CONSOLIDATED COMMENTS TO SPECIFIC QUESTIONS

Comments received on Question 1: Do you have any views / comments on the impact of the proposed DP law on specific sectors? Do you have any suggestions on measures to mitigate this or any other anticipated impact?	
S/n	Comments
1	The proposed legislation does not specifically mention biomedical research conducted by academic researchers. They include health surveys, and other studies like cohort studies that require personal ID for tracking purposes. One of the means of contact is the use of telephones in some of the surveys. Perhaps, this may be covered by the proposed legislation on Biomedical Research, and as such, a clause to indicate its exemption from this particular Bill would be helpful so as not to confuse researchers and subjects. The need for a good DP Framework to cover such research is necessary and useful, to protect and assure both researchers and potential subjects.
2	I think that the model for the laws can be effectively implemented.
Comments received on Question 2: With reference to paragraph 3.8, do you have any views / comments on the concurrent application of the DP law with existing sectoral regulations?	
S/n	Comments
1	I think that the model for the laws can be effectively implemented.
Comments received on Question 3: Do you have any views / comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11?	
S/n	Comments
1	Among the personal identifiable information (PII) such as NRIC, email address and mobile phone, it is NRIC that deserves urgent and full attention. This is because the NRIC is used for many commercial and legal transactions, including SingPass authentication, and may be easily obtained by various means i.e. running sms-based contests, dumpster diving for various receipts (many loyalty cards use that as the unique identifier), obtaining old sign-in log books of building visitors, etc. These are just some of the more obvious and easy means of obtaining the NRIC and can be subsequently used for fraud, identity theft and other illegal activities. The DP Law needs to put a stop to needless collection of such data, and allow for businesses to transition their processes and systems towards including checks and balances and strict policies on the collection, use and systemic disposal of these data when it is no longer needed. In certain industries where the impact of privacy is great e.g. financial or healthcare, businesses should be encouraged to either encrypt, mask or store an algorithmically hashed copy of this information. Casual use of the NRIC should be discouraged e.g. as login userids.
2	Definition of personal data looks adequate.

3	We are a data firm that stores business data/ directories of individuals. This is strictly - Business Phone - Business Email - Company Name The are a great many companies specifically in the USA etc. like Jigsaw, Dun and Bradstreet, OneSource that do the same thing. This business is critical for the functioning of the information technology product industries, as a vast majority of them including companies like Oracle etc. use these methods to commucnaite with their potential customers. A good definition of hat is personal date or What IS NOT personal data is required.
4	I think it is wise for the regulations NOT to prescribe specific examples of what and what isn't PII/SPI. Technology changes to fast for regulations to keep up these days and by leaving the definition open a bit you can easily cover future PII/SPI points. As I said in comment 1 I think things like email need to be covered since that is one primary way we communicate today and thus creates a persona about us.
5	I assume that personal data that will be kept secure will include basics such as name, address and phone number (as is the definition in the UK). I would further seek that no holder of that information may charge not to release it to the public domain. The current situation with many telecom providers and listing companies is that a private individual must pay them a recurring fee to return to their default state of anonymity. In doing so they are operating a process similar to extortion or blackmail. Ideally the use of personal data for any purpose other than the primary contact needs of the business or organisation that holds it should be an "opt in" system by default rather than an "opt out". Great work on this, I am glad that Singapore is coming in line with International levels of personal privacy. Thank you.

Comments received on Question 4: With reference to paragraphs 3.15 to 3.16, do you have any views / comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views / comments on the proposed approach to the protection of personal data of the deceased?	
S/n	Comments
1	Privacy of deceased records is important as this can also be used for fraudulent activities. However, I believe that this can only take place in small incremental steps as the use case scenarios are not immediately obvious. As a start, I believe that it may be sufficient to

	provide some means to electronically identify if a person involved in a transaction appears in the death registry. This needs to come from a trusted centralized source such as the Registry of Death rather than the organisation's own customer records which is not authoritative.
2	I think it would be difficult to check who has deceased. Would companies be obliged to check the Registry of Births and Deaths? There is a fee to check on persons within the register. My preference would be for all companies to treat the data for living and dead persons equally, instead of inserting another layer for deceased persons.
3	I think the regulation SHOULD cover the deceased for a undetermined time. We are seeing major fraud in the US when it comes to the decreased and by hopefully creating an explicit opt-in standard for data belonging to anyone you could easily help diminish the abuse of deceased data since it shot;don't be captured, stored, processed anymore.
Comments received on Question 5: Do you have any views / comments on the proposed organisations covered by the DP law?	
S/n	Comments
1	As a start, I feel the types of organizations covered in the proposed DP law (for the private sector) is comprehensive enough. However, as a complementary effort, the DP framework governing the public sector needs to either be reassessed or addressed further. One might logically conclude that the effects of unsolicited marketing activities are the consumers' own doing as they are the ones who provided the data in the first place. However, as an individual who almost never freely gives up her personal particulars and contact information through surveys and such, I too have fallen victim to such intrusive activities on a daily basis due to the "illegal" transmission of data through merchants and organizations that make it mandatory for one to fill out some form of paperwork. This is a sever breach of trust, as I believe most consumers have no idea as to how their particulars got passed around in the first place. With this framework, I hope it will give data management some structure. The opt-out process will only be successful if the general public is fully made aware and properly educated. In particular, I hope proposed DP law will cover (probable) instances where: • Telcos, banks sell customers' basic data to private companies providing SMS/telephone/fax marketing solutions • Employees of telcos, banks, public organizations engaging in the illegal trading of private information as a result of their privileged roles in the company, that allow them access to such information • Telcos, banks, etc. outsource their telephone/SMS marketing to smaller private companies • Inter-merchant/agency trading of information The examples listed above far from exhaustive. However, in order for the DP law to successfully take flight, a strong partnership between the smallest merchants (e.g. recording one's particulars during the purchase and selling of a used mobile phone) and the largest organizations must be fostered. The government needs to come down hard on individuals and organizations who flout these

	practices that in extreme cases, cause severe day-to-day inconveniences to individuals. Thank you for putting the public's views into consideration. Looking forward to the passing of this in Parliament.
2	Please apply this to all organisations. Exclusions for low turnover organisations just present a loophole for someone to create a shell company to do their marketing for them. Please do not allow this to happen. I'm not sure that "light touch" is the way to go. Many laws in Singapore have been crafted and then administered with a "light touch". This creates uncertainty in the market. Laws written should be strictly enforced, otherwise the law should not be passed. Administrative discretion makes a mockery of the rule of law and opens the way to abuse. In this case, strong action should be taken to enforce the letter and the spirit of the law once an individual complains.
3	I am of the view that all entities should be covered, large and small, government or private. If small SMEs are exempted, then businesses would "go small" in order to go under the radar and avoid regulation. e.g., data miners would keep turnover small, etc. The other issue is one of detection and enforcement by MICA. I am sure Minister will not have time or resources to go after the small businesses who violate the DP Law . I suspect also that the businesses who will more likely violate the DP law will be the SMEs due primarily to their ignorance of the law. On the other hand, large companies such as MNCs would have DP management systems to manage such issue. As for public sector, the government should compel all government agencies to comply with DP law too. This is to assure the population that their private data is safe in the hands of the government. Maybe specific regulation would be needed to regulate the public sector, but it should not be left to "internal guidelines".
Comments received on Question 6: With reference to paragraphs 3.20 to 3.22, do you have any views / comments as to whether the DP law should extend to organisations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore? Do you have any suggestions as to how the DP law could be implemented if it should apply to such organisations?	
S/n	Comments
1	My comments are as follow: 1. Increasingly organisations do engage foreign telemarketing companies to undertake the telemarketing function. Besides holding these primary organisations responsible for the collection and processing of personal data, there should be a provision that extends the reach of the DP law to such contracted foreign businesses, but not limited to telemarketing companies, that collect, process and use personal data. They should similarly be subjected to Singapore law so long as the set of personal data can identify a natural person in Singapore.

	2. Extending the above explanation, should a contracted foreign business ignores or refuses to comply with the requirements of the proposed DP law, a separate provision should compel the primary organisation to take necessary steps to prevent abuse of personal data by the contracted foreign business partner.
2	It would be easy for a Singapore telemarketing company to circumvent regulation by hiring or outsourcing a company say in Malaysia or India to undertake the telemarketing. In that sense, it would work better if the laws could protect the consumer if the Singapore companies hiring the telemarketers were held responsible. 3rd party telemarketing companies are often hired on behalf of a bank to do their marketing - it has to be clear who the law is addressing: just the messenger, or the actual source of the message; or both. It would deter banks and other institutions and oblige them to be more careful on data collection and usage if they had to comply, regardless of where or how they send the message. So yes, I would suggest that the law extends to Singapore companies regardless of where their calls are made from.
3	It is hard to enforce the law on entities outside of Singapore. Should the law cover these entities and their agents? As a matter of principle, they should. Should these entities or their agents subsequently operate in Singapore, enforcement action can be taken against them. However, it is probably more important to restrict the sale, distribution, transmission of information to entities not registered in Singapore. This should be made an offence. Some companies may put their data centers overseas. So long as the data is demonstrably under their control, and they continue to be responsible for the use and misuse of the data, this can be allowed.
4	All organisations even those outside Singapore should be regulated. If not, the culprits would move their business offshore (Indonesia, etc) to do the same thing out of the reach of MICA. Whilst enforcement will be difficult, but at least the law is in place to regulate this problem.
5	Overall I think the regulations should apply to ANYONE/ANYTHING who collects and processes data on citizens of Singapore. Today we are very aware that the Internet doesn't understand bounds and we need to begin to look at applying data protection standards no matter where they are located. now, the issue arises on how we then apply and enforce that on others say in the US. I suggest that you apply standards to companies regardless where they are and if needed impose sanctions or bar those companies who don't follow the regulations from doing business in Singapore which might even include banning their web addresses from being seen.

Comments received on Question 7: Do you have any views / comments on the proposed general exclusions from the DP law?	
S/n	Comments
1	Information on a persons business card, should be excluded form coverage Business data like 1. Name 2. Email 3. Business phone Rationale: a. Business data is generally considered NOT CONFIDENTIAL b. company employees and staff know it c. He will not be compromised in any way if people know he is working at X OR Y d. It is necessary for various checks like employment verification, etc. etc. e. Necessary fro trace and commerce f. It is increasingly available through sources like LinkedIn and other means like green book etc.
Comments received on Question 8: With reference to paragraph 3.26, do you have any views / comments as to whether there should be exclusions for artistic and literary purposes under the DP Act? How should these exclusions be defined if exclusions for artistic and literary purposes should be provided for?	
S/n	Comments
	Nil
Comments received on Question 9: Are there any other exclusions that should be catered for under the DP Act?	
S/n	Comments
1	I worry that by building exemptions that you will see people use that as an excuse to not protect things like email address and the like. I think that companies must realize that in this day of age in terms of increasing data breaches they need to protect data AND I think with the ongoing collection and sharing much gain permission to process any data.
Comments received on Question 10: Do you have any views / comments on the proposed general rules under the DP law?	
S/n	Comments
1	This is important. Many organisations collect NRIC numbers, date of birth, etc. etc. completely unnecessary for the provision of services. This is wrong and dangerous because may banking and finance organisations, and public sector ones as well, depend on this information to identify a person, and an unnecessary distribution of such information facilitates identity theft.

2	1) I strongly support clause 3.31 where "an organisation may not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal data beyond what is necessary to provide the product or service". It is not uncommon to see large organizations, including Banks (which are supposed to comply with the banking secrecy requirements of the Banking Act (Cap 19)) put in additional disclose-as-they-wish clauses in their agreements with consumer. Organizations, banks & telcos included, should be prohibited from requiring consumers to consent to disclosure regimes that offer less confidentiality than what the proposed DP Law and other sectoral laws (e.g., Banking Act) require. I cite 2 examples below from the Banking sector that appears to contravene the banking secrecy requirements. a) From [redacted] Loan Offer agreement: "Without detracting from the Bank's rights of disclosure under law including the Banking Act (Cap. 19) and under the Terms & Conditions Governing Accounts & Services, the Bank is given the further authority by you to make all disclosures whatsoever and for such purposes as the Bank sees fit in respect of the accounts or other transactions which you have with the Bank to:- ... (g) any other person or body to whom the Bank considers such disclosure to be necessary or expedient." b) From [redacted] Loan offer agreement: "You hereby consent to the Bank disclosing, from time to time without notice and whether before or after termination of your accounts/facilities/Facility, any information and data relating to you and/or your accounts/facilities/Facility/securities/guarantees (whether held singly or jointly with any other person) to any party, whether in Singapore or elsewhere, for such purpose as the Bank in its discretion thinks fit." The DP law must unequivocally prohibit organizations from requiring consumers to consent to such 'above the law' disclosure regimes as a condition of supplying their product or service.
3	One of the companies that we run is an recruitment agency. Personal résumés were sent in response to advertisement It will be onerous to company with the law under such circumstances as no centralized system exists to track the resume and their contents
4	Referring to Point 3.38, or elsewhere, the accountability to comply with DP law should also provide a reasonable time frame (eg. 14 days for individual requests for deletion of personal data or 30 days for legal consultation and make good of organisational compliance procedures) for organisations or their appointed individuals to act and make good any requests or demands.

5	3.32: Consent should always be explicit. Circumstances where consent such as in 3.33 and 3.34 may be implicit should be specifically defined in the DP Framework. 3.38: Organizations should be accountable to all individuals whom they have personal information on. This should include them having to disclose their sources of information (i.e. from whom/where the organization received the individual's personal data) as well as recipients (i.e. whom/where the organization sent the individual's personal data), failing which the organization should be held criminally liable for infringing on the privacy rights of the individual.
Comments received on Question 11: With reference to paragraph 3.35, do you have any views / comments as to whether individuals should be deemed to have given consent for organisations to collect, use or disclose their personal data if they are notified and given reasonable time to opt out but do not?	
S/n	Comments
1	We should not have to "Opt-Out" or "Unsubscribe" to any email/marketing calls if we did not explicitly "Opt-In" in the 1st place! Silence does not mean consent!
2	More often or not, consumers' personal data are also disclosed to third parties for commercial purposes, most likely to have commercial gain. Nowadays, it is not unusual for consumers to receive phone calls from some organizations which the particular consumer has no contact before – when queried how do they obtain the personal data (e.g. name, handphone numbers…etc), the callers would refuse to specify, or just say "it's in our database". Rules and regulations should be imposed to restrict the organizations to disclose consumers' data to any third parties.
3	Privacy should always be opt-in, unless overriden by urgent circumstances such as the Infectious Diseases Act. Marketing activities are not considered urgent circumstances. All such exclusions need to be clearly spelt out by the DP Law. Most importantly, many such privacy notices are written in a legalistic way. Where possible, organisations should provide these in simple English so that all consumers are left with no doubt about the ambiguity of the collection, usage and retention of the personal identifiable information (PII). The enforcement of withdrawals of consent is not an easy thing to do. Similar to CASE who handles consumer purchase complaints, there needs to be a third-party authority where such grievances can be redressed. Hopefully, the DP Law will also identify deterrants for those who shows a record of poor enforcement of privacy law.
4	It is unfair to the consumer to say that they should choose to opt out. This is because at times, certain data collection companies (eg., lucky draw organisers, businesses holding a promotion) merely "inform" the user that their information will be shared, with 1) no indication of whom the data will be shared with, and 2) no option for the user to opt out. In such instances, opting out means giving up the chance to use the service. This is not good for the business or the individuals.

	It is thus proposed that data collectors offer an option for the user to opt out, or to at least allow the user to indicate their area of interests. A person who indicates in the form his interest in real estate may, for instance, be deemed to have consented to his data being obtained by a real estate agent, but not by an automobile company. Data collected before this regulation is implemented will be governed by existing regulations.
5	It should never be the responsibility of individuals to "opt-out". It is the job of the organizations to convince individuals to "opt-in" instead. Unless explicitly allowed by individuals, organizations should never have the right to collect, use or disclose personal data.
6	Please do not have deemed consent. It is wrong to place the onus on the individual. Also this should apply to data collection via electronic means where "check boxes" granting consent are already "ticked" so that an unwary consumer discovers that he has consented without consciously making a decision.
7	With regard to 3.35, I agree that it is unreasonable to place the burden of establishing consent on the individuals. As a principle underpinning the DP Act, burden of establishing consent should rest with the organization. The DP Act should explicitly spell out that by default, if an organization is unable to establish consent, then the organization is not allowed to disclose that individual's personal information.
8	On the balance, Opt Out method is easier for businesses. As for consumer, if the DP law works properly, consumer always has the right to request the business to stop collecting or using his personal information (so there is protection for the consumer). MICA may want to issue guidelines as to what constitutes Opt Out. Example, when filling an online form, and the check box for "do you want more information" is by default checked (but user can uncheck if he wants), would this be considered Opt Out? (I think the answer is "yes").
9	opt-in is the only way to go these days. Unfortunately with email and other communication based technologies, they can't always be reliable. Emails breaks, gets junked, blocked, etc. I also feel that companies will abuse a opt-out approach like they do now in the US by say we tried, but to what level did they try? explicit opt-in is the way to go
10	As an organization we have worked with opt-out schemes in the US for quite some time, and there is limited burden on an individual as long as he is made aware of how an opt-out notice may be given to the organization (post and email addresses provided by the organization plus links in electronic messages can make this painless), and as long as there is no timeframe by which such an opt-out notice must be given (the individual should always have the right to opt-out of unsolicited commercial messages).

11	The opt-out approach of consent can be problematic for persons who are not fluent with the law, are not informed of this approach, or who are simply ignorant that such a provision exist. It becomes more tedious to inform individuals and establish consent if communication is difficult due to language or other barriers. This is more so if that natural person is deceased and has previously not established an enduring power of attorney.
Comments received on Question 12: Do you have any views / comments on the proposed rules on collection, use and disclosure of personal data?	
S/n	Comments
1	I really welcome the intent of the proposed Data Protection regime. There is currently a very widespread practice of requiring the NRIC number for any submission. This could range from as trivial a transaction as an SMS entry to a radio/TV talkshow or a lucky draw coupon at a supermarket to a really important legal/financial document. If some sort of verifiable identification is required, could (say) the last 4 digits in the NRIC suffice (like what is only now being adopted for credit card numbers printed on acknowledgment slips)? This, together with the name could be used to verify the individual, and then only if required. While I fully support NRIC disclosure for legal/financial transactions, I wonder if it should be allowed to be so freely asked for and disclosed for the more trivial matters. Would this not increase the size of the problem unnecessarily by increasing the amount of data to protect?
2	The proposed rules also does not state a preference for aggregated data as opposed to individual data. Organisations should be encouraged to store the personal data for record/investigative purpose and use an aggregated form of these data wherever possible, especially for non-critical functions such as marketing purposes. The proposed rules as specified in 3.53 also seems to be very vague on what are those "unique circumstances" where public agencies may be exempted from the DP Law, other than one reasonable example in the form of public justice. The clause in 3.18 also seems to imply that the public sector may be governed by a different privacy regime from the private sector. If this is to be the case, the public sector needs to standardise on what is the baseline used across all agencies and what exactly is this information used for as this is not evident today. To give a very simple example, compare the [redacted] "Feedback" function [redacted] and [redacted] "Feedback" function [redacted] - why does [redacted] require Contact and Email to be mandatory fields while [redacted] does not, and what does [redacted] intend to do with these mandatary data from the Contact and Email fields? The privacy statements used by all agencies will need to provide more transparency on this process for the public sector to be effectively governed by a separate privacy regime.

3	3.46 The DP Act also recognises that the collection of personal data without consent may be necessary to enable certain organisations to perform their functions effectively. For example, when an individual has consented to organisations' disclosure of his or her personal data for a credit report, a credit bureau compiling the credit report would not need to obtain additional consent to collect the personal data. [redacted]: Currently, consent is required from the individual (ie consumer) before we can release the credit report to a 3rd party.
4	The requirements appear onerous, and therefore a good definition, is vital Leaving it ambiguous will lead to all kinds of misinterpretation. A more / well framed definition is required to prevent frivolous legal activity/ ;lawsuits etc. E.g. Is a business phone number considered as personal data?
5	3.41: Verbal agreements never stand up in court and hence should never be allowed. Only written consent from the individual should be allowed. 3.42: As with 3.32, special circumstances should be specifically defined. 3.44: What constitutes as "employee personal data" must be specifically defined.
Comments received on Question 13: Do you have any views / comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organisations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organisation? Are there any other exceptions that should be provided?	
S/n	Comments
1	Where personal information is provided to an organization by an individual the organization should not need additional consent for use of that information in furtherance of the business relationship that then exists with that individual, whether that is for future contact with the individual (unless that individual has opted-out of such communications) or for internal use within the organization.
2	3.45: Organizations should exercise due diligence in protecting and using member information. Whilst organizations could be exempted from seeking explicit consent in collecting members' information, permission should still be sought from the individuals before their personal data is used.

	3.46: Individuals should be allowed to "opt-in". 3.47 & 3.48: Organizations should still be held accountable and disclose their sources of information as well as recipients (See 3.38). 3.53: Outside of national security and defense, consent should always be sought before disclosure. Too much leeway is currently given to the police and law enforcement agencies that fundamental rights to privacy are often neglected.
Comments received on Question 14: Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined at paragraphs 3.60 to 3.61?	
S/n	Comments
1	Businesses should have the sense to engage reliable service providers, and ensure that data is well protected, via means such as having the providers sign a non disclosure agreement. Therefore, it makes no business sense to dictate whom they may or may not deal with. Indeed, doing so may even affect their business. Agree that the current recommendation is sufficient on this aspect, that companies should exercise due diligence by themselves in protecting these info.
2	If we upload teh data to a website in the cloud. We have no way of knowing where the data is residing. It is managed by the cloud. It will then be difficult to know what is inside and what is outside Singapore
3	On one hand yes I do since it makes my and customers jobs easier, but on the other I worry about abuse without some sort of adequacy ruling. Seems today that without that sort of process that you won't be able to go after those who abuse the information. I am against BCR though as they take to long and usually are unnecessary and take up deal time if both side already know what they have to do like in the EU. With BCR's attorneys will go back and forth for days when a simple adequacy ruling would suffice
4	Individuals must give consent before their personal data can be transferred overseas. It should be the responsibility of the individual to decide whether the jurisdiction is safe to send their personal data.
Comments received on Question 15: Do you have any views / comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67?	
S/n	Comments
1	I agree that retention and records management for personal data is important and makes the burden of privacy data record-keeping bearable. From a practical application perspective, Singapore does not yet have any standards or specification for records

	management (RM) like DOD 5015.2, MoReq2 and VERS - the closest equivalent may be industry standards like HIPAA or the Electronic Transaction Act (ETA). Organisations in Singapore are also not educated on the difference between archival and records management, and most of them are merely doing some form of tiered archival and backup which is not complying to proper disposal of privacy data. Thus, the legal or regulatory framework may need to work towards a specification for RM which serves as a baseline for privacy records (or any other records). Organisations may also need to be incentivised to go for education from experts such as the National Archives, so that they can develop their own corporate retention scheme as policy.
2	As a recruitment company it will be very difficult to comply . Data about individuals sit in over 100 PCS distributed in the home and in the office It will be difficult to ascertain and hence comply with this
Comments received on Question 16: With reference to paragraph 3.67, do you have any views / comments as to whether organisations should be required to specify the retention period when collecting personal data?	
S/n	Comments
1	Yes, organisations should either state the retention period upfront, or declare the presence of a retention scheme internally. This will force organisations to think about whether they really need to collect such a data, and also consider adopting a "default rule" as a baseline for managing the lifecycle of such data.
2	It is not practical to stipulate duration of information. Consumers will also start to compare why company A keeps information for 3 months, while another keeps it for 3 years. Better to leave it to the business to decide. It should suffice if the DP law has an obligation upon business to make the private information no longer traceable to the individual, after it has no longer any use for it.
3	As long as an individual has an on-going opt-out right, a limited period of retention is unnecessary and can be burdensome on and costly to the organization (especially in light of the fact that individuals will sometimes “play the system,” and an organization’s inability to keep a history would make it that much more vulnerable).
Comments received on Question 17: Do you have any views / comments on the proposed rules on access to and correction of personal data?	
S/n	Comments
1	As a recruitment company we get tonnes of personal data every day. It will be very onerous to comply with this as the data is not sit on one central system, but spread over 100 PCS

Comments received on Question 18: Do you have any views / comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism?	
S/n	Comments
	Nil
Comments received on Question 19: Do you have any views / comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views / comments on the criteria for breaches that would warrant financial penalties?	
S/n	Comments
	Nil
Comments received on Question 20: Do you have any suggestions on specific guidelines that the DPC should provide to help organisations achieve compliance with the DP law?	
S/n	Comments
1	Subsidiary Regulations, Codes of Practice, Guidelines, etc should be made public without payment of fee, and they should be easily accessible. MICA should make it clear about the legally binding effect of the COP and Guidelines by a clear statement to that effect at the start of the document. This is to provide certainty to the business and consumer.
Comments received on Question 21: With reference to paragraphs 4.11 to 4.14, do you have any views / comments as to whether a one to two year "sunrise" period would be appropriate?	
S/n	Comments
1	1 year would be sufficient for implementation. 2 years is a bit long, and I think it will give businesses too long a runway to gather as much private data as possible to be grandfathered under "Existing Personal Data".
2	I think a two year period. I doubt if vast sections of the industry are even aware of what personal data means. I suggest a greater and more inclusive discussion with sectors be called for and a more informal discussion. This should be done in phases

Comments received on Question 22: With reference to paragraphs 4.15 to 4.19, do you have any views / comments on the proposed treatment of existing personal data?	
S/n	Comments
1	Absolutely not. Currently individuals have no idea as to which organizations have their personal data and where their personal data has been sent to. It is imperative that organizations seek consent from individuals at the enforcement of the DP Act.
2	With regard to existing collected data, Mica proposes to deem that consent was previously obtained. After the legislation comes into effect, however, fresh consent must be sought if an organisation intends to use existing personal data for a new or different purpose. (from Business Times article) Feedback: It should not be deemed that consent was previously obtained with regard to existing collected data. This enables the organisation to use existing personal data as long as the purpose is the same (e.g. to advertise) even though before the law came into effect, the person may not have consented. By the new law, he, unfortunately, is deemed to have consented. The law should start on a fresh slate. Anyone who registers after the law comes into effect is deemed to have not consented to use of personal data for whatever purpose, whether his data was previously used before the law came into effect or after.
Comments received on Question 23: Are there certain organisations that may require different transitional arrangements?	
S/n	Comments
	Nil
Comments received on Question 24: Do you have any views / comments as to whether a National Do-Not-Call registry should be set up in Singapore?	
S/n	Comments
1	YES, PLEASE! I feel very strongly that a National DNC Registry needs to be set up. It's high time. I am often plagued by unwanted calls from property agents, insurance agents, and other such like nuisance people who are trying to sell something or other, not only on the land line but also on my mobile. These people are a big nuisance and a waste of my time. I am tired of scolding them. The worst of the lot are the property agents. One agent after another from the same company will call. There must be a way to stop them from bothering us.
2	I am strongly in favour of setting up a DNC registry for the following reasons: 1. Time Savings for Both Companies and Individuals The DNC registry will provide individuals who are not interested in advertising to opt-out and this will save time on both the company and individual. Most individuals who are not interested in products that are advertised via telemarketing will politely refuse and hang up when called by a telemarketer. However, there are those who are either

	shy or do not feel comfortable rejecting another individual straight up. This will cause them undue stress as they struggle to try and get an enthusiastic telemarketer to hang up or give up. These individuals who are not interested will also not tend to purchase the products that are advertised. This means that the telemarketer might spend 10-15 minutes and be chasing a lead that will never close the deal. 2. Win-Win-Win Solution The DNC registry is one that is opt-in. This means that only individuals who wish to opt-in will be in it. For those who do not care or do not mind receiving advertising, they will still be contactable by businesses who advertise via telemarketing. This is a win for the businesses. The second win would be for individuals who are interested to opt-out of advertising. They will be able to do so, and such, save their own time and save the time of businesses. This is a win for the businesses and the individual. Thirdly, consumers can be on the DNC registry, AND at the same time choose to receive advertisements from select companies. For example, to receive offers from their mobile phone provider or ISP. This means that the individual will be able to choose what they are interested in, and receive adverts based on that, which means that the purchase rate will be higher and companies will be more efficient in their telemarketing efforts. 3. International Standard Many countries have already implemented a National Call List. Namely (from Wikipedia): • Do Not Call Register (Australia) • National Do Not Call List (Canada) • New Zealand Name Removal Service • Telephone Preference Service (United Kingdom) • National Do Not Call Registry (United States) • Bel me niet register (Don't call me Registry) (The Netherlands) This is something that is widely appreciated and accepted and it will be a good idea to have it in Singapore as well. 4. Personal Interest Personally, I have been keeping track of this issue and I have also hoped that Singapore will have a DNC Registry as well. This day has finally come and I am totally in support for it. I sincerely hope that the Ministry of Information, Communications and the Arts will consider the implementation of the Do-Not-Call Registry.
3	1) There must be a proper avenue for consumers to report SPAMMERS.

	2) There must be an authority in place to enforce a jail penalty or a heavy fine tough enough to deter potential SPAMMERS. If MICA cannot enforce the above, the Do-Not-Call proposal will just be another USELESS FOR SHOW ONLY policy for SPAMMERS to laugh their ass off.
4	Thanks you for this long overdue initiative!!!! Love you lots for this and please get it up and running asap! I want to register myself!
5	Read the article on Yahoo News. I am supportive of this initiative. :) I suggest that anyone/company that violates this law may be fined and compensate even the consumer (ie the recepient of the SMS). For instance, whenever I receive irritating SMSes, I wished that I can forward it to a Governmental body or Police who can investigate how my number ever got there. Several times, I replied UN or un to unsubscribe and they still SMS me. Also, telemarketing is even worse. Cos they can call ANYTIME and you are forced to pick up (compared to SMS where you can reply later). Calls can come in the middle of meeting or dealing with important clients. The advertisers should be fined and compensate the recipient. It is frustrating and irritating. Although one can argue to say that you can ignore it if you don't want it, it is irritating... it is analogous to salesmen knocking on your door frequently to sell stuff or services. You can ignore them if you don't want to open or buy but the problem is you gotta see or answer it to know that it is not something important; cos the "door" (like the phone) is where important things come from too. And being "forced" to look or answer or entertain to check if there is something important is disruptive and frustrating. Another possible law to address this is that we can have a registry for recipents (HP owners) who are willing to receive SMS adverts for a fee by the senders (advertisers). So for instance, if I'm on this registry, for each Advert I receive, the sender has to pay me $5 (for telemarketing calls) $1 or or $0.50 (to receive an SMS). So advertisers have to be selective and send only if they feel it is worth it (instead of free flow spamming). And recepients get a bit of consolation if an unrelated SMS advert comes along and disrupts their daily activity, or causes unnecessary fright (eg someone working but relative sick and jumps at every phone call or SMS, fearing that something bad happened and the hospital called).
6	Regarding the National Do-Not-Call registry: it is also important that individuals are able to identify the responsible telemarketing companies directly. Telemarketing activities are often outsourced to multiple third-party companies that could even be based outside Singapore. This "loophole" can easily be exploited to continue sending unsolicited messages to Singaporeans regardless of the new

	law. Telemarketing companies, national or international, should be held directly accountable for their actions. Every commercial message or call should come with the name of the telemarketing company, to allow the consumers to identify and keep track of the companies that have been sending the messages. This mobilises the public to help the government with the enforcement of the new law and identify potential (repeat) offenders. In addition Singtel, Starhub, M1 and other communication service providers have a key responsibility to block offenders from continuing their telemarketing activities/companies and getting new telephone lines after breaking the rules to continue their malpractices. Currently it is far to easy to set up a new call-center even after repeated violations because there is no "blacklist". Foreign-based telemarketing companies can also easily circumvent any regulations or laws because our telcos do not take any action.
7	Yes, fully agree with a Do-Not-Call registry. In fact, this should not just be restricted to calls through phone calls and sms, but should also be extended to cover snail mails and faxes.
8	Individuals who receive unsolicited calls from telemarketers or any other organization should have every right to prosecute that organization for illegally acquiring their personal data. A "Do-Not-Call" registry again places the onus on the individuals as compared to the organizations holding their personal data.
9	Yes, it should be set up. This prevent nuisance call from organisation that may have purchase personal data from another company for the purpose of telemarketing. Consumer must be given the authority to decide if they should receive such info.
10	I had for the past 2 months received about 5 unsolicited calls from insurance company, bank and other business entity. When asked about how they obtained my phone number, they said my 'friends' had provided my number to them but they did not know the name of my 'friend'. With that, it was not genuine that my friend had provided them with my phone number. Perhaps the law should look into this area as well. It could be a way to get around the law.
11	Television-marketeers in the pure sense of the word may not address the problem of cold calls generally. The registry should also apply to insurance agents / property agents / banks etc who data mine personal particulars and call individuals *repeatedly* despite being informed that we are not interested in the services that they are offering. The existence of other regulatory bodies (eg, CEA for estate agents, MAS for banks) should not detract from the proposed registry applying to such industries. ALSO, if a complaints-based model is to be adopted, cold callers should not be allowed to 'hide' behind blocked caller-IDs. this would

	frustrate the lodging of complaints.
12	I would think that it is critical that consumers can opt out of receiving telemarketing calls because it is very intrusive. I think that the law should not be applied to SMSes and Faxes because they are less intrusive, I think that businesses should be allowed to promote their goods and service through these means.
13	Very timely indeed, to put in place this law. The problem with SMS spam & telemarketing calls are so serious today. Some feedback: Section 5: DNC absolutely is a must. DNC must apply to both business, and individuals (eg. agents broadcasting ADV SMS). DNC registration must be made easy for public. Suggest using SingPass for authentication. Section 4: Penalty definitely needed for breach of DNC. Propose 1-2 strikes = warning, 3-4 strikes = fine, >=5 strikes = jail term. Section 4.14: Sunrise period of 1 year is good enough. SMS SPAM is a huge problem today.
14	I read from The Straits Times Online on your plan to implement consumer DP regime for Singapore. I would like to applause and thank you for looking into this seriously. Over the recent years, my colleagues, friends and myself have all been very frustrated receiving unsolicited SMSes, unwanted telephone calls from banks / insurance companies / overseas investment / slimming centers etc. Even with the <UNSUB> feature is just not effective enough! We get even more SMSes from property firms when we UNSUB! The SMS numbers that are used to send us the text messages are different all the time. On average, I am getting 4 SMSes from property firms, personal loan private companies, tuition agencies etc. Recently, I received an unsolicited call from [redacted] Bank trying to sell me their banking services. I asked them where they got my number from. The contact center agent told me their marketing department gave them my number. I told her that I have never ever dealt with [redacted] Bank. So in the first place, I am wondering how did my particulars get passed around ?

	With a contact center background, I know of countries like Australia has very strict laws preventing companies / organizations to call consumers without their prior consent or OPT-IN for emails and SMS permissions. It is time we implement such laws here in Singapore. Otherwise with the advancement of technology and with the ease in which our personal data are being sold for profits; and our data being passed around, we need to put all these under control before things get out of hand.
15	A registry would be an excellent idea. However, it would be easy to circumvent the laws via online calling from a PC or using a phone with no listed number to call. Consumers often cannot identify the callers because their mobile phones show no number. Online technologies enable companies to call via Skype (which registers no number or says "Blocked") and also email blasting can be done via subscription services from overseas based servers. So there is a limitation to what a registry can cover - and telemarketing companies will likely be able to circumvent the law very easily. Suggestions: 1) Perhaps Singapore law can specify that telemarketers MUST provide a viable phone number on display when calling that can be placed on the registry; or a viable email address that can be placed as well. Email is an increasing issue that should be addressed on the same level as phones. I have received emails again and again from the same companies, in spite of unsubscribing or informing them. It is indiscriminate, and the laws need to look at that. 2) Also, what would be helpful is implementing a rule of conduct of how telemarketing, marketing surveys must be conducted. Those who call must immediately identify themselves - name, NRIC and phone number - and perhaps that can help somewhat in making telemarketers aware of their obligations in identifying themselves. 3) Companies should offer an option for the consumer to be taken off their marketing list immediately, should they request it on the phone. I have done so before, but after some waiting and asking for the manager. This option should be built in immediately, so that the need for a registry does not become the only option for consumers.

	Reinforcing better behavior will help to make this work better.
16	I am in full support of the government's proposal on National Do-Not-Call Registry. Hoorah! Finally someone has taken this great initiative to stop all nuisance calls and SMSes. Yes please ensure all organisations not to abuse the consumer's database by selling them and reselling for advertisements or soliciting or worst still scam purposes! Please also include this National Do-Not-Call Registry to all mobile suppliers to name as an example [redacted] and the others etc. Ever since I have changed my service provider from StarHub to SingTel, I have been receiving SMS from [redacted] telling me what wonderful sites are available for my download, etc. I have no interest in this but if I do I will go search for it myself. I do not like or need anyone to "push" any SMS to tell me about it. Obviously if it is a "push SMS" it means that particular offer isn't attractive or is of not use to me. I look forward to this launch and will certainly celebrate it in a big way. Thank you for this initiative.
17	Yes, please set up do not call list. This is long overdue. Also, please ensure company are responsible to heck he list, even if they out soured the calling to telemarketing.
18	Living in Singapore is beginning like HELL! I had so many SPAMS that it costs me money (exceeded my SMS limits) and time. As I travel overseas frequently, several times a week to Malaysia, my roaming SMS is $0.51/SMS or even more in some countries (Vietnam, Cambodia)!!! Many of these spams are totally irrelevant to me. For examples: Buying properties in Orchard costing $8-26M!!! Buying new cars, perfumes, sales, lucky draws, etc. Just do not know how they got my mobile no. They (spammers) disturb my meetings, lunch time, dinner time and even my sleep late at nights about 2.00AM (computer sent?)!!! Some of the banks are resorting to this dirty marketing tactic. Are they trustworthy institutions or just cheap spammers??? Here are some of my suggestions: ========== 1) Fine every spam message, say $10.00 (100 messages is $1,000.00). Must be heavy enough to be deterrence. 2) To make life easy for consumers to report spam, have ONE mobile no. ???????? so that consumers can just forward spam

	messages to. This centre will act on the input. If the spammer can prove that they have the consent of the recipient, then, they must show documents to this centre which decide and reply to the recipient; 3) Limit to only ONE marketing item, say SPA, from the company. The company cannot promote other items such as perfumes, clothing, shoes, bags, car, properties, electronic, etc.… without further authorisation from consumers. This is to prevent disguises – excuse promoting other items. 4) Have all banks and reputable institutions (Uni, colleges, charities, hospitals, clinics, etc.) sign commitment not to spam or make it a LAW. If consumers confidential info are compromise, fine the bank/institution heavily, say $1000.00 per customer (they have lots of money)!!! 5) How do we stop spammers from overseas who sent messages via Internet, and sometime late at night? Any expert to help? 6) Why not have "privacy Law" in Singapore? Just follow other developed countries, no need to reinvent the wheel/laws. I hope we can have some common sense laws to protect our privacy, security (our confidential data can be used to buy products) and peace.
19	I like to give the following feedback on the Do-Not-Call Registry: 1) NRIC numbers are very important information which when fall on the wrong hands could result in dire consequences. All forms requesting for a person's NRIC should only ask for the last 3 or 4 digits with the letter, e.g. XXXX123G or XXX1234A. 2) Restriction on the information to be filled up on lucky draw coupons. Ideally it should only contain NRIC (last 3 or 4 digits with letter), name, gender and a contact number. 3) All forms or coupons must allow customers the option to fill in a telephone or cell or email address. 4) Telco service providers should only allow the use of their sms messaging services on condition that the sender of such services allow the sms message recipients the option to unsubscribe. At the moment some messages come without this option. This is to allow people who do not wish to register themselves for the DNC service but at the same time would like to have a control on what they would like to receive. 5) Subscribers for such a service should not be allowed to change their telco numbers. This is to discourage subscribers from changing their telco numbers when they find that too many of their recipients have unsubscribed to their messages. 6) The "Do-Not-Call" service must also apply to banks, credit card companies as well as insurance companies. I have on many occasions received telemarketing calls when I was overseas despite giving umpteenth instructions for them to remove my cell number from their telemarketing data base.

20	if we provide a long transitional period for companies, some of them will abuse it to continues spam us as the last burst of fire. If companies can not comply to the new "Do not call" registry standards, companies should cease all email/sms/phone advertising immediately. It is not a life and death situation for them as there are other alternative advertising channels. Hence a 3 months grace period is already more than sufficient. Heavy fine should be slapped on errant companies to deter future spamming. S$100/ S$1000 per spam call complaint? the amount should be high enough so that companies will no longer find it worth while to indulge in spam advertising. They should be punished for causing public nuisance and responsible for lowering productivity at work. What right has marketing companies has to sell our contact information away for profit ? They should be severely punished for violating our privacy. Most important thing is to implement this quickly by telling the public, where do we go to enrol for DNC registry ? can we register now?
21	Yes, MICA should set up a DNC Registry. Some things to consider: 1. The registry should offer users a way to filter what they which to receive or not receive, and not just a flat no or yes. For example, while I am not interested in financial products like insurance, credit lines and credit cards, I might want to receive information about new property launches while I'm hunting for a property. Later, after I have found a property, I could then go into the registry and indicate I do not wish to receive any communication about property launches. 2. Expanding on (1), telemarketers could in fact use the registry as a source of interested parties. This would actually work favourably for point 5.6: "telemarketers will benefit by being able to effectively target a genuine group of consumers" and gain more support from organisations.
22	I was agree to STOP them using our mobile no. without our consent to sms or call us from Housing estate or Banks.
23	I would like to applaud the move of MICA to set up a "Do not call" registry and would certainly like to be part of it when it comes online. I have an additional comment to make the law more robust. As consumers, we are often given forms to fill up that would sometimes ask for our personal details. Unknowingly, our details are sold to other companies, as a) there isn't an "opt-out" box we can select, and

	b) there is probably a fine print somewhere in the form that states that they can handle our information in any way they like. What I would like to suggest is that even if consumers had unwittingly given their personal details for a particular purpose and found that it had made its way to the telemarketers, that consumers on the registry can be immediately exempted from the calls. Obviously, if they are called, then the usual fines and penalties should apply to the offending company.
24	Regard the following acts may not be a good move. Our Country is very small and everyone is trying to make a living by calling or educate prospects. Surely a lot of industries such as outsource will be affected, everyone will be out of job.
25	I am 100% for an enforcable National DNC Registry. It will be good for such a DNC registry to have an interactive feature for individual with specific transitional need to opt-in-and-out for selected service or product marketing of their choice as and when the individual desires them (ie the DNC registry must be "interactive" for individual to opt in and out for selected service or products from selected firms as and when they need them, and not the one-switch-opens-all architecture). Vendors are definitely going to save a lot of unneccessary wastes and receipients who have no use for such messages or calls will be spared an incessant nuisance and cost as well (roaming charges for receiving such unwanted sms and calls are very expensive). And one minor incidental benefit at national level may be the freeing of manpower resources for more beneficial work to ease our local "manpower shortage" and potential to cut back on the so-called imported "foreign talents" on EP or WP, not that I share the term "talent" which our government has bestowed on such imports. Thank you for the initiative. I think Minister Lui Tuck Yew may turn out to be one of those so called "leader" that will prove himself to be just that - a leader. Nice work and I like that!
26	Yes! Yes! Thank you! Thank you! Finally. Suffered long enough. Make very sure it covers unsolicited phone calls and sms as indicated in the document.
27	1 - Yes, a national do-not-call registry is needed urgently. 2- Once a number is registered, there must be No exceptions whatsoever to allow unsolicited phone calls and/or messages to that

	registered number. (The newspaper mentioned some possible exceptions. No exceptions must be allowed.
28	Thank you for the opportunity to submit views. Some specific comments, including on the assumptions used as a basis of this consultation: Often, sales calls are made by other units or sub-units of organisations with which a consumer DOES have a relationship. Rather than regulate the flow of such information internally within large corporations, an opt out list is an efficient and effective way to ensure consumers' rights and expressed preferences are respected through a binding mechanism. Regarding the existing Code of Ethics - While industry self regulation through best practice is commendable, these are largely opaque to consumers. There is also no assurance of compliance, nor the ability to police this. I have countless personal experiences where a request to a telemarketeer to remove me from thier list has been met with rude remarks, or they simply hang up. It may be useful to consider requiring such service providers to allow access to recordings of their calls (many do for internal purposes) for audit and investigative purposes. This ensures the regulator has the wherewithal to investigate abuse, but this power need not be flexed except in cases which warrant. This additional layer could help keep service providers honest. I fully support the registry and mechanism and the role of cellular providers should also be considered in this equation. For instance, there could be a technological solution to this where each phone number can be tagged with the preference of whether or not to accept such calls. Telemarketeers' lines should also be registered with telcos, and calls originating from these lines can be blocked to those who have selected that 'no calls from spammers' preference. However, I am not convinced that a separate independent body is required to police this. This is part of the regulatory function of the relevant authority. A unit or department would suffice. If the idea of an independent body is to co-opt industry players to share the burden, this sets the body up for potential moral hazard. A regulatory unit, which regularly publishes its activities and empirical trends for transparency purposes should meet the needs of this policy.
29	The setting up of a national Do-no-call registry will inevitably results in a higher cost and it begs the questions of who will be paying the bills for costs associated with the operation of such a registry. Most consumers will be concerned with unsolicited callers who may somehow gotten their numbers, emails, fax numbers from private banks, data, marketing companies who sell such contact data. The important questions to address here is what are the deterrence in preventing such “selling” of contacts. Most standard contracts in registration forms will include some clauses that state the companies/ organizations that received your particulars reserve the rights for itself and its associated companies or companies appointed by it to gather and offer suitable goods and services to you. How does the new proposed Consumer Data Protection Regime address such issues? Does a registry works? What if consumers continue to receive unsolicited calls from other countries such as Hong Kong, China,

	India...etc. who offered some “scams” to request for monies transfer? I am sure most of you would have encountered such calls from time to time, or at least read about people being cheated out of their monies by such scams calls. In order of such proposed or refined Data protection regime to work, the “being protected party” likely consumers must have the rights to demand identification information by callers, and “addressing” channels must be made available for reporting of such cases. The law must require any unsolicited callers, faxes, emails to identify themselves, and upon request to explain what are the sources that these individuals/ organizations have received the contacts or data from. It will also be interesting to find out if the proposed consumer data protection regime could even have an effect on the common spamming of emails and faxes which most individuals receive every now and then. If the proposed or refined law could not be reasonably expected to reduce these spams, or the returns (results) from implementing these laws could not deliver saving in business costs or significantly reduce abuse of data; then please simply just keep where things are and avoid the spending of government monies (be it national registry, setting commission to investigate...etc.). To end, most people will want things that are free and as the survey results show, 98% will prefer a do-not-call registry, but it is important to address why in the first case was there a data abuse? Did any body ever voluntarily subscribe to a “please call me” registry? Most provide their contact information in case any matters that concerns them could be addressed in a fast manner. And if data has value, how would this law affects the behaviours of individuals/ companies that prosper from selling of such data? And what if, people demanded that all 100% of individuals/ organizations to be automatically included in this do-no-call me registry? After all, none of them has ever fill a please call me form for your [fill in companies of products & services]. Regards, A “Thank you for working on making the nation a better place, but do remember to compare the cost & return to see if it justify” citizen
30	Personally i have been receiving too many nuisance calls from bankers and retailers as well as sms everyday . I think this issue has been out of control of too long and its time your side can do something . Why don't we work the other way round , those who want to receive calls or sms can register to opt in otherwise don't disturb us with all these nuisance calls or sms everyday .
31	We have been receiving a huge number of SMS from housing agents, developers for new projects launched. We also received SMS from banks and financial institutions which we are not a customer, offering free credit cards, immediate credits and so on. As a result, we have been spending a huge amount of our private moments reading all these unwanted "trash" SMS and lower our productivity. It is especially annoying when you receive these trash SMS while driving, and you will lose your concentration on road traffic and jeopardize the safety of road users. Our suggestions are as follows:

	1) make these thrash SMS senders pay the receivers at a hefty fees if they so choose to send the SMS; 2) ban mass sending of SMS by private individual and company; 3) limit the number of SMS an individual or private company could send; 4) limit the time of the day an individual or private company could send bulk SMS, so that they will not send SMS in odd hours of the day; 5) ban the use of SMS as a tool for survey by an individual or private company; also ban them from political parties; 6) the use of "unsubscribe" from the list of receivers always ineffective and in many cases it will result in receiving more trash SMS, therefore it should be made mandatory for Telcos to remove the link between these senders and receivers. We hope that MICA could help the majority of mobilephone users to screen off , or at least reduce the unwanted SMS being sent to them so that they will have a better quality of life.
32	A do not call registry can be an effective and efficient way for individuals in Singapore to opt out of receiving unsolicited telephone sales calls, SMS and fax messages. However, it is important to properly define “unsolicited sales calls” so that the registry does not encompass communications that are desired, stem from a prior or existing business relationship, or are for customer service needs (i.e., are not a solicitation). For example, “unsolicited sales call” can and should be defined to mean “a sales call (i.e., one for the purpose of solicitation of a consumer good or service) other than a call made: - In response to a request of the person called; - In connection with an existing debt or contract, payment or performance of which has not been completed; - To any person with whom the telephone solicitor has a prior or existing business relationship.” (taken from Florida Statutes Section 501.059, Telephone Solicitation) Also, there must be a fair way for the solicitor to maintain adherence to the registry, such that there is no expectation that changes will be made to the registry and must be captured by the business on a daily or otherwise frequent basis; this would be too onerous and expensive (and perhaps impossible) to which the solicitor to comply. Florida publishes its registry on a quarterly basis and prohibits calls made to numbers existing on the then-current quarterly list. Dates of publication of the new registry should be made known well in advance so that solicitors can prepared to vet against all such newly published lists.
33	As a consumer who has been repeatedly pestered by these telemarketing companies who keep calling despite their promises not to call and getting us to sign their "DNC registry" while all govt agencies such as the police, IDA or MICA claim that they cannot do anything, I very strongly think that the current proposed legislation needs to have more teeth to be effective.

	First of all, no charges should be levied on the consumer, even under the title of service recovery, for accessing and correcting their records (Point 3.70). It is the respective company which has a customer's personal details in the first place, and asking a consumer to pay (even a small amount) for accessing and/or correcting that data is outrageous to me. Does the current proposal mean that even if an agency's data is incorrect and I am being affected by it, I may need to pay to access it and have it corrected???? There should instead be a penalty mechanism which puts the onus on the credit bureau or a similar agency to verify its facts first and if some data is erroneous and not corrected even after the customer has pointed out the inaccuracy (free of cost), then the agency should be penalised and the affected customer should be compensated for the harassment. Under Article V (National DNC registry), there should be a punitive mechanism whereby the affected customers are reimbursed by penalising errant telemarketers, and the penalties should rise exponentially for repeated and wilful non-compliance by the companies.
34	This is the right thing to do immediately, without any hesitation, as I'm being bombarded by unwanted text messages and phone calls (particularly in mobile phone and at times in the landline) You have my 100% support in this regard
35	At last! I'm 100% for this law. If they are calls from service providers with an existing business relationship eg I have an account with this bank, or I just bought a product from them, I am satisfied that I am always given a form to sign to opt in/ out. Plus they should be able to tell me where they got my contact from. So that is not a worry for me. The real demons in my experience have been the property companies. In the past few years, we regularly get cold calls from established agencies like [redacted] and [redacted] or their hires asking if we want to sell our property. When I ask how they linked my home number to my property (which really scares me), they refuse to tell me. I have spoken to their managers, written to their Boards but they never bothered to get back to me. Once, my then 8-year-old answered the phone and the lady didn't know our name and asked him to give her his "mummy and daddy's name and handphone number". I now continually remind my kids not to give my contact to anyone even when they ask nicely or sound like a friend (he says he was caught off guard cos she sounded like my friend) because I need to guard our privacy against such unscrupulous practices. Just a few nights ago a [redacted] from [redacted] called our home number again asking us if we wanted to sell our house. This time he knew my husband's name(again, really freaky because he could not explain how he knew our name and had our home telephone). As usual, I insisted he remove our contact from whatever "legal" or illegal mailing list he was using and took down his name. But until this Act is made law, I have very little faith that this will be the last call from strangers who know my name, know where I live

	and know my home number and do not feel accountable to me to be able to explain how they got this information or how they will use it.
36	I agree with the setting up of national DNC registry. The registry is workable only if the leads (telephone numbers) are given by the telemarketing companies to the telemarketers after the companies have checked them against the registry. However, most telemarketers get their leads from all sources, from clients, papers, name cards, Internet, etc. These leads "belong" to them and they usually are reluctant to pass them on to their companies.This will not be a problem if telemarketers have the same means to check their leads against the DNC registry. If not, a possible solution would be to get telcos to provide a distinct ringtone for numbers that are listed in the DNC registry (just like the different ringtone you hear when the person you call is overseas). In this way, telemarketer can immediately hang up the call when he/she hears this ringtone after dialing a number listed in the registry and there is no need for the company or the telemarketer to check the registry (no additional cost).
37	I applaud mica's effort on this. Some comments/qns pls: Has mica considered including email addresses in addition to telephone/fax numbers in the do-not-call registry, and perhaps call it a do-not-contact registry? Today, many of us receive far more spam emails than cold calls from tele marketeers. May I know how can an individual specify the Organisation(s) to be barred from contacting him? If the organization changes name (for whatever reason eg RBS bought over by ANZ), does he have to update the registry himself or will the Registry be smart enough to track such changes? Is mica also tightening law to prevent Organisations from selling or passing on individuals' personal information to tele marketeers or other organizations without consent from the individuals? Could you explain how you intend the enforcement to work? Does the burden of proof land on the individuals? If so, quite cumbersome isn't it (eg. a Tele marketeer engaged by a debarred org that I have listed in the registry continued to call me using a tel with number withheld)?
38	As a fellow civil servant plagued by numerous nonsensical calls throughout the day by telemarketers, it is a relief to hear that a national Do-Not-Call Registry would be set up. I would be excited and would definitely be one of the first few to put my number in it. I

	grow tired and extremely frustrated with the numerous calls I receive, and it is even more frustrating to receive those calls during office hours when I'm expecting calls from important guests. Imagine the numerous times I was on standby to receive VIPs only to get interrupted by a call on behalf of XXX bank. It is extremely annoying. I think interruptions on the phone in the form of calls and SMSes are even more disrupting than emails (which can conveniently be channelled to the Junk Folder). Calls and SMSes unfortunately have yet to develop a filtering function. I have called up many organisations to put me on their "do not call" list but recently I have started receiving SMSes about property, insurance, credit cards, home tuition, air con servicing, etc. It is extremely annoying. Responding "UN" to unsubscribe just gave me more spam from different sources. The surprising thing is, every SMS and call that comes in is from a different number (I know because I've been keeping the number in a "blacklist" so that I won't pick up the call again). I am astounded by the number of telephone numbers they have! Enough of me sharing my woes. I would like to kindly share an idea on operation that I have. MICA could set up a system (perhaps an online complaint depository of sorts) for folks on the Do-Not-Call registry. Should anyone on the list receive any call or sms, he or she could log on and report the phone number, name of the caller and other like details of the call for MICA. Once the number of complaints against that particular phone number, person or organisation reaches a critical number (3 would be good!), MICA could take action against the organisation. I hope the regime would bring about more peace to fellow Singaporeans. Kudos to MICA for coming up with this. Better late than never! I look forward to relief from such SMSes and calls.
39	I would strongly support setting up a do not call register. I have purchased two off the plan properties some time back. For the last six months my mail box has been bombarded with letters from real estate agents. ReL estate agents also keep trying to call my home line at night and on weekend. I no longer answer my home phone number as I am fed up receiving calls from agents. I will still cut off my phone line. Establishing a register and new privacy rules are well overdue.
40	I applaud the recent announcement of the plan to implement "Do-Not-Call" registry for unsolicited calls and SMSes. However, I hope the implementation would not severely affect the livelihood of many individuals and SMEs who rely on unsolicited SMS to survive. Firstly, SMSes are different from calls, they should not be categorized in the same category. I personally, and I believe many people as well, do not mind SMS advertisements as they do provide me with information that may be relevant and useful to me and they can be easily deleted, but unsolicited calls are just too much of a nuisance. Putting them in the same category and meting out the same

	punishment may seem too harsh for SMS offender, in particular, if the person is an individual trying to eke out a living instead of joining the unemployment queue. Besides, I am of the view that punishing senders of unsolicited SMS cannot prevent leak of personal data and should not be used for the purpose of consumer data protection. More often than not, these senders obtain the data through third party. They are just using the already leaked personal data, at worst, in a irritating but probably the most harmless way. Secondly, if the SMS offender is using his/her own mobile phone or equivalent that can only send out not more than 10 SMSes per minutes due to the limitation of the mobile network bandwidth allocated to SMS, they can cause only limited nuisance to the public. In comparison, bulk SMS sending through Telcos or SMS brokers of Telcos on behalf of corporations with deep pockets, they can blast out at least ten thousand SMSes in one hour. These are the major sources of nuisance if not managed properly. I therefore feel that to protect the interests of small companies and individual agents relying on unsolicited SMSes, we should distinguish the punishments for unsolicited calls from unsolicited SMSes, and further distinguish the treatment of unsolicited SMSes sent by different means. If I may suggest, instead of using the “Do-Not-Call” registry to control SMSes, we can emulate our successful way of controlling the traffic using ERP. For example, the law can require all unsolicited SMS to begin with the word “<ADV>”. Telco can easily implement software to collect “SMS Advertisement tax” on behalf of the government. Those who violate, if reported by the recipient, can then be severely punished as it is tantamount to evade tax. There should also be a differential in tax by taxing those bulk SMSes heavier or ban them out right since the “damage” is potentially higher. In any case, big corporations who can afford the more expensive bulk SMS would have better wherewithal to advertise using other means. Besides, we should also show our compassion to the plight of those individuals and small companies eking out a living. Certainly, with the experiences in many other countries, whatever the method, we would not see the end of unsolicited SMSes. The aim is to reduce the inconvenience of the recipients when his/her personal data is somehow leaked. At the same time, we should not severely affect business activities, particularly those individuals and small businesses. As recipients of those unsolicited SMSes, we should be compassionate enough to tolerate a little inconveniences and understand the need of others to make a living. Furthermore, I believe some ingenious companies would come up with an SMS filter Application for the phone that would filter off all SMSes beginning with “<ADV>” if the demand is there. As for the country and the government, the control of SMSes can be done by varying the level of tax, instead of, like the experience in Australia, forcing out SMS advertisement to neighboring countries outside of our jurisdiction and losing the SMS advertisement revenue all together.
41	In the past 10 years, I have received calls yearly asking me how is the condition of my pots and pans when I have never buy any from this company. During the first 8 yrs , I was v polite n told the aunty I hv never buy any pots n pans from them n pls stop calling.yearly, they insist on calling. I suspect this is a small set up n the bosses are uneducated but in the business of selling highly expensive pots n pans to housewives

	n rich tai tai who are not educated. I guess it was my mother in law who had passes my tel numbers to them.... And recently , after a food chain open in marina n offer a lucky draw dip, I rec many SMS Fr private loan operators offering me loans .And suddenly , I rec three SMS from overseas telling me I had won something. I can't help but feel that the lucky dips offered by the marina food court or during the PC show has something to do with it fir the spikes of unsolicited SMS starts during the same period. Now, there are no more such SMS after I did not participate in any lucky draws. I attended a showroom to look at property yesterday afternoon n was directed to write down my particulars b4 they serve me.After I left, I get SMS one hr later asking me to see properties launches in the other parts of Singapore. At night, I get three to four calls from Telemarketers who do not even know the name of the agents they are representing!!!! When I asked which property agent company n the agent name, the young naive telemarketers actually have to covet the mouth piece n ask err ,what is the name of the agent n what company?Property agents should not employ young girls n boys to call clients at night when the young do not even know who they are representing n what is the name n tel no of their bosses. And callers do not even bother to identify themselves or rushed through on an incoherent rant hoping we don't rem their company nor names but trying to say their sales pitch first. In improving the DNC registry , the gov might want to improve on telephone etiquette first via education n courtesy campaigns. The young has lost many values n amongst them they don't know is rude not to call at night n they don't speak well n are not articulate .They don't identify themselves n even ask me who I am or calling out my IC name like I am some criminal. In short, pls disallow companies from selling our data via lucky draw slips that they may have collected.Disallow property firms from mass selling our data or input our data in their company system to be shared by their agents . But what can u do to small companies whose bosses are not educated n insist their aunties call To survey on the condition of the overpriced woks n pans they sold to your mother in law?

42	Please help to include residential numbers as part of this proposed data protection policy. Ever since this has policy has been raised, I have been getting numerous telemarketing calls to my residential line now. I am just wondering if it is because there is only 1 owner to the residential line and I am not the owner to this line and they see this as a way to overcome this policy. As we all know a residential line has only 1 owner and by calling me via residential line, they do not see it as infringing on this proposed policy in future, we definitely need to include residential lines as part of the scope regardless of who the owner of that residential line is. These telemarketer calls are causing disturbance to my mum(in her 70s) and my nephew who needs to take their afternoon naps. Feel free to let me know if you need more information.
43	I am in full support of a National DO NOT CALL registry. I have been a victim of harassment by many text messages from property agents and countless calls from SPAs, Fitness Centres, etc. Everytime I ask them to delist me, they will say ok but they will call me back the next month. We should not let these companies harass us. We have the right to not receive calls from these parties as it is a waste of our time.
44	Yes. Please, please set it up as soon as possible.
45	Instead of an opt out, this should be an opt in. The mobile phone number is as much an identity of an individual as our NRIC these days and it is personal. Unsolicited calls and sms should be viewed as an invasion of privacy. Searching and learning about products we want is so easy these days, why should we waste our time entertaining unsolicited calls for product we have no interest in? I have saved over 80 unsolicited sms on my phone, all from different numbers. There are also lots from the same numbers with repeated messages, several times over. There are also instances which I have stupidly opted out. I said stupidly done so because I believe my number would passed on. Maybe this isn't the case but I have lost faith in the system. The Code of Ethics and a DNC for specific organisation; this is the first time I have come across this and I doubt if any companies adhere to the so called Code of Ethics. Self-regulation means no regulation and no policing. I have lost count of the number of times I have received sales call from the same organisation despite my protestation. The most recent being GE Money.

	Like many, I am away for business quite often. I leave my phone turned on 24 hours a day incase of family emergencies or client calls/ sms. Too often I have been awoken in the 'middle of the night' by unsolicited calls and sms instead. To add insult to injury, I end up paying for the call roaming. Of course there are numerous other times when I received such calls in the day time. Why should these nuisance call benefit the telco at my expense? Why should we be bothered with any extra cost incurred by telemarketing organisations when I have already been paying for it for so long? When will MICA start protecting the consumers' interest instead? So I say again, it should be an opt in rather than opt out. These calls and sms benefit the few at the expense of many. I pay for my mobile phone not the call centre or the sms generating companies hiding behind a faceless number. We already get bombarded by advertisements and sales pitches everywhere we go. Do we need more? Shouldn't our personal mobile phone remain as such, personal.
46	I am concerned about the Act being too restrictive such that businesses are unable to send sms or fax to anybody at all, thereby affecting businesses functioning and resulting in lesser Singaporeans being employed overall. The Act should be not restrictive such that businesses can sms or fax their services if they come to know that whoever that person or organisation is selling something or advertising some products or services which is related to their businesses or location and may need their services then exemptions should be made. For example:, let say a company advertise in the newspaper looking for employees, then job websites should be allowed to email or fax their services to that company or say a person is advertising their properties for sale, then housing agents should be allowed to send sms or fax offering their services. Otherwise with too much restriction, there is not much room for businesses to functioning properly. Remember that many years ago, hdb letter boxes were open and mailers can be distributed but when hdb letter boxes became only locked ones, then mailers went to owners' homes instead thereby creating security risk when owners are not at home for many days. Solution to one problem creates another set of worse problem instead. I hope the government will think carefully otherwise at the end of the day, Singaporeans may be the ones badly affected as solution to one problem creates another set of problems instead. SMS should be exempted from the scope because it is free incoming local and overseas. The problem is incoming overseas calls that cost much money to users when they are overseas, that should be the focus, telemarketing calls and not sms. Most complaints are from such overseas calls charges when a person is overseas.

47	Yes! Great to have a DNC registry. In addition to setting up a DNC registry, please also consider setting up a Marketing Callers (MC) registry where all unsolicted marketing calls can only be made from registered phone numbers in the MC registry. Having a MC registry will help the public to check the identity of marketing callers. In addition, the registered phone numbers for marketing calls should also have a unique prefix (eg 1700) such that the public can easily know that it is a marketing call before answering the call. Please also use part of the registration fees of MC registry to fund local educational institutions to develop free phone software for blocking unsolicited marketing calls. If all marketing call numbers have the same uniquely identifiable prefix, it would be simple to implement such software in every phone sold. In addition to blocking unsolicited marketing calls, please also extend it to unsolicited marketing sms. If possible, please also engage telcos to provide marketing calls barring software or feature in all the phone they sell directly to the public. The involvement of telcos will help to accelerate public access to phones with blocking software for unsolicited calls. Businesses and affiliates that fail to comply should be fined a substantial amount that will make any of their intended violations unprofitable. Having a small fine of eg $10k will not defer businesses if they can make millions from unsolicited marketing calls. To close the loop, please also consider barring businesses from engaging marketing agencies that make marketing calls from overseas. This will help to ensure enforcibility as any noncompliance would have been commited locally. A MC registry will be relatively more efficient to manage and it can also complement with the DNC registry. Singaporeans work hard and deserves to be uninterrupted at work. Studies have already shown that unsolicited marketing calls disrupt productivity. Our nation needs to maintain and increase productivity to remain competitive. Please kindly consider implementing public-oriented solution to fight unsolicted marketing spams for the public interest and the much needed productivity for our economy.
48	I support the setting up of a DNC. In practical terms however, MICA needs to set guidelines on what is meant by reasonable effort to check the numbers. Do businesses need to check daily or weekly or monthly? Also, how will the DNC numbers be checked? Manually (one at a time), or can we export entire excel spreadsheets from the DNC and compare with the business' list of customers? Or, do businesses upload their list of customers to DNC and DNC checks for us?
49	Hope all is well. There are a couple of stuff which we hope to see with regard to the Do Not Call Registrar: 1. Extension of coverage for the Do Not Call Registrar

	a. Fixed and Mobile numbers (call, sms) b. Fax numbers c. Email d. Home and office address 2. Who should be covered under the regime? a. Local Singapore companies b. Overseas call centres or companies targeting at Singapore consumers 3. Methods of consumer submission (mobile number, email, address info) to Do Not Call registrar a. Via SMS b. Via Web c. Via reply to direct marketing companies after receiving unsolicited sms or email d. Categories of exception companies which they would accept cold calling/sms/email 4. Methods of checking with Do Not Call Registrar a. Should allow bulk checking by Direct marketing companies (online or direct connection between call centre and the Do Not Call registrar) b. Should allow single number checking (via web) for individuals (property agents, insurance agents etc.) 5. Funding of third party company hosting the Do Not Call Registrar a. Would MICA fund the initial project set up? b. Could the hosting company make money by charging consumer on a monthly basis to keep their number in the registrar? c. Could the hosting company charge direct marketing companies or individual for information request?
50	I have some feedback: (1)Considering Singapore mobile operators selling so many prepaid SIM cards and there are many recycled mobile numbers in the market, It is a high cost to maintain this system accurately. (2)When a SIM card was sold in 7 eleven, the related information must be updated to the central system. (3)Who will run this system? Running such a system will be paid by the government? (4)In USA, it is profitable to run such a system by charging subscription fee. In Singapore, it is hard because Singapore is so small and the user base is not big enough. (5)If subscription is charged too high, telemarketor will disappear in Singapore. It is not a good thing for business.

	(6) There is No fish in pure water !!!!!!!!! I have an idea: If a consumer does not want to receive marketing materials, he/she need to pay one S$10/year. Then we have enough $ to run this system. Or consumer will pay another S$1/month to mobile operator and then mobile operator will run this service. This service must be fee accessable for business entities.
51	Yes and also and dont email registery perhaps
52	I whole heartedly support this proposal for the setting up of a Do Not Call Registry but clarity has to be given with regards to contact information collected prior to the proposed legislation. A typical person in Singapore would have filled in more than 50 lucky draw coupons or survey forms, magazine subscriptions etc. and blindly agreed to (if it is even printed at all) the use of such information for marketing purposes. What are the obligations of these organisations that have sold/bought/used such data when an individual opts in to the registry? For this to work, the public at large has to be educated on the consequences of providing such information without any thought to personal privacy. Organisations should also be made responsible for highlighting the intended use of such collected information in a manner that an average individual would notice and understand.
53	There should be a more detail analysis and a comprehensive software development for this implementation. THE DEVIL IS IN THE DETAILS!!! As i foresee your normal phone enquires cannot handle the sheer volume of calls by both the public and the pte sectors. EXAMPLE: 1:50,000 CALLS WANT TO REGISTER WITH YOU AND 10,000 CURIOUS QUERY.. 2:THOUSANDS OF COMPANIES WANT TO VERIFY THEIR DATABASE CONSIST OF THOUSANDS OF PHONE NUMBERS BEFORE ANY MARKETING. 3:YOUR PHONES LINE ARE DOWN. There should be a website created to let public to register and ALSO software development to allow thousands of companies accessing your website at the same time for verifications.Those companies may want to verify their own thousands of numbers by

	each individual against your list. Eg: companies have 300k database each want to verify the numbers before marketing.How to download or do a scan for verifications ?? Consumer protection is good for the public but it should not be anti pro business and increase the marketing expenses unnecessary for the whole industry. BECAUSE, consumer will ultimately have to PAY for the unnecessary increase in marketing cost in the long run.
54	I am most elated to hear that such service will be implemented, and it is high time the relevant Government bodies should look into this matter to protect the public's personal data. Recently, during the Presidential Election, I was very surprised that I had received an SMS on campaigning message from [redacted], whom I do not know him personally. I replied to the sender and advised I do not understand how on earth they had got my personal mobile number which was totally unethical?! In the past, I have also been receiving many SMS and phone calls from unknown persons trying to sell their services, which I had never reveal my personal data to strangers before. The Government bodies should STOP those unscruplous retailers and organizations from selling their database and intrude into one's privacy without the knowledge of mobile owners. This is totally unethical and uncalled for! I look forward to your reply.
55	I feel that telecom should allow user to block out spam SMS or calls from certain people and user should also be given the options to block all if some group of people really feel agitated. Some SMS contain real bargain or deals and we still want to receive those so we should have options to cater to selectively block or the options to block all spam sms and calls depending on the person preference. Telecom should also help user to block spam SMS and calls free of charge at the request of the users on the telephone rather then user have to always reply to unsubscribe via sms which sometimes the spam company don't bother and still keep on spaming us. Telecom should immediately block any particular number from sending sms to user on their telecom side and send also send a warning note to the company to stop sending the same sms if a lot of people are complaining to the Telecom customer service of the same company. I am not interested in loans and property but people keep on sending me sms to take up loan or buy property. Maybe Telecom should have some sort of intelligent SMS system to block all the property and loan sms once the system detected this key words in the sms.

56	a) There is a need to clarify the roles and therefore, the duties and responsibilities of different stakeholders (such as between the telemarketing company and the client (e.g. banks). b) To consider (an increasing trend) on how to manage the issue of overseas calling (telemarketing) centre. Are these subjected to the framework ? If not, is that a potential loop hole ? Understand that there might be difficulty in enforcing on overseas entity, however, how about consider that the client (companies that must have a presence in Singpaore, otherwise why would they want to sell their product locally) to be partly responsible and legally culpable for non compliance by their appointed marketing agents c) To understand the impact of potential abuse of the do not call registry. The registry will become an open source of mobile phone numbers database. There is a need to understand the implication to prevent abuse. (would somebody mine the data for other purposes??) Perhaps a study of overseas experience and their measures would be good.
57	I'm making reference to today's Straits Times article on the new law to protect consumers from unsolicited marketing by companies. I like to provide feedback that unsolicited & unwelcomed marketing by banks should also be put into law to be banned. MICA should also examine & review how banks inclusive, use database, as well as how it can be passed on to external companies, leading to a chain & flood of marketing messages, which basically intrudes into the privacy of consumers & create inconvenience & disruption. This in turn could translate into a cascade of law into what's prohibited, so Singapore can provide good protection for consumer's privacy & positioned itself as a hub for consumer data-protection law. For your consideration in consultation with the public.
58	With regards to the announced legislation to protect consumer data, I applaud MICA's effort in championing such a cause in preventing our personal data being misued. May I also suggest that such laws should apply to unsolicited ads and sms by property agents, which constitute more than half of such abuse. What's more, when some of them are very insistent in bombarding us with their blast.. At the same time, some tuition agencies as well as software companies are also culprits in such deeds. If u require more info on such companies which had violated our privacy (despite calls to unsubscribe), I can provide you with such details. Wishing you good health & success in bringing MICA to greater heights.
59	I want to ask if there is law to govern/restrict companies to send unsolicited sms advertisements to public that we don't subscribe for? I

	have been receiving SMS ads for a while, and annoyingly, I suspect their "UNSUBSCRIBE" feature doesn't really work (perhaps intentionally, or worse, it is used to confirm that my phone number is valid). I have tried to unsubscribe from their services many times, but I still receive similar ads only coming from different phone numbers. I suspect the fact that they use bulk phone numbers to send SMS ads makes it hard for anyone to tell whether they originally come from the same company / business / vendor / owner / etc. The lack of transparency makes us, the mobile phone owners, hard to enforce the bulk SMS ads vendor to take any unsubscription requests seriously. Before the SMS ads becomes another uncontrolled email spamming business (we can filter email spam, but we don't have technology to filter SMS yet), I sincerely plead MICA to take the matter seriously and urgently. I would like to share possible set of policies that MICA may want to implement: 1. To have bulk SMS ads vendors to register the list of phone numbers that they still/will/intend to use to send SMS to public. The registration is to relevant channel of authority/body (e.g. MICA) and this information should be kept in MICA registry for 2 months or so. This information can be made public and can be queried by anyone possibly from an online website. This is so that anyone can look up who the owner/vendor who send the SMS ads by the sender number, and to report to relevant authority when their unsubscription request is not followed up / handled seriously. 2. No vendor is allowed to use unregistered phone number to send SMS ads. Relevant authority also has to impose fine or sanction in event where a vendor fails to conform with this regulations, and possibily making repeating offenders out of business. 3. Upon receiving unsubscribe request from mobile phone owner, bulk SMS ads vendor must unregister the owner's mobile phone number to make sure that he/she will not receive SMS ads in the future. This unregistration must be regulated, i.e. it must be done within 24 hours, and the mobile phone number must be hard-deleted from the database and this information should not be retained or shared/sold to 3rd party. Otherwise customer may unsubscribe from one vendor, but start receiving similar ads from different vendor or vendor's business partners/clients. 4. This regulation only applies to advertisement business. I.e. it should not apply to 24-hours instant/periodic SMS alerts provided by financial institution like Banks. 5. To prohibit sharing of mobile number information between bulk SMS ads vendors and their business partners/clients. 6. To ask telco operators (Singtel, Starhub, M1) to be able to advise their customers of customers' rights and possible actions that they can take when recieving unsolicited SMS ads.

	7. To exercise public awareness about the existance of such regulations, individual rights and actions that each mobile phone owner can take when recieving unsolicited SMS ads. This can be done via local newspaper, television, etc.
60	1. It is not clear, however, whether a service provider like a bank can still continue to call its customers for telemarketing purposes if they have listed their numbers in the Do-Not-Call Registry (from Straits Times article) Feedback: banks should also be subject to the Do-Not-Call Registry. 2. Location-based marketing, where retailers broadcast promotional SMSes to consumers who are physically near their shops, is also allowed. (Straits Times article) Feedback: This should not be allowed where people have registered with the Do-Not-Call Registry. If this is not able to done owing to constraints of technology, then the rule should be that location-based marketing not be allowed as it is an invasion of one's privacy which the shopper cannot avoid (unlike people advertising by distributing flyers near the shop which the shopper can accept or decline).
General comments	
S/n	Comments
1	• Organisations should not be allowed to use unlisted telephone numbers or call centres outside of Singapore to contact individuals • Organisations should not allow data to be used by third party vendors in any instance even with non-disclosure agreements between contracting parties. • Only registered organisations should be allowed to collect specific data such as age, gender,date of birth, NRIC IDs, addresses, contact numbers.
2	Many of us, I am confident I can include you the reader, have been subject to unnecessary intrusions by marketeers who somehow got their hands on our data. It would be good to have the law on the consumers' side to protect our privacy. To me, Consumer Data Protection comes in a three parts: 1. Data Collection • What data to collect? Today, in almost every form (from application forms to contest forms), they typically ask for data like

NRIC #, Date of Birth, Telephone, and Email. Some even ask for Income, Marital Status, etc. They put it down as mandatory and we, consumers, willingly provide. When some of us do not provide, like myself, we may be told that we are not eligible for this or for that. For example, I was even asked by Courts, some years back, for my NRIC # so that they can create a customer number. In addition to my NRIC, other particulars, such as DOB, Telephone, email, income, marital status were all requested. When I refused to divulge all these details, they told me that they could not create my customer number and I could not purchase the item. To which I provided S1234567A as my NRIC, and so on. The sales clerk was clearly unhappy but that I think it was because she would be queried by her manager for not getting these juicy bits of details about her customer.

There are certain situations where data such as the above are required - loans from banks, hospital stays, mobile phone line purchases, certain governmental applications, etc. But these, or at least the guidelines, should be clearly spelled out. I do not, for a single moment, think any every day retail transactions would require any of such details to be revealed. Name, credit card numbers, delivery address, telephone numbers are the norm. NRIC may be requested for verification but not recorded.

- Where to store? As data storage becomes increasingly available, it would not be surprising to find these data points stashed up somewhere on a large data server. These data servers should be protected from prying eyes. I have heard that some of these data servers are protected with a single password that can be easily broken.

- How long to store? These should be segregated by the types of transactions. For example, for mobile phone line transactions, these data points should be kept for as long as the account is opened. For others, the timing may vary. A reasonable time may be determined by how long the warranty period of product/services has. In essence, storing customer data for anything more than a year for any normal retail type transactions would be considered too long, in my opinion.
  2. Permission to Use

- Explicit. The effective, and preferred way, to protect consumer privacy is the OPT IN method. This basically prevents any law-abiding company from using the data collected from customers who are not legally savvy or who just could not care less.

- Implicit. This is often used in contests where consumers who want to benefit from promotions are enticed to put down personal data in order to do so. There should be some provisions to allow consumers to enter contests while divulging the minimal amount of personal information. This has been in effect in the US & Europe for many years. Only names, address, and possibly contact details (like telephone numbers & email) are requested.

- How the data is being used. It should be EXPLICITLY provided in any request for personal data as to how these data points are going to be used. General use terms like "general marketing" should not be considered ample.

	3. Penalty • In Singapore, any law without a painful enough bite would not have the desired effect. • Legal prosecution is a must. (Just look at the way some of the road rage incidents go... as the police deemed these to be civil, they would not get involved, and hence nothing really gets done) • Civil recourse (this is sometimes not possible as this requires some "loss" to be suffered. Identity theft is hard to proof. Questions on how to police it, well. Maybe put it in as an item for the statutory audit to be confirmed by the external auditors.
3	Hi, I think the above scheme is a long time coming and I'm wholly supportive in it. The main culprits in misusing individuals data are mainly, job agencies (online or print) and universities/banks. You have no ideas how many sms and calls I have recieved from gyms, property agents, banks etc. The data are sold over many times among different organisations I hope the authorities could set up an enforcement to clamp down on the abuse of personal data.
4	I have highlighted these interest last year when the Job-site asking for details & never come back to me as though I am a fool waiting for the job outcome. Recently I apply for loan from the money-lender, they too printout my HDB, CPF statement with all my details after they have review, they said I am NOT qualified for the loan, they too never give back to me except they said will shredded the documents but I never see them do that. After few days, another money-lender sms me & offer a loan which taken me by surprise as I wonder how this company got my details when I don't even have their company tel no. MAS should implement that once the money-lender already interview the borrowers & if they are disqualify, it should be return the whole set to us instead of keeping it & forward it to the 3rd party, by the way... can I sue these companies that sells my data to others?
5	Kudos, cheers and bravo to MICA for spearheading the Consumer Data Protection Regime. It is a total invasion of privacy for corporations to sell/buy/and use consumers' personal data and contact information. The consumers become helpless victims. Who in the first place gives the banks and other organizations the permission to divulge the personal information of their clients? It is most irritating to receive unsolicited marketing calls and sms. It is worse when we are overseas and have to pay for these calls and messages. Often there is a time difference too when we travel.

	Often, these calls and sms come from private or unrevealed telephone numbers. Will the telcos cooperate to trace the perpetrators under the proposed law? If they do not, many of these telemarketers will get away with the law.
6	It is about time such measures be implemented. There has been ever increasing infringement of privacy by way of unsolicited sms messages, email etc over the years. While many a time Singapore love to cite other countries as examples, for such protection it seems to take a feet dragging process to implement. Is there any justification in the first place for the delay in implementation ? Or is it because of commercial consideration that MICA has turned a blind eye to the problem ? I hope the process will be speeded up as many consumers are finding it very irritating to say the least and the main culprits are the telcos as far as MMS and SMS are concerned. Next are financial institutions and other commercial entities.
7	would love to see that all lucky draw claim should be based on the numbers given and not on personal details, such as IC number & HP numbers. Very often after filling up our HP numbers, I will received many sms from insurance company, loan, etc ..etc. Nowadays, most shop required IC number & HP number for member (discount) card. Hope you can also look into this.
8	Who give them the right to sell our info for profit ? Companies who sells customer database for profit should be similarly fined heavily. Before during transition period before the registry is set up. These companies should be warned that what they are doing is illegal and subjected to fine.
9	Below are my comments on the proposed framework a) To reconsider exempting small business from the framework to prevent potential loop hole for exploitation (e.g. large organisation will appoint a "small business" to manage their sale process and hence, circumvent the system in place). The impact to the small businesses to be included in the framwork should be small since as of currently, most small businesses are typically not collecting

	consumers' data anyway. b) Consider opt in rather than opt out as deemed to have given consent for the collection and use of data
10	There is another area that needs to look into, that is the publishing of names, addresses and phone numbers in phone directory and on the Internet (www.phonebook.com.sg). Unless the subscriber opts out with a monthly fee, the numbers are published. It is time that the new privacy law looks into this area where private information about individuals can be searched and extracted. Maybe the Telcos should published the numbers of those who opt in, by default everybody should be considere opt out and do away with the residential phone directory and Internet search totally. This easily available contact information allows scammers to target people more easily.
11	I really look forward to the DP Act. In fact I've been asking the team who are in charge of SPAM control how they can do something previously but was disappointed that they were unable to. When I read the preliminary guidelines of the DP Act, I'm happy to see something can be done about such database selling. These people have been spamming us weekly through emails and SMS. They are not effective and created a lot of public nuisance. These companies spammed our emails and asked us to buy their databases which they've sourced through events and probably buying databases illegally from other legitimate companies (who've breached their clients' privacy). I believe company like below should be prosecuted if the DP act comes into force. We really need the DP Act to come into force ASAP to remove these nuisance companies. Kindly take note of the contact info below and be ready to call them up to enforce the DP Act when it is passed.
12	I tried to open a bank account for my wife - just a savings account, and was given the account opening form. Buried in the terms and conditions was a consent to release my wife's particulars to the banks' "business partners", whatever it means. When I pointed it out to the bank's executive and then manager, both said that the bank respects confidentiality and would not release the information to 3rd parties. So I asked that the clause be deleted but the bank refused. The account was not opened. My concern is that consent obtained in this way is wrong in that the consumer's attention is not drawn to this clause and that although there may be technically a consent obtained, it was not consented to with full knowledge. Can the legislation be drafted in such a way that such consents be made in a separate form or at least drawn to the individual's attention?

13	Kindly include: the Date of Birth as one of the data to be protected. This is important as many banks use this information for identity verification prior to proceeding on phone-banking operations.
14	I would like to give some feedback on the DPC. 1) Condominium or any private Estate - Suggest they write our particulars like name & Mobile phone instead of exchanging our NRIC for a Pass. 2) All Telcos, Insurance Co, Banks or any establishments - Just verify our NRIC instead of making photocopy or scan our NRIC. Presently All telcos scan or photocopy consumers' NRIC when contact is signed. I feel that verifiny the data is good enough. They should not make copy of our NRIC at all. Insurance Company - Why should they make copy of our NRIC when we collect our money upon maturity of the Insurance Policy? Verifying is good enough. 3) Contest through SMS - Now Contest Organisers require contestants to include our NRIC numbers for any SMS contest. They can do without asking NRIC numbers. Contest Organisers can add a clause like - "Prices will be given to holder of the mobile numbers".
15	I am a member of the public, and I don't have views on all the questions. However, I am very glad that we are coming up with such a law because I am innundated with unsolicited phone calls and SMSs every day. Sometimes this costs me money or wake me up in the middle of the night, especially when I am travelling overseas. I hope that such a law can be implemented quickly and enforced robustly. The rationale for the law did not express an important point - why should there be a law to protect consumers? International standards is one thing, but does that mean that we are just following the pack? One reason laws are created is to protect those who are in a weaker position from those who might abuse their power. In this instance, individuals are in a considerably weaker position to protect their privacy because they lack the resources of organisations. Hence, the need for society to step in to protect individuals.
16	On the just-announced Act on Personal Data Privacy and Security, it's about time. Why did it take us so long?

What should be in the Act?

- The rule is "opt in" rather than "opt out".

That is, whoever or whatever organisations/agencies/businesses that collect personal data, must explicitly ask the person if he/she wants to receive any "cold calls" or information or advertisements. It must not be that the person must ask to be excluded. It must be assumed that the "default" choice is that the person does not want to receive anything other than the specific services he/she is "buying".

- Current state is that cold calls, etc include a clause to "unsubscribe".

This should not be applicable for at least 2 reasons: (1) Most people won't bother - and the advertisers knows this. (2) There can be costs to unsubscribe. eg: The costs of a responding SMS (to unsubscribe).

Example: Mobile phone service providers make money by allowing advertisers SMS-"blasts". They make money when users respond to unsubscribe. There should be some penalty or onus on these providers to unsure that the advertisers prove that their "blasts" are based on authorised "opt-in" lists of clients. If not, these service providers should also be penalised. (Many parallels: airlines are fined for flying in illegal immigants - although the latter were just paid passengers with seemingly proper travel documents; house owners who rent to people with seemingly proper immigration documents - the onus is on them to double check with authorities on the authenticity of those documents; etc.

- Whenever anyone gets a "cold call" or an unsolicited SMS, etc, and if he/she asks from where the cold-caller obtained his/her data/number/etc, the cold-caller, by this Act, must respond.

This will stop some if not most current practices. Of the remaining, with the given response, the person may then trace the source of the information and take action against any unauthorised release of data. A special agency/department may need to be set up to handle such "complaints" and traces.

- Whenever a person applies to buy a new policy, insurance companies "share" data on the person (to decide to authorise the policy or not).

How and to what depth of information shared are not known - especially to the person. This is not only unfair (to the person) but is totally non-transparent. This state of affairs must be corrected. Insurance companies or anyone should not have the right to "share" information. If they do, then it must be clearly stated and made know to the person, to what depth and from what sources. Such a

	practice should also be applied to information-keeping agencies like credit bureaus, etc. Penalties must be clearly stated. • There must be clear definition of who and what agencies are allowed to collect what (depth of) data. It is conceivable that a security guard can copy visitors' personal data and later sell them. Example: What agency can legally withhold a visitor's NRIC as security collateral for entry? • The Act should be retroactive to some extent. Especially on mobile phone service providers.
17	Currently, the SGNIC registration policy of .SG Internet domain name disallows the masking of registrant's contact details in the public WHOIS database. This opens up an avenue for spamming and even stalking since the registrant's home address can be easily viewed by anyone if the registrant doesn't have an alternate Singapore address to use for registering his/her domain name. This is especially true for students who want to have a .SG website but only have their home address to use for registration. Non-SG domains, such as .ORG, .NET, .COM, do not have this restriction, which is useful because it protects the registrant's personal particulars. Such privacy protection has been in place for non-SG domains for a very long time. It's bewildering the we have such primitive restriction in place for .SG domains, which is detrimental to the growth and vibrancy of Singapore .SG websites as a whole. People may choose .ORG or .NET over .SG because their privacy is protected. If the rational is to only let Singapore dwellers own .SG domain names, then the rule can be changed to make the registrant submits proof of residence to the domain registrar during the domain name registration process, for which, this info can be filed and kept confidential by the registrar instead of publishing the personal contact info (address, phone, name, etc) in the public WHOIS database. Please consider this in the upcoming consumer data protection regime. Thank you.
18	Personal Data (names, telephone numbers and addresses) are listed in telephone directories freely distributed should be restricted as default. Currently, subscribers have to pay a fee to have their details unlisted. This is an old legacy that is no longer relevant in current times. There are organizations that scan the data in the phone directories and sell these data to marketing companies. This creates unnecessary spam mails and unwelcomed telemarketing calls.
19	This would be a great step forward for Singapore in terms of protecting peoples' personal information and privacy. This is also increasingly important at a time when information can be shared across multiple platforms in an instant.

	The proposed Data Protection Act is clearly a move in the right direction. However, the emphasis seems to be about not disrupting organizations as much as protecting the personal information of individuals. As a result, many of the points raised seem lukewarm at best and do not reflect any conviction towards maintaining a clear stand on the issue. A step in the right direction, but lacking in conviction. MICA should be applauded for taking this step towards greater protection of individuals' data. The challenge now is to make it such that organizations would never even think about illegally obtaining, collecting, using or disclosing personal information