannot be addressed by PDPC's general guidance and existing published resources**; AND c. the query **does not amount to a request for legal advice**. ii. While the intention underlying the proposed EPG framework (at paragraph 5.3) is correct, we have the following concerns regarding the proposed framework: a. the criteria of "complex or novel" and "cannot be addressed by PDPC's general guidance and existing published resources" are difficult to apply in practice. For example, would a case be considered "novel" because there is no published PDPC decision which has addressed it before or because the facts of the case have not arisen before? b. who will decide what is "novel"? c. the criterion "does not amount to a request for legal advice" may be difficult to apply where the guidance sought amounts only in part for legal advice. iii. It is also equivocal whether the EPG would be legally binding. The PDPC's paper mentions that other jurisdictions' data protection authorities can issue guidance that is legally binding (at paragraph 5.4), but the paper later states, in relation to the chargeability of PDPC's determinations, that "a more rigorous assessment will be required in order for PDPC to provide determinations that are binding *under the EPG framework*" (emphasis added, at paragraph 6.4).

Question No.	Comments
	iv. If the determination by PDPC is legally binding, this creates the possibility of misguidance. If not binding, organisations would not pay for or rely on it. v. Lastly, the facts of every case will have its own set of unique facts. Hence, the EPG may never be exhaustive enough.

PART IV: SECOND, THIRD AND FOURTH SCHEDULES TO THE PDPA (SOLICITATION OF FEEDBACK ON EXCEPTIONS TO CONSENT)

PUBLIC CONSULTATION PAPER

No.	Comments
1.	**Research Exception** We propose that the current exception for consent for use of personal data for research purposes (Third Schedule, paragraph 1(i) read with Paragraph 2; and Fourth Schedule, paragraph 1(q) read with paragraph 4), (collectively, the "**Research Exception**") be refined. The digital economy will present new opportunities to conduct research and development through the use of data analytics. Insight from such projects could lead to great benefits such as the development of new products and services. However, current issues as to how the current Research Exception is structured trigger issues as to the scope / applicability of the Research Exception, and the difficulty of applying the Research Exception. ***Issue 1: Scope of Research Exception*** As a starting point, it is not clear what "research" covers and a clearer delineation between service improvement analytics and research and development may be needed. Certain uses of personal data, though analytical in nature, are not "research" requiring consent or an exception to the consent obligation. For example, the PDPC has, in the PDPC's Advisory Guidelines on the Personal Data Protection Act for Selected Topics (para 2.4), given the example of a telecommunications service provider analyzing personal data in order to manage its network and carry out short-term planning enhancements to improve the quality of mobile services provided to the individual. However, if considered further, it is possible to see where further insights derived from the use of such data are not strictly for "planning enhancements to improve the quality of mobile services". At one extreme end of the spectrum, use cases for such insights may include development of new products or services which have no connection to current services. Whilst it is easy enough to see some distinction between the former ("service improvement") and the latter ("pure research" – to coin a phrase), when does an organization's use case of insight become "research" requiring consent / the exemption from consent? We would propose either a definition of research which carves out "service improvement" type uses of personal data from "research" under the PDPA, or, alternatively, to classify all uses of data in this spectrum as research purposes.

No.	Comments
	Issue 2: Criteria for the Research Exception We submit that the application of the Research Exception, as currently framed, is not without its challenges. A fuller discussion of this issue can be found in the PDPC Digest ("Data Analytics: Considerations When Repurposing Transactional Personal Data under the Personal Data Protection Act" by Lim Sui Yin Jeffrey & Lee Yue Lin, 2016). There are 4 limbs to meet under the Third Schedule (para 2(a) to (d)), and 5 under the Fourth Schedule (para 4(a) to (e), the last of which includes 5 other sub-limbs). Additionally, both requirements under the Third and Fourth Schedule pose practical issues which have rendered (in practice) it mostly impossible to apply. To take an example, the requirement that it is "impracticable for the organization to seek consent" is difficult to apply. "Impracticability" can vary according to the circumstances. For example, is consent "impracticable" if there are difficult questions of how to frame consent? (for eg. if research is ongoing / open-ended, or – as is the case in most data analytics use, potentially capable of multiple use cases). Additionally, what numbers of data subjects and what costs involved in a consent gathering exercise would trigger / cross any limits of what is "practicable"? Other examples relating to the difficulty in addressing the requirement of impracticability is the fact that even if there is availability of contact information, the cost of procuring consent, resources required to monitor consent – all are practical issues which, even if they are not technically impossible, could be "impracticable" by a question of degree. When then, would a consent collection exercise be practicable or become "impracticable"? Such a situation is not conducive for clarity and certainty. Other hurdles include providing that the "linkage of the personal data is not harmful to the individual" and that "the benefits to be derived from the linkage are clearly in the public interest". Such a formulation is more germane to a research regime grounded in ethics, such as medical research, and is difficult to apply in the context of say, private research into the efficiency of a search engine for travel services, or, say the potential for providing a new financial service. How would "public interest" be weighed in such a situation? If in fact, the key goal is to require organisations to conduct their research in a responsible and accountable manner, then what is essential would be for organisations to be able to apply a governance framework that assures that responsibility and accountability rather than requiring that all research use cases fit a particular profile. Perhaps guidance can be taken from the approach under the Human Biomedical Research Act 2015 (with appropriate modifications) ("HBRA"). In the HBRA, internal governance bodies (IRBs) undertake the job of assessing and approving medical research and appropriate steps are undertaken in the case of serious adverse

No.	Comments
	reactions and other eventualities arising from the research project. There is a requirement for the organization to establish, inter alia, its own system of checks and balances to support governance of the research. Whilst we would not advocate adopting the wholesale stringency of the HBRA, we believe the use of an internal governance body / office to review and approve (and also to keep track of and account for) research would be preferable to the current prescriptive regime, as it will allow the organization flexibility to address research use case scenarios without sacrificing governance controls. For this reason, we would propose reforming the Research Exception along the following lines: e. Organisations should be entitled to conduct research for internal business purposes (including research and development) provided that the data protection officer is notified of (and approves) such research, and is given full details of the personal data to be used, the category of impacted data subjects, and a description of the appropriate safeguards to the personal data involved in such research. f. The data protection officer may exercise his / her discretion to approve, disapprove, or approve with provisos (eg. asking for operational safeguards, or limiting the length of searches, or requiring a regular reporting / update of the conduct of such research). g. The organization must have a policy in place that establishes the foregoing framework which includes what operational and legal measures are to be put in place to support the research and what to do in the event of a data breach or a breach / abuse of any research. h. Where external research collaboration is required, the collaborating parties are to ensure that there are appropriate agreements and policies in place for such collaborations, including the implementation of safeguards and the right to require the participating collaborating entities to take steps to remedy breaches. i. The Research Exception should disclose to data subjects, under access obligations, research usage except where confidential and proprietary information would be revealed, and provide a limited right for the data subject to have his / her personal data withdrawn from research (to take effect prospectively – with appropriate exclusions of any obligation on the organisation to undo research or work product already completed). Additionally, we note that it would be important for data subjects to have some autonomy over whether they can permit the use of their data for research. On this note, we would also observe that the access obligation would give data subjects the opportunity to discover that their personal data had been the subject of research, and it would be also be helpful to make it expressly clear that the data subject could,

No.	Comments
	further to discovery of the use of data for research purposes be given a right of withdrawal of consent for further use of the data for research. To make such a right of withdrawal practical, the effect of such a withdrawal could be limited to prospective use, and not require organisations to unwind / reverse work done earlier. With such appropriate governance regimes in place, we submit that the Research Exception can be utilized more effectively particularly by organisations willing to place governance and safeguards over research being done.
2.	Exception in connection with disclosures to public agencies in the public interest Exception 1(g) of the Fourth Schedule refers to an exception from consent where a disclosure is made to a public agency which is "necessary in the public interest". Based on the current wording of the exception, it would appear that the ability to rely on the exception will depend on the ability to prove the (1) necessity from the perspective of (2) the public interest. Whilst public agencies may well be prepared to confirm that they are operating for ultimate benefit of the public interest, it is not clear to organisations who interact with such agencies how they can discharge the burden of proof that a disclosure was so necessary. "Necessity" is a qualitative assessment and a difficult one to make – there may well be other avenues at achieving a particular public interest objective which impact the case for necessity. Additionally, the public interest assessment is not one that a public agency may necessarily assist a disclosing organization in making, especially since public agencies are exempt from the application of the PDPA. It follows that the burden of assessing whether something is indeed in the "public interest" falls to the private organization – which may not be best placed to make such an assessment. We proposed that both the exception be reformed to (1) relax necessity to "reasonably in the public interest", and then to (2) empower organisations to confirm that the matter is in the public interest if the request is issued by a public agency in its formal capacity (eg. from the letterhead / business email of an officer of the public agency). The former will eliminate conducting analysis of theoretical questions of necessity and the latter will avoid requiring private organisations to undertake public policy consideration exercises.

CYBERSECURITY AND DATA PROTECTION COMMITTEE

No.	Names	Remarks
1.	Amira Nabila Budiyano	Consultation subcommittee member
2.	Anil Narain Balchandani	
3.	Boxall Lynette Maureen	
4.	Bryan Manaf Ghows	
5.	Jansen Aw	Consultation subcommittee member
6.	Kang Poh Sing	
7.	Kao Kwok Weng Jonathan (Gao Guorong)	
8.	Kevin Elbert	
9.	Khoo Yong Jie	
10.	Leow Jiamin	
11.	Lim Kian Kim	Committee chair
12.	Lim Seng Siew	Council representative
13.	Lim Sui Yin Jeffrey	Committee vice-chair; consultation subcommittee member
14.	Lua Limian, Jeremy	
15.	Maheswari Rani D/O Krishna	Consultation subcommittee chair
16.	Ow Shi Jack	
17.	Pang Keep Ying Joey	
18.	Prasad S/O Karunakarn	
19.	Quah Pern Yi	
20.	Shakti Krishnaveni Sadashiv	
21.	Tan Ming Kirk Richard	
22.	Michael Ho	Law Society secretariat
23.	Stella Chen	Law Society secretariat