THE LAW SOCIETY OF SINGAPORE'S COMMENTS ON
THE MINISTRY OF COMMUNICATIONS AND INFORMATION AND
THE PERSONAL DATA PROTECTION COMMISSION'S
PUBLIC CONSULTATON PAPER ON THE DRAFT
PERSONAL DATA PROTECTION (AMENDMENT) BILL, INCLUDING RELATED AMENDMENTS TO
THE SPAM CONTROL ACT

1. The Law Society thanks the Ministry of Communications and Information ("**MCI**") and the Personal Data Protection Commission ("**PDPC**") for providing it with an opportunity to give its comments on the draft Personal Data Protection (Amendment) Bill including related amendments to the Spam Control Act ("**Draft Bill**"), as set out in the Public Consultation Paper issued by MCI and the PDPC (the "**Paper**"). We welcome the PDPC's efforts to provide guidance in this area and thank the PDPC for taking into account the views of our community of practice.

2. For the purposes of the submissions, we have organised our response according to the sections and paragraph sections detailed in the Paper. For completeness, we would like to highlight that we have not been able to canvass full views on each point of the Paper relating to the Draft Bill given the extremely limited time given for review and response. In the interest of brevity and for the foregoing reason, we have tabulated and provided a bullet-point collated summary of our comments to each section in **Annex A** to this document.

3. The Law Society's Cybersecurity and Data Protection Committee (the "**Committee**") remains eager, able and willing to engage the PDPC in further consultation or discussion in respect of any points the PDPC may wish to clarify further or to provide additional feedback. Any further queries in this regard may be directed to the Law Society Secretariat supporting the Committee at lpi@lawsoc.org.sg.

4. We look forward to hearing from you.

The Law Society of Singapore
28 May 2020

ANNEX A

Section/Paras of the Paper	Issue at a Glance	Comments
Part II: Strengthening Accountability (paras 10 to 12)	Accountability principle	The Committee notes that the increased emphasis on accountability is supported by policy reasons. Accordingly, the clarity offered in including an explicit reference to this principle is welcomed by the Committee. However, it is noted that the second line of para 11 of the Paper states: *"This will make it clearer that organisations are accountable for personal data in their possession or under their control, and are expected to be able to demonstrate compliance."* The Committee therefore recommends that in line with the above, section 12 of the PDPA be amended to make it clear that organisations are "expected to be able to demonstrate compliance". In this respect an additional sub-section is recommended to be added to give effect to this requirement, if this is the intention of MCI/PDPC. The Committee also questions whether by effect, accountability as a principle (and particularly whether an organisation is able to demonstrate compliance with its own policies/breach management plan) will now be taken as another deciding factor or as mitigation in any investigations of a breach incident. The Committee urges that guidance be given in this respect so that organisations are able to understand how exactly their behaviour vis-à-vis this principle could affect or penalise them.
Part II: Strengthening Accountability (paras 13 to 26)	Mandatory data breach notification requirement	The Committee notes that *"[d]ata breach notifications are central to organisational accountability because they encourage organisations to establish risk-based internal monitoring and reporting systems to detect data incidents."* Generally, the Committee welcomes a breach notification requirement, whether as part of the accountability principle or otherwise. However, the Committee suggests certain recommendations and proposes that clarification be provided in the forthcoming Regulations as to the following:- *Notification criteria*

Section/Paras of the Paper	Issue at a Glance	Comments
		1. Firstly, it is unclear as to what form of documentation will need to be provided for the notification to PDPC. The Committee recommends that in order for organisations to be able to provide sufficient information for PDPC's consideration (i.e. making this a priority while dealing with other business considerations and implications of such a data breach) and in a format that is facilitative, such notifications are prepared with the assistance of legal counsels/representatives, who would be able to structure the notification properly and include the requisite details. 2. In stipulating a numerical threshold that constitutes "a significant scale", the Committee notes that placing a low threshold starting from 500 individuals, would mean that such notifications will likely to have to be done in almost all cases, rather than not. For bigger organisations, where the number of individuals' personal data that is collected/held could be more than a smaller organisation, 500 individuals could be a mere 1% of its entire database. The Committee recommends that the number be given in a range or a percentage proportionate to the number of individuals' personal data that the organisation keeps instead. This would ensure that notification is required for data breach that is on "a significant scale", relative to the organisation. Further, in stipulating categories of personal data which are likely to result in significant harm to individuals, this would mean that there is an implicit segregation of different personal data and their respective value. There is no separate definition of "sensitive personal data" in the PDPA, and this appears to be a deliberate legislative decision. Nonetheless, if MCI/PDPC intends to create such segregation by carving out what are "more important/risky" data categories, the Committee proposes that clarity is given in this regard, as it would affect how an organisation structures its policies, as well as the level of cyber-insurance that it may obtain accordingly. In conclusion as to the above, the Committee questions the usefulness of such criteria and whether they can be easily and meaningfully applied by organisations. *Assessment and notification timeframes* 3. It is unclear what is considered "unreasonable delay". The Committee recommends that clarification be given through examples, so that organisations could apply the examples to

Section/Paras of the Paper	Issue at a Glance	Comments
		themselves and their respective situation. This appears essential, given that "[u]nreasonable delay in assessing or notification of data breaches will be a breach of the data breach notification requirement." 4. In a situation with a DI, it is unclear as to what is "undue delay". Likewise, the Committee recommends that clarification be given through examples, so that organisations and DI could apply the examples to themselves and their respective situation. Further, the Committee welcomes the exceptions provided under para 22 of the Paper. In relation to the proposed timeline and the deadline of 3 calendar days to notify PDPC, the Committee is of the view that for most organisations without the necessary resources to handle this in-house, 3 days would be quite a stretch. The Committee therefore believes that this reinforces the need for such notifications to be prepared with the assistance of legal counsels/representatives, who would be able to structure the notification properly and include the requisite details.
Part II: Strengthening Accountability (paras 27 to 29)	Removal of exclusion for organisations acting on behalf of public agencies	The Committee notes recommendation 4.4(a) of the PSDSRC Report that the PDPA be amended to cover agents of the Government. The present section 4(1)(c) of the PDPA excludes organisations acting as agents of public agencies (including Government ministries, departments, organs of state and specified statutory bodies) from the application of the Parts III to VI of the PDPA (the "**Data Protection Provisions**"). Under the usual principles of agency, an agent acting on behalf of its principal may bind the principal to certain legal obligations with third parties. In the context of the PDPA, such third parties may include individuals whose personal data is collected, used or disclosed by an agent of a public agency on behalf of the public agency (its principal). With the removal of agents of public agencies from the ambit of section 4(1)(c), such agents appear to be required to comply with the Data Protection Provisions in relation to the collection, use and disclosure of personal data on behalf of their principal. This is not entirely clear as the agent's principal would continue to be excluded under the amended section 4(1)(c). For example, in relation to the requirement to obtain consent for the collection, use and/or disclosure of personal data under section 13 of the PDPA, where the collection of personal data is

Section/Paras of the Paper	Issue at a Glance	Comments
		done on behalf of a public agency, it is not clear whether the agent would be required to seek consent since it is, legally, performing the collection for its principal and the principal is not required to seek consent under the PDPA. If the agent is required to seek consent, this raises the issue of whether the agent's principal is bound by the agent's conduct in relation to the collection of personal data and also when it (the principal) subsequently seeks to use or disclose the personal data. Conversely, other Data Protection Provisions may not affect the principal even through the agent is required to comply with them. For example, an agent may be required to protect personal data in accordance with section 24 of the PDPA and this would not seem apply to its principal if the principal is excluded under section 4(1)(c). However, there is also a potential impact on the principal since the agent may be required, as part of its obligations under section 24, to ensure that its principal protects the personal data to the same standard as that required under the PDPA. The Committee suggests that MCI/PDPC consider clarifying legislatively how the change will affect the obligations of agents of public agencies under the various Data Protection Provisions. MCI/PDPC may also wish to consider implementing a limited exclusion for agents of public agents, such as what is presently provided for in section 4(2) in relation to data intermediaries. If the intention is for such agents to be treated as data intermediaries under section 4(2), MCI/PDPC may wish to clarify whether section 4(3) applies in relation to public agencies.
Part II: Strengthening Accountability (paras 30 to 36)	Offences relating to egregious mishandling of personal data	The Committee notes recommendation 4.4(b) of the PSDSRC Report that the PDPA be amended to bring non-public officers to task for recklessly or intentionally mishandling any personal data and that this will bring the PDPA in line with the Public Sector (Governance) Act. The Committee further notes from the PSDSRC Report that this is meant to reinforce the individual's responsibility and accountability for personal data they handle. The Committee notes that the proposed amendments are a significant change to the PDPA as employees of organisations who are acting in the course of employment are presently excluded from the application of the PDPA's Data Protection Provisions under section 4(1)(b). For employees who are acting the course of employment, the new offences generally introduce a new criteria which determines whether the PDPA applies, that is, whether they are authorised by their employer. In the absence of such authorisation, they would be committing an offence even if they are acting in the course of employment. This is made clear in section 53(1) of the PDPA which

Section/Paras of the Paper	Issue at a Glance	Comments
		provides that any act done, or conduct engaged in, by a person in the course of his employment (an employee) shall be treated as having been done by his employer as well as by him. The Committee notes from para. 32 of the consultation paper that the intention is for the new offences to not apply to employees acting in the course of employment. MCI/PDPC may wish to consider expressly providing for this legislatively, perhaps in section 53, so that the new offences do not apply to all employees acting in the course of employment. Employees who are not acting in the course of employment are potentially subject to the Data Protection Provisions today, such as if they use personal data collected by their employer for their own purposes. With the new offences, such employees may face enforcement action under the new offence provisions as well as section 29 of the PDPA. Furthermore, as a result of section 53(1) (noted above), the same issue potentially arises in relation to employers whose employees commit one of the new offences while acting in the course of employment. In general, the Committee is of the view that acts which constitute one of the new offences should not also amount to a contravention of the Data Protection Provisions (or vice versa). MCI/PDPC may wish to consider excluding acts which constitute one of the new offences from the ambit of section 29. Such an approach is not inconsistent with the policy position stated in para. 31 of the Paper. The Committee notes that para. 32 of the Paper states that the individuals who will not be subject to criminal sanctions under the new offences include "academic researchers who re-identify anonymised data as part of their research work and teaching of topics on anonymisation and encryption; and individuals who independently carry out effectiveness testing of organisations' information security systems either as a white-hat hacker or as part of bug bounty programmes" (emphasis added). It is not clear whether this is intended to apply where such individuals are authorised by their employer, as indicated in the opening sentence of para. 32. In the Committee's view, academic researchers and white-hat hackers would not necessarily be authorised. Furthermore, their employers (if they have one in this context) may not wish to provide such an authorisation as they would then be liable for contravening the PDPA. In view of this, MCI/PDPC may wish to expressly exclude specific conduct, such as academic research and/or white-hat hacking, from the ambit of the new offences. The Committee notes from para. 33 of the Paper that the new offences are not intended to apply *"in situations where the conduct is in the nature of a private dispute for which there is recourse under private law (e.g. ex-employee taking an organisation's customer list when joining a*

Section/Paras of the Paper	Issue at a Glance	Comments
		competitor)". At the outset, the Committee notes that these situations are not excluded from the ambit of the new offences as drafted in the Draft Bill. Further, it is not clear when conduct which constitutes an offence is or is not also "in the nature of a private dispute for which there is recourse under private law". It is arguable that all unauthorised uses or disclosures of an individual's personal data would have recourse under section 32 of the PDPA (the right of private action), or other branches of the law, where such use or disclosure is not consented to by the individual or not otherwise authorised by written law. Further, private legal proceedings would be aimed at providing a remedy for losses and damages suffered or preventing further losses and damages, and not as a sanction against the conduct in question. Overall, while the Committee understands the policy intent for the PDPA not to be "used" by the parties in purely commercial disputes, private legal proceedings (especially under section 32) have a role to play in ensuring the protection of individuals' personal data. MCI/PDPC may wish to consider taking action under the new offences notwithstanding any separate private legal proceedings. In relation to the new offences: • Concerning when an individual is authorised, as disclosure of personal data is generally subject to an individual's consent under section 13 of the PDPA, MCI/PDPC may wish to consider also providing for authorisation by the individual concerned in relation to the new section 35B (this would not seem to be applicable to the new section 35C and 35D); • In addition to the act of disclosure, the new section 35B criminalises an individual's conduct which causes the disclosure of personal data. This would appear to include actions such as those causing accidental inadvertent disclosures, which may give rise to a contravention of section 24 of the PDPA. For example, if an individual fails to comply with his employer's security policies and this leads to disclosure of personal data, it would appear that the individual commits an offence under this new section. MCI/PDPC may wish to clarify if the new section 35B extends to requiring employees to comply with applicable security requirements established by their employer or if the reference to "the individual's conduct" is meant to refer to conduct directly related to the act of disclosure (such as intentionally exposing personal data for others to view without directly giving the data to them);

Section/Paras of the Paper	Issue at a Glance	Comments
		• In relation to the new sections 35B and 35C, as personal data may be in the possession and/or under the control of two or more organisations simultaneously, it would appear that no offence is committed as long as one of these organisations authorises the disclosure or use of personal data, even if the others do not. MCI/PDPC may wish to consider clarifying if this is indeed the intended position.
Part III: Enabling Meaningful Consent (paras 37 to 42)	Enhanced framework for collection, use and disclosure of personal data	The Committee notes that the enhanced framework includes the expansion of deemed consent, the introduction of two new exceptions and enhancing the research exception. We discuss this further below. **I. <u>EXPANSION OF DEEMED CONSENT</u>** **<u>Deemed consent by contractual necessity</u>** The Committee notes that the expansion of deemed consent by contractual necessity is limited to where it is reasonably necessary for the (a) conclusion or (b) performance of a contract or transaction between an individual and an organisation. Further, the proposed sections 15(3) and 15(4) are subject to the proposed section 15(5), which introduces an additional safeguard for P, whereby the contract between P and A can specify or restrict P's personal data to be disclosed by A to B or the purpose for such disclosure. However, in practical terms, the Committee views the proposed section 15(5) to be more useful/applicable where a contract is **already concluded** between P & A as contemplated in the proposed section 15(4). Further, in the event data is disclosed where P has only "a view to contract" as per the proposed section 15(3), and the purpose of disclosure is that it is "reasonably necessary for the conclusion of the contract between P and A", it is uncertain what happens to the data if the contract falls through, as it appears that there is no provision dealing with the same. It is noted that at Part 3 of the New First Schedule, paragraph 11 sub-paragraph 5 provides that all personal data collected must be returned and destroyed in the context of a business asset transaction which does not proceed/is not completed. The Committee considers and proposes

Section/Paras of the Paper	Issue at a Glance	Comments
		that perhaps there ought to be a similar provision for section 15(3) in the event the contract falls through. **<u>Deemed consent by notification</u>** It is noted that the proposed section 15A is also subject to section 15(2). The Committee is of the view that there seems to be adequate safeguards to protect P's interests: 1. The organization must (i) notify P of (a) its intention to collect use or disclose P's personal data and (b) the purpose of such intention and (ii) give P a reasonable period to opt-out of the collection, use or disclosure of his/her personal data for that purpose. 2. Even if P fails or neglects to opt out within the specified period, and P is deemed to have given his consent, P will still be able to withdraw his/her consent to the collection, use or disclosure of personal data. 3. Organisations will have to assess and determine that the data use/collection is not likely to have any adverse effect on the individual, after implementing measures to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual. It is noted that appropriate notification needs to be given by the organisation. However, it is unclear as to what could be an appropriate form of notification. The Committee recommends that guidance be provided in support of the same, so that organisations can benefit from the enhanced deemed consent framework. The Committee also notes: *"In order to rely on deemed consent by notification, organisations <u>are required to assess and ascertain</u> that the intended collection, use or disclosure of personal data for the purpose is not likely to have any adverse effect on the individual after implementing measures to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual."* It is currently also unclear how the assessment process ought to be. It is thus recommended that just like how a Data Protection Impact Assessment was rolled out, a similar form of assessment can be provided to guide organisations on factors for consideration. The Committee notes that at para 38 of the Paper: *"Organisations also may not rely on this approach to obtain consent to send direct marketing messages to the individuals. Individuals will*

Section/Paras of the Paper	Issue at a Glance	Comments
		also be able to withdraw their consent to the collection, use or disclosure of their personal data". The Committee welcomes these safeguards. We agree that while the interests of organisations by reducing compliance costs and enabling use of personal data for business purposes/enhancement are advanced through such measures, individuals are still given some form of protection against unwarranted use and/or disclosure. **II. <u>NEW EXCEPTIONS TO CONSENT REQUIREMENT</u>** **<u>Legitimate Interests Exception</u>** The Committee welcomes this exception as it can serve to detect or prevent illegal activities, threats to physical safety and security, etc. There appears to be adequate safeguards for individuals: 1. the accountability requirement imposed on the organisation to assess and determine that the data use/collection/disclosure is not likely to have any adverse effect on the individual, after implementing measures to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual. 2. the organisation must disclose to the individual their reliance on legitimate interests to collect, use or disclose personal data. 3. the organisation cannot use the data for sending direct marketing messages to the individual. However, the language of the new provisions does not seem as protective of the individual as compared to the GDPR (this is contrasted to because para. 39 of the Paper references protection frameworks in other jurisdictions including the EU). We therefore turn to the same in order to understand the considerations or working behind the proposed exception herein. It is noted that the wording in Recital 47 of the GDPR is somehow more "conscious" of the individual and his reasonable expectations: *"The legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing,* ***provided that the interests or the fundamental rights and freedoms of the data subject are not***

Section/Paras of the Paper	Issue at a Glance	Comments
		overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller." Also, there is no clear definition or explanation as to what can constitute "adverse effect". This is in contrast to the GDPR which does set out what could constitute the same under Recital 75. The Committee proposes that if this exception is included in the manner it is currently provided for under the new provisions, a definition is provided, or where possible clarity is provided in further guidelines to be issued by MCI/PDPC in due course. **Business Improvement Exception** It is noted that the following could fall under this exception: (i) operational efficiency and service improvements; (ii) developing or enhancing products/services; and (iii) knowing the organisation's customers. Nonetheless and since this exception relates to the use of personal data collected in accordance with Data Protection Provisions, the individual theoretically ought to have some initial layer of protection. However, it still seems that the dispensation of the individual's explicit consent to the use of his personal data by an organisation for business interests/improvement/enhancement overrides an individual's right to expressly decide. Therefore, care must be taken and additional safeguards might need to be looked into. The Committee recommends that MCI/PDPC issues guidelines clarifying as to what could be construed or falling under the ambit of (i), (ii), and (iii) to prevent them from being read too broadly in the interests of an organisation. Just because consent can be withdrawn by an individual does not mean that the harm has not already been done. This exception also appears to lack the "public interest" element of the Legitimate Interests Exception. **III. RESEARCH EXCEPTION** For both use and disclosure of data, there appears to be adequate confidentiality safeguards as far as publishing the results of research is concerned. Also, organisations must ensure there are

Section/Paras of the Paper	Issue at a Glance	Comments
		no adverse effects on the individuals whose data is used/disclosed. However, what amounts to adverse effects is not defined. Additionally, there are more stringent requirements for disclosure, in that the public interest element must also be satisfied. The less stringent restrictions on organisations for the use of personal data for research purposes without consent is welcome as its objective is to enable organisations to carry out research beyond the purposes of improving business products or services, for example, for advancements in scientific research and development and research in education, arts and the social sciences.
Part IV: Increasing Consumer Autonomy (paras 43 to 52)	Data portability obligation	**Scope of Data Portability Obligations** The Committee notes that the scoping of data portability obligations is similar to regulations in other jurisdictions and strikes a balance between individual rights and business efficacy. MCI/PDPC can consider clarifying the circumstances when the porting organisation can continue to (or otherwise has to cease to) collect, use or disclose an individual's personal data, after completing the porting request. For example, a porting request may be made to explore the viability of better service or options from another service provider, but the porting organisation can continue to collect, use or disclose the individual's personal data to provide services until the individual terminates service. MCI/PDPC can consider inserting "or machine-readable" after "electronic" in proposed section 26E(2)(a) such that it reads: "is in electronic *or machine-readable* form on the date the porting organisation receives a data porting request relating to the applicable data". There may be instances where data is no longer stored in electronic form but is nonetheless retrievable or recoverable by the porting organisation. It is not inconceivable that an organisation may store basic personal data and "derived personal data" in electronic form while retaining other personal data to be retrieved/recovered as and when needed. For organisations that simply do not store personal data in electronic form, regulations can address this by only requiring such organisations to transmit the data in their original machine-readable form.

Section/Paras of the Paper	Issue at a Glance	Comments
		<u>Interaction with Access Obligation</u> The Consultation Paper notes that data portability obligations are separate from personal access requests. In addition to encapsulating these as separate sections of the PDPA, MCI/PDPC can consider expressly stating so in the new Part IVB on the data portability obligations. There should be further consistency between data portability and personal access requests, for example the technical and process details do not need to be different between the two regimes. **<u>"Derived Personal Data"</u>** It is not clear that excluding "derived personal data" from data portability would serve the goal of preventing or at least reducing prejudice caused by "fast followers", as individuals appear to still be able to get access to "derived personal data" and pass this on to the receiving organisation. The existing exclusion of personal data that "*if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation*" appears to be sufficient although this may still result in disagreements over what would be "confidential commercial information" and whether the disclosure would "harm the competitive position of the organisation". Given the alleged confidential nature of the information, individuals and the receiving organisation are unlikely to get sufficient information to challenge the assertion. A separate dispute resolution process may be required. In the event of a dispute, PDPC can consider mandating a mediation prior to review by PDPC in the event that an organisation rejects a porting request. Given that data is being ported between organisations, external counsels or DPOs can make the necessary representations to an independent mediator or adjudicator.
Part IV: Increasing Consumer Autonomy (paras 53 and 54)	Improved controls for unsolicited commercial messages	**<u>SCA will cover messages sent to IM accounts (para 54(a) of the Consultation Paper)</u>** The Committee would suggest that MCI/PDPC now consider extending the prohibition to IM accounts mutatis mutandis to in-app notifications and/or a mobile device's notification (e.g. push notification) feature. As indicated in the Public Consultation Paper, the objective of the proposed amendment is to provide consumers with greater control over unsolicited marketing messages

Section/Paras of the Paper	Issue at a Glance	Comments
		against the backdrop of "technological advances [that] have fuelled the increased use of marketing tools". On such a principle, the regulation of unsolicited marketing messages should be technologically agnostic, to reduce the necessity of future amendments to account for changes in the channel of delivery. In the same vein, the definition of "instant messaging service" (for the purposes of the Spam Control Act) as proposed, may therefore be too restrictive ("…***exchange*** *messages with other users*…") given the objective to protect the recipient from unsolicited, *unilaterally sent* marketing messages, i.e. in principle, for the prohibition to be triggered, it should not be a condition that the *recipient* is also able to send messages on such a platform. In this regard, compare also with the current wording of section 5 (*meaning of "unsolicited"*) in the current Spam Control Act. For context, we note that in the earlier *Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy*, there were concerns raised in relation to whether the prohibition should extend to in-app notifications, mobile push notifications, and pictures/videos which contain commercial messages. In the context of the previously proposed omnibus act which combines DNC and Spam Control provisions, the PDPC had suggested that the prohibition will not extend to in-app notifications or a mobile device's notification feature. In light of the above discussion, perhaps this should be reconsidered. **Obligation and liability on third-party checkers (para 54(c) of the Consultation Paper)** The Committee concurs that the proposed liability on third-party checkers would enhance the accountability by stakeholders in the overall regulatory regime. However, the Committee would suggest that MCI/PDPC consider and clarify the interaction of: (a) the new obligation and liability on third-party checkers as proposed, the one hand; and (b) the existing safe harbour for network service providers under the Electronic Transactions Act ("**ETA**"), on the other hand. In relation to (b), Section 26 of the ETA provides that:

Section/Paras of the Paper	Issue at a Glance	Comments
		"26.—(1) Subject to subsection (2), a network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on — *(a) the making, publication, dissemination or distribution of such materials or any statement made in such material; or* *(b) the infringement of any rights subsisting in or in relation to such material.* *(1A) Subject to subsection (2), a* ***network service provider shall not be subject to any liability under the Personal Data Protection Act 2012 in respect of third-party material in the form of electronic records to which he merely provides access****."* In particular, a "network service provider" is not defined in the ETA, and the express exception in Section 26(2) of the ETA in relation to the PDPA ("*in respect of third-party material in the form of electronic records* ***to which he merely provides access***") may theoretically be read broadly to include access to information about the DNC Register. Since the proposed amendments will be to the PDPA, the interactions between the safe harbour in the ETA and the new liability on third-party checkers should ideally be clarified for the avoidance of doubt, as well as to minimise perceived inconsistencies or uncertainties between statutory instruments.
Part V: Strengthening Effectiveness of Enforcement (paras 55 to 57)	Enforcement of DNC Provisions under administrative regime	**Change of status of infringement sections in DNC Provisions from criminal offences to enforcement under administrative regime** The Committee notes that there are policy reasons behind the change, and concurs with this, provided that an equivalence in proportionality and due process continues to be applied in the administrative sanction regime, including transparency of decisions.
Part V: Strengthening Effectiveness of Enforcement (paras 58 to 60)	Increased financial penalty cap	**Increase of the ceiling for financial penalty from S$1 million to the greater of S$1 million or 10% of organisation's annual gross turnover.** The Committee notes that there are policy reasons behind the change, and notes further that the calculation of the gross annual turnover is of the organisation and not any related company or group

Section/Paras of the Paper	Issue at a Glance	Comments
		of companies. The Committee suggests that it may be necessary, on a case by case basis, to consider whether there is in fact "turnover" available (e.g. where the company is a support services company generating no turnover, etc.). Where so, the new position will effectively mean that there is no change to the ceiling (i.e. there being no turnover, the ceiling effectively remains at S$1 million). This may be a policy decision, and if so, then the Committee is fine with that approach.
Part V: Strengthening Effectiveness of Enforcement (paras 61 to 63)	Require attendance	**Introduce an offence for a person who fails to comply with an order to appear before PDPC, etc (para 62 of the Consultation Paper)** The Committee concurs with the need to provide recourse under the PDPA against organisations which refuse to reply to PDPC's notice to produce information / statement when required, so as to strengthen the enforcement bite of MCI/PDPC. However, the MCI/PDPC may wish to consider extending the qualifier of "without reasonable excuse" to the proposed limb (b)(bb) of Section 51 of the principal Act, for consistency with the language of the earlier limb (b)(ba). In the same vein, the MCI/PDPC may also wish to clarify whether timelines may be extended if legal representation and/or advice is sought, so that it is not an offence for a preliminary refusal of appearance. MCI/PDPC may also wish to make clear to the public that lawyers could assist to facilitate the process for efficient investigations by PDPC, or otherwise provide administrative avenues for concessions, waivers, etc so as to create flexibility for contingencies and enhance business confidence in the regulatory framework.
Part V: Strengthening Effectiveness of Enforcement (paras 64 to 67)	Statutory undertakings	The Committee supports the introduction of statutory undertakings (or "voluntary undertakings" as they are referred to in the new section 31A) in the PDPA as this would provide greater clarity to organisations on the effect and operation of such undertakings. In this regard, there are 2 areas where the current provisions are not clear. First, if an organisation gives, and PDPC accepts, an undertaking under section 31A, to what extent does that preclude an investigation or enforcement action under sections 50 and 29 respectively of the PDPA? The chapeau of section 31A preserves the effect of sections 29 and 50. The Committee notes from para.

Section/Paras of the Paper	Issue at a Glance	Comments
		66 of the consultation paper that PDPC may investigate the underlying breach if the organisation fails to comply with the undertaking, but the consultation paper is silent on the situation where the organisation is in compliance with the undertaking. Further, the Committee notes that there may be circumstances where an investigation is merited even though the organisation is in compliance with the undertaking, for example, where PDPC has reasonable grounds to believe that the underlying breach was more serious than what was informed to it by the organisation when it gave the undertaking. MCI/PDPC may wish to consider including an additional provision in section 31A to clarify that PDPC will not investigate the underlying breach while an undertaking is in force except in certain specified circumstances. The Committee is of the view that this will provide greater clarify to organisations and enhance the effectiveness of the statutory undertaking regime under section 31A. Secondly, to what extent does the giving of an undertaking under section 31A amount to an admission of a contravention of the PDPA? Unlike section 29, which applies where PDPC is satisfied that an organisation is not complying with one of the PDPA's Data Protection Provisions, section 31A(1) applies a lower standard, where PDPC "has reasonable grounds to believe that [inter alia] an organisation has not complied, is not complying or is likely not to comply" with the Data Protection Provisions. PDPC may have such grounds based on an investigation under section 50 or from information provided by the organisation in question. In any case, the issue arises as to whether the organisation must admit to the contravention, especially where the circumstances are such that it is not clear that there is, or will be, a contravention. The Committee suggests that MCI/PDPC clarify legislatively that the giving of an undertaking does not amount to an admission of the facts constituting the possible contravention, or that the organisation has contravened the PDPA. This would encourage organisations to make use of this mode of addressing possible contraventions without affecting the ability of PDPC to enforce undertakings or investigate the underlying breach.
Part V: Strengthening Effectiveness of Enforcement (paras 68 to 70)	Referrals to mediation	**Introduction of power to approve one or more mediation scheme(s) and provisions for operator(s) of mediation scheme(s)** The Committee concurs with the proposal to fortify the use of mediation as a means of expedient dispute resolution. Since the mediation is against the backdrop primarily of dealing with disputes under the PDPA, the Committee is **strongly of the view** that all mediation schemes must include arrangements where a

Section/Paras of the Paper	Issue at a Glance	Comments
		Singapore law qualified legal advisor is required to assist in the preparation and review of mediated resolutions save where the mediator himself / herself is a Singapore law qualified legal advisor. This is to ensure that any mediation agreement is determined as enforceable and compatible with the legal basis and framework of the PDPA.
Part VI: Others (paras 71 to 73)	Preservation of personal data requested pursuant to access and porting requests	**<u>Requirement for organisations to preserve personal data requested pursuant to an access request for prescribed period (para 72 of the Paper)</u>** The MCI/PDPC may wish to clarify the interaction between the proposed preservation obligation and the existing Retention Obligation under the PDPA (presumably the preservation obligation would constitute "legal purposes" for retention under section 25 PDPA), for example: (a) First, data intermediaries of an organisation may process the information to which access has been requested. The MCI/PDPC may therefore wish to clarify that the preservation obligation extends to data intermediaries, perhaps on notice by the instructing organisation (or similar). By comparison, the Retention Obligation expressly applies to data intermediaries by virtue of Section 4(2) PDPA. (b) Second, where an organisation has scheduled periodic disposal or deletion of personal data (e.g. as part of a corporate retention schedule), the MCI/PDPC may wish to consider obliging the organisation to identify the requested personal data "as soon as reasonably possible after receiving the access request" (cf. para 15.39 of Chapter 15 of the *ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PDPA (revised 9 October 2019)*) and ensure that the personal data requested is preserved while the organisation processes the access request. In this regard, there is also a tension with the Retention Obligation in that organisations ought not to preserve personal data "just in case" possible access requests need to be met: cf. para 15.40, *ibid*. (c) Third, the MCI/PDPC may also wish to clarify how the organisation may be apprised on *when in time exactly* the right of the individual to apply for reconsideration and/or appeal can be

Section/Paras of the Paper	Issue at a Glance	Comments
		considered to have "been exhausted", so that the organisation may lawfully (subject to the Retention Obligation) proceed to destroy or anonymise the personal data in question. In addition to the above issues, the MCI/PDPC may also wish to consider addressing the costs for preservation, and whether they should be borne by the requesting individual. In particular, should cost allocation be left to contract and/or to be stated in privacy policies (e.g. as part of the notification regime)? This may need to be compared with the position taken under the data portability provisions – for example, in the *Response to Feedback on the Public Consultation on Proposed Data Portability and Data Innovation Provisions (Issued 20 January 2020)*, the PDPC suggested that the PDPC does not intend to prescribe the fees that organisations may charge for data porting, but will provide guidance in Advisory Guidelines. For our present purposes, would a similar position be taken for preservation costs under the proposed section 32A of the Principal Act?
Part VI: Others (paras 74 and 75)	Prohibitions to providing access	**Third Party Data Forming Part of Ported Data** Individuals may not be aware that personal data of third parties may be included. Individuals should be made aware of this fact and be required to give express instructions or directions to release such data whether as part of the data porting or personal access request. Measures should be in place to obscure or anonymise such data if the individual elects not to do so. On the basis that the data being ported is personal to the individual, and is being transferred at the direction of the individual, it is logical that data that can identify a third party can be included as part of the data to be ported. However, there must be sufficient safeguards in place to inform the individual that such data can identify third parties and the individual should expressly direct the porting organisation to port such data. There should be measures in place to obscure or anonymise such data if the individual elects not to do so. The same should be applied to personal access requests.
Part VI: Others (paras 76 and 77)	Excluding "derived personal data" from Correction and Data Portability Obligations	It is not clear that excluding "derived personal data" from data portability would serve the goal of preventing or at least reducing prejudice caused by "fast followers", individuals appear to still be able to get access to "derived personal data" and pass this on to the receiving organisation. The existing exclusion of personal data that "if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation"

Section/Paras of the Paper	Issue at a Glance	Comments
		appears to be sufficient although this may still result in disagreements over what would be "confidential commercial information" and whether the disclosure would "harm the competitive position of the organisation". Given the alleged confidential nature of the information, individuals and the receiving organisation are unlikely to get sufficient information to challenge the assertion. A separate dispute resolution process may be required.
Part VI: Others (paras 78 to 81)	Revised exceptions to Consent Obligation	The streamlining and consolidation of the exceptions to consent are welcome as they simplify where consent is not required for the collection, use and disclosure of personal data, collectively and separately.

PREPARED BY THE LAW SOCIETY'S CYBERSECURITY AND DATA PROTECTION COMMITTEE