Submission to

PUBLIC CONSULTATION

ISSUED BY MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS

PROPOSED CONSUMER DATA PROTECTION REGIME FOR SINGAPORE
13 SEPTEMBER 2011

By

Associate Professor LIM Yee Fen (Hannah)*

B2-B-62
Division of Business Law
Nanyang Business School
Nanyang Technological University
Nanyang Avenue,
Singapore 639798

Email: yeefen@ntu.edu.sg

Office: 6790 6136

* The author gratefully acknowledges funding from a EU Centre Research Grant from the EU Centre in Singapore. All the opinions expressed herein are the author's alone and are a result of being a legal practitioner and scholar in the area of data protection for over 10 years.

Summary of Major points

- The whole regime should focus more on the security protection and enhancements that come from a solid data protection regime.
- The EU gold standard of only allowing relevant and **necessary** data to be collected for specified and **legitimate purposes** should apply.
- There should be specific provisions concerning NRIC numbers. Two specific prohibitions are essential. First, no private organisation should require persons to disclose their NRIC numbers unless it is required by law. Second, no private organisation should be allowed to use the NRIC number as the means of identifying the individual.
- Data should be required to be processed on a confidential basis.
- Personal data should not be freely shared without the consent of the data subject.
- The DPC should be empowered with privacy audit powers
- The telecommunications sector, including ISP may require special treatment.
- The definition of personal data in practice should pay heed to the EU Article 29 Working Party Opinion on the concept of personal data
- There should be some protection for certain kinds of sensitive personal data.
- The law ought to require the deletion of personal data pertaining to deceased individuals unless required to be retained by law, or, where it is in the public interest to do so.
- There needs to be transparency of the privacy protection in the public sector. The statements made in paragraph 3.18 are internally inconsistent. Singapore should not aspire to the standards that were set by the Malaysian government in this area of data protection.
- The data protection regime should extend beyond Singapore - other laws in Singapore have extra-territorial reach, eg s 11 *Computer Misuse Act*.
- The exemption for the collection, use or disclosure of an individual's business contact information if it is solely for the purpose of enabling the individual to be contacted in relation to the individual's employment, business or should not be allowed.
- There should be no exclusions for artistic or literary purposes. The laws collection of personal data and photography in public spaces will interact with each other. There should be a specific exemption for photography in public spaces with exceptions to the exemption.
- Other possible blanket exclusions suggested concern procedures to determine entry into universities and hiring processes by employers.

- Data outsourced for processing to off-shore entities is not adequately protected.
- There are problems with the implied consent concept currently proposed.
- Large organisations should not be able to deem consent through notices and placing the burden of objection on individuals
- Minors below a certain age should not be able to give consent.
- The test for the collection of data is ineffective for protecting personal data.
- Organisations should not be able to disclose or share data without consent.
- It is problematic that the data protection regime implicitly allows personal data to be sold.
- There should be protection given for personal data that is illegally disclosed and which was obviously available to the public, albeit for a short period of time
- The employment exemption is too widely worded.
- The exception in paragraph 3.47 is too broad and is open to abuse.
- The research purposes exception is far too broad and too loose.
- The transfer of data offshore principle is ill-conceived when the whole regime is considered.
- Organisations ought to be required to specify the retention period at the point of collecting the personal data
- The exemption where it is “impractical for organisations to grant” access is unclear and too broad.
- The last exemption elaborated in paragraph 3.72 needs to be considered in conjunction with its overlap with Tort law.
- The exemption regarding references given for the purposes of education or employment is ill-conceived when the whole regime is considered. A better approach is suggested.
- The maximum penalty is not high enough when compared with France. Much also depends on how the penalty is levied, eg per breach.
- A breach notification requirement to the DPC *at the very least* should be mandatory. In the event of serious breaches, there should also be mandatory breach notifications to affected consumers. The time period should be as soon as possible, and not 1 month or 2 weeks like Citibank and Sony have done in 2011.
- A sunrise period of 12 months would be ideal.

- For existing data, individuals should be given the right to withdraw their consent, or to have their personal data deleted during the sunrise period.
- Do-No-Call Register is a wonderful initiative and a bonus to the data protection regime.

Specific Comments

Paragraph 3.3
It should be noted that compliance with the general data protection regime may, in fact, result in low or zero costs. This is so if the data protection laws mandate lesser amounts of data can be collected. Many organisations in Singapore tend to collect too much data from consumers, much of it is unnecessary but it is the mentality in Singapore that to collect more is better. If organisations collect lesser amounts of data, the reduced amount of data collected will mean that organisations will have less amounts of data under their control and hence, will have less to worry about in terms of errors, corrections, data security etc.

Paragraph 3.5
The role of the DPC to focus on educating businesses and the public is absolutely essential to change the mindset and culture amongst Singaporeans and Singaporean businesses. A complaints-based approach is the preferred regime. However, it is wise to give power to the DPC to conduct audits of its own accord, whether or not they are regularly conducted. The experience in the EU has been that without the threat of "on the spot" checks such as audits, organisations tend to slide into complacency about protecting data. It is also the experience in the EU that self audit reports submitted by organizations are useless for encouraging compliance with data.

For example, the EU Data Protection Supervisor has often found that what was submitted in the self-audit reports were vastly different from what they found when they conducted site audits. If the DPC is empowered with auditing powers, it should not increase any costs for organisations to comply with data protection laws because the organisation would already or should already be in compliance with the data protection laws, but yet it is a powerful incentive for businesses to comply. The only costs that may be incurred if an organisation is actually audited is perhaps the cost of one employee for duration of the site visit.

Paragraph 3.6
Is it one of the aims of having the data protection laws to comply with EU standards on data protection? If so, the exclusion of the public sector from the data protection legislation, and without clear enunciation of the actual rules governing the public sector, would make it extremely unlikely that the Singapore data protection law can be found to be adequate.

Paragraph 3.7
The technology-neutral approach is to be commended. The coverage to include all types of electronic devices such as mobile phones, tablets such as iPads, will be most helpful as many people and organisations utilise such electronic equipment extensively to store personal data.

Paragraph 3.8
The general baseline law applying concurrently with existing sectoral regulations

is the most workable solution as the other sectors such as health, banking and finance all have, or will have stricter rules governing them. MICA may wish to consider if the telecommunications sectors such as Internet service providers, and mobile phones telecommunication providers require special treatment.

Paragraph 3.9
The definition of personal data is sufficiently broad, for example, it appears to include an individual's mobile phone number (paragraph 3.11). It is hoped that in the actual implementation eg guidelines, heed will be paid to the points made in the EU Article 29 Working Party Opinion on the concept of personal data (Opinion 4/2007 on the concept of personal data of 20 June 2007 (WP136)).

Paragraph 3.13
The extension of data protection law to include non-electronic forms of personal data will bring about consistency. It is envisaged that since electronic forms of personal data are included, this would mean that personal data on devices such as mobile phones, and tablets would also be covered.

Paragraph 3.14
There does not appear to be any special protection for sensitive personal data. Whilst the desire for simplicity is appreciated, there ought to be protection for special categories of personal data that is particularly sensitive. These types of sensitive personal data can either be specified by category or can be defined generally as a class.

Whilst Article 8 of the EU Data Protection Directive prohibits the collection of and processing of special categories of data that are sensitive, Singapore need not take this extreme approach. However, there should be some protection against the collection and processing of some kinds of sensitive personal data generally with exemptions from the prohibitions. Data relating to health, employment, debts, financial standing may qualify as sensitive data in the Singaporean context. For example, many marketing questionnaires, surveys as well as applications for privilege cards for stores, cosmetic brands, department stores, restaurants, routinely collect information on an individual's salary or salary range and their date of birth. This type of information should not be collected at all by these organizations because if the information falls into wrong hands, they can be easily used to target individuals with high wealth for illegal purposes. Whilst marketers obviously would like to market their goods and services to those with wealth, this type of information should not be made available to them.

Paragraph 3.15
The personal data of deceased individuals should be protected, however, it may not fit neatly into a data protection regime that is designed to cover living individuals. Footnote 16 is unclear about what happens to the personal data of deceased individuals who have been deceased for more than 20 years. The law ought to require the deletion of personal data pertaining to deceased individuals unless required to be retained by law, or, where it is in the public interest to do so. This may be difficult to implement unless the data controller is informed of the death, but once the data controller is informed, then the data controller must delete the personal data. An example of where this is currently practised is the

providers of free e-mail. Many of the free e-mail providers such as Gmail and Yahoo will delete the e-mail accounts belonging to the deceased once they have been provided with copies of the death certificates.

Paragraph 3.17
The application to all persons by excluding a natural person acting in a personal domestic capacity is highly sensible. The exemptions in Australia, especially to small businesses with annual turnover of less than $3million, have proven to be riddled with many problems.

Paragraph 3.18
This paragraph states that the public sector in Singapore is governed by its internal rules and regulations regarding data protection. It also states that these internal rules are consistent with the principles of model code.

Two points can be made here. First, the model code is extremely light in protecting data of individuals. On the one hand, paragraph 3.18 claims that the public sector rules are based on the model code, which are extremely light, but yet on the other hand, the same paragraph claims that the public sector rules provide similar levels of protection for personal data as the proposed data protection law. With respect, this is not possible. The proposed data protection law gives much greater protection than the model law.

Secondly, whilst it is appreciated that the public sector will require data sharing for the essential functions of government and law and order, the rules should at least be made clear. It is true that in jurisdictions overseas such as Canada and Australia, the public sector is governed by a different set of data protection rules. However, those rules in those jurisdictions are codified and/or published. Furthermore, in Australia for example, an aggrieved data subject has rights of recourse where personal data has been misused by the public sector. The issue here is not about the collection or sharing or legitimate use of personal data by public agencies. Rather, the concern here is that there are adequate safeguards in place against misuse by staff or inadequacies in the technical systems.

It is true that Malaysia's personal Data Protection Act passed in 2010 only applies to private sector organizations. However, I do not think it is wise for Singapore to aspire to the standards that were set by the Malaysian government in this area.

Paragraph 3.22
It is true that where an organisation has no presence in Singapore, that it would be difficult to carry out investigations into any complaint made. However, to limit the scope of the data protection law in such a way is to deprive the regime of much force. Furthermore, other laws in Singapore have extra-territorial reach, eg s 11 Computer Misuse Act. For example, many marketing calls that are received in Singapore, come from China and India, who are obviously collecting and processing personal data. If the data protection regime does not include activities outside of Singapore, then it loses the opportunity to investigate and to give relief to Singaporeans.

Similarly, large multi-national organisations such as Facebook have been found

to routinely collect and process personal data without its subscribers knowledge. If the data protection regime is not given the power to pursue such breaches that are widespread and rampant, then, it is a regime that has limited force. Whilst there is the practical issue of enforcement against such out-of-jurisdiction activities, the mere fact that we have laws that these multinationals have flouted will often be enough for them to change their practices. This has already occurred numerous times with Facebook when it was forced by the Europeans to alter its computer programs and company practices and to cease the data collection and processing and sharing.

As data can be collected, tacked and processed over the Internet easily, using cookies, web bugs or even explicitly, it should not matter whether the personal data collection and processing occurs in Singapore or not and it should not matter where the organisation performing the collection or processing is located. This will also avoid arguments over the location of the activities. For example, some may argue that the collection is not made in Singapore even though the user is sitting at a computer in Singapore because the data captured may never be stored on a computer in Singapore.

Paragraph 3.25
The exemption for news organisations in the course of news activity is sanctioned by Art 9 of EU Data Protection Directive and whilst not ideal, but given the tight guidelines for one to be a news organization in Singapore, this should not pose problems.

The exemption for the collection, use or disclosure of an individual's business contact information if it is solely for the purpose of enabling the individual to be contacted in relation to the individual's employment, business or profession is problematic. There does not seem to be any justification for this exemption. In fact, it can be covered already by the principle of implied consent. So, for example, if one hands to another one's business card, there is obviously implied consent that the details of the individual's employment, business or profession can be collected and there is an invitation, albeit implied, that one can be contacted, by either the recipient of the business card or the organisation to which the recipient belongs. There is therefore no need for this exemption. This exemption will only encourage more marketing or cold calls. For example, it is arguable that individuals' contact details can be collected, used and disclosed for the purpose of being contacted to buy anything that the business may need, from printer cartridges, to mobile phones, to signing up business credit cards and so on. This exemption would actually burden SMEs as they may likely face an increase in unsolicited contacts from marketers. For large organisations, it is not feasible to list all their phone numbers on the Do-Not-Call Registry.

As a practical matter, I have received numerous marketing calls on my office number. If I were to put my office number on the Do Not Call Register, these marketers can still collect and process my telephone number under this exemption. It would be neater and cleaner if there were no such exemption.

Paragraph 3.26
There should be no exclusions for artistic or literary purposes. It is inconceivable

that one's personal data protection can be so easily lost if some nosey person using the guise of creating an unauthorised biography can be exempt from the law. This goes against the very heart of the rationale of protecting an individual's privacy. The same arguments also apply for plays.

As for photography, there may need to be some clearer understanding of how the collection of personal data and photography in public spaces will interact with each other. On the one hand, if there are no exemptions for photography, then, any photographs taken in public spaces will have to ensure that no individual's face is captured, as the capture of an individual's face will clearly fall under the definition of collection of personal data. This may be impractical, especially if tourists are simply snapping holiday shots in busy places such as Orchard Road.

It is suggested that the data protection law allows a narrow exemption for the taking of photographs in public places. In addition, MICA may also wish to consider whether it wishes to insert provisions covering the taking of photographs in public places of essentially embarrassing activities. In the UK, and other countries where the media is less restrained, the courts have had to create torts to protect well-known identities and celebrities from the prying eyes of the press whilst they go about their daily activities. While Singapore does not have such an unruly press, clarification in the Data Protection Act may serve to avoid any legal disputes landing in the courts in the future.

Other possible exclusions

The employment setting throws up some questions about the protection of personal data from both sides.

From the side of the employer, there may be a desire to obtain as much information as possible about a potential employee before hiring that person. As such, employers would want to be able to collect as much information as possible about that person before making a decision on hiring. In some European countries, companies have been prohibited from doing this as there are no general exemptions for employers in the course of making hiring decisions. In fact, companies in Germany have fallen foul of the law by accessing publicly available information about a potential employee on Facebook. This is somewhat problematic as on the one hand, a company is required to exercise due diligence in its hiring process but yet, its hands are tied if there are no exemptions from the data protection law allowing it to do so.

However, the exemption to employers should only be in the course of the hiring process, and not otherwise. Such a narrow exemption will also prevent unsuccessful applicants for jobs from seeking and accessing the personal data company has on him or her, including what sources were used and challenging the hiring decision. The employment setting issues is further discussed below.

Similarly, there is an issue for applications to universities here in Singapore. When I was a full-time professor at NUS Law School from 2007 to 2011, the admission process was very rigourous. The students had to sit a written test, as well as attend an interview with members of the faculty. During the interview

process, notes obviously had to be taken, and reports had to be submitted, and all applicants had to be ranked. If there are no exemptions, however narrow, for the selection process of university entry, then all of this information would clearly constitute personal data, which all unsuccessful candidates are entitled to access. This would not be an ideal situation as the contents of those reports are for internal purposes and are confidential to each university.

I would therefore also suggest a blanket exemption for universities in the process of admission of students.

Paragraph 3.28
The proposal of not having any distinctions between data controllers and data processors is very sensible. This distinction which has been adopted in the EU has been found to be cumbersome and unworkable.

The holding of an organisation responsible for data protection even though it has been outsourced is also very sensible. However, it is unclear from the consultation paper what happens if the outsourcing is done by a company located overseas. It appears from paragraph 3.22 that any activity, including outsourced data processing, that does not occur in Singapore will not be covered by the data protection law. This would appear to be a major loophole which can lead to an abrogation by the original organisation of its duties to protect personal data. It should be made explicit that even when an organisation outsources to an offshore location, that organisation is still responsible for the management of such personal data. This is especially needed if the government persists with its current stand that the Data Protection Act should only cover activities located in Singapore.

Paragraph 3.31
The prohibition that 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 is to be commended. The necessity test that is used here is to be applauded as it gives high protection.

Paragraph 3.32-3.33
The inclusion of implied consent is to be commended for its practicality. However, the legislation perhaps should specify whether or not it is possible for multiple implied consent to be deemed, and whether the primary purpose of collection can be implied, in addition to secondary purposes. It appears that the primary purpose can be implied, as well as secondary purposes. If this is the case, it may be too loose and the primary purpose should be explicit and not implied. And from there, implied purposes may be inferred.

It is also troubling that one of the criteria for inferring implied consent is “it would be awkward for organisations to have to obtain explicit consent from the individual”. This is unnecessarily broad, given the actual example given in paragraph 3.33, which is relatively narrow.

For example, if one visited a TCM provider, could the TCM provider argue that it is “too awkward” to obtain explicit consent from a patient to process her personal

data for a secondary purpose because it concerns female private parts?

The meaning of deemed consent or implied consent needs to be more tightly worded. In any event, the examples given for deemed consent or implied consent are not very helpful as they are obviously cases dealing with serious matters such as one's life and health. There are many other industries, such as real estate agents and telemarketers who are likely to abuse the implied consent if it is not tightly worded.

Paragraph 3.35
The proposals set out in this paragraph are unfair and it would be more appropriate for use in the scenario concerning existing data prior to the sunrise period. Large organisations should not be able to deem consent through notices and placing the burden of objection on individuals. If organisations want to collect, use or disclose personal data, they obviously have the means and resources to do so, hence, they should bear the burden and costs of obtaining consent. Individuals, have limited time and resources, and should not bear the burden and time and trouble of having to opt out. It is unreasonable on individuals to waste their time where it is the organisation who wishes to obtain all the benefits.

Paragraphs 3.36 and 3.37
The suggestions here in these two paragraphs are to be commended. However, it is unclear from paragraph 3.37 whether minors have the capacity to give consent. This has been an issue in some overseas jurisdictions where websites collect the personal data of children younger than 13 years old without parental consent. These often come in the guise of competitions where children can win prizes but in actual fact, the data collected far exceeds that is necessary for the competition. Of course, children being children, are not in any position to understand the ramifications of what they are doing. I would recommend that in order for children to be protected, that children under a certain age should be deemed lacking in capacity to give consent.

Paragraph 3.38
The requirement of having a data protection officer is highly commended, Even though this may or may not be a dedicated data protection officer.

Paragraph 3.40
The test here for the collection of data is somewhat unclear. The test seems to be that organisations may only collect personal data for purposes that would be considered appropriate in the circumstances. If this is the case, then this is weak protection. The test is focused on whether the *purpose* for collection is appropriate. Many times, there is of course an appropriate purpose for the collection of personal data - it is the extravagant amount of information collected that ought to be curbed. The focus here ought to be, like in many other jurisdictions, whether or not what is collected is appropriate or necessary *for the purpose.*

As an Australian, I am amazed and appalled at how much information is often collected by organisations for simple things such as lucky draws, joining a

privilege card program at the eatery or even to be on the mailing lists of a brand of cosmetics and a large department store. This is the type of excesses that the data protection legislation should curb. It is inconceivable that a cosmetic counter at Robinsons would require the name, date of birth, NRIC number, E-mail address, home address, home telephone number, mobile phone number, occupation, and a whole host of other information from a customer just so that they can send out mailers to customers about special promotions. The amount of information collected is simply disproportionate for the purpose. By having so much personal data of customers, the organisation is also exposing itself to greater security risks and cannot hope to adequately protect the personal data of its customers. With the large amount of information that an organisation holds, the risk of fraud, identity theft, and other crimes is substantially increased.

It is for this reason that the proposal in paragraph 3.40 is in practice useless. In the above scenario, the cosmetic counter would of course satisfy the test of having a purpose that is appropriate, but the amount of personal data collected is simply astonishing. If the government allows such excesses to continue, it will render the whole data protection regime useless as people will be under the illusion that they must hand over so much information, and without realising that handing over so much information will jeopardize their own financial and personal safety.

Paragraph 3.41
The last sentence of this paragraph appears to allow organisations to share personal data with each other as long as the purposes for the collection and the holding of the personal data coincide. This is a terrible and unfair proposal from the perspective of the consumer. It also makes it impossible for the consumer to control or to even know which parties have their personal data. An example will illustrate the point. A consumer may have given her personal data to a real estate agent to help her find a unit to buy or rent. Under this proposal, the real estate agent would be permitted to pass on her details to another agent as the purposes of both agents would appear to coincide. However, the consumer may not wish that her abusive husband know about her plans to rent the unit as she wishes to escape from the abusive relationship. Under the current proposal, many agents could legally collect and disclose the intentions and the personal data of the consumer without her knowledge or consent. Imagine if amongst the many agents, one of the agents know the husband, and not realising the full context, reveals to the husband that he has found a unit for his wife.

Paragraph 3.42
All the exceptions here appear to be sensible and reasonable but the general test of what is considered to be “impractical” ought to be narrow.

Paragraph 3.43
This appears to be a practical approach, however, should there be any protection given for personal data that is illegally disclosed and which was obviously available to the public, albeit for a short period of time? Instances of this may be where, for example, compromising photos were obtained and disclosed without consent. The data subject should have protection to prevent the continued distribution, or disclosure of the photos.

Paragraph 3.44
This is a problematic proposal. In footnote 24, the ambit of the exclusion is that "does not include data that is not about an individual's employment". In this modern age of employment, there is actually very little that employers will argue that does not fall within the category of "about an individual's employment". In many organisations, a person's health, a person's marital status, the number of children one has, where one goes for their annual leave, and so on are all information about an individual's employment. This proposal, in effect, allows the employer to collect almost any personal data about the employee without consent. This may also become problematic in sexual harassment cases. Both the alleged harasser and the victim may end up having their personal sexual history, sexual partners and so on being documented and collected by the employer. The conglomeration of data poses substantial risks if they are accessed or disclosed, even if through human or technical fault, and not through deliberate action.

The proposal amounts to a blanket exemption for employers as much data can be argued to be "employee personal data" and can be argued to be "reasonable for specified purposes".

At a more general level, there should be guidelines given that provide that only a small number of persons within an organisation should have access to an individual's personal data. For example, at the National University of Singapore, the database of the library is somehow linked to an employee's database so that the librarians have access to the home address and telephone numbers of its borrowers, namely all the staff at the National University of Singapore. This is totally unnecessary, as the library can contact the staff member through the office address or telephone number. By giving employers exemptions from consent, this sort of lax management of employees' personal data will continue, and it may be very difficult for an individual to trace where their personal data is being linked or disclosed. There are too many weak links in the system.

It is suggested that all employment data should be governed by the data protection law with the exception of hiring processes as explained above.

All organisations should be required to seek consent for the collection of personal data for identification or internal circulation purposes. However, in the security conscious state of Singapore, it may not be tolerated by any employer that an employee should decline photo identification for security reasons. Hence, in the event that an employee refuses consent for photo identification, should the employer have the right to terminate the contract?

Paragraph 3.47
This proposal is practical but is problematic in its current form. It is true that such scenarios will often arise in the health setting, such as when a patient is elderly, and may not communicate well and may require another person to furnish their personal data. However, the exception should be more narrowly defined to refer only to instances where the data subject requires or desires the services. Otherwise, the exception is too broad and is open to abuse.

Paragraph 3.49
The prohibition on secondary uses is commendable, as is the requirement that the use or processing be reasonable and fulfil only the purposes for which the consent was obtained.

The same objections raised in relation to paragraphs 3.42 to 3.48 are also applicable here.

Paragraph 3.51
The general rule here regarding disclosure is problematic for the reasons already explained above. Disclosure of personal data should not be permitted without consent. The whole point of personal data protection is so that individuals can control their personal data to a certain extent and thereby protect personal data. The proposal set out here in reality gives individuals very little protection.

Just because an individual has consented for his or her data to be collected for a specific purpose does not mean that the individual will also consent for the personal data to be disclosed to another party for the same purpose. Another two examples may assist to illustrate the point. A consumer may give her personal details to a car dealer as she is looking to buy a second-hand Porsche. This does not mean that that she would want to buy a second-hand Porsche from another car dealer, given the rather sleazy nature of some second-hand car dealers. However, under the proposal, the disclosure of her personal details by the first car dealer to the second car dealer would be perfectly legal as the disclosure would be "in-line with" the purpose for which the individual's consent was originally obtained.

Secondly, if one were to apply for membership of gym or spa or any other organisation, or even to apply for a store's discount or loyalty card, much more detail about oneself would need to be provided. Again, all these organizations would be free to pass on the personal details to organisations offering similar services. Worst still, consumers' personal data can be legitimately **sold to third parties**. The domino effect of the proposal in this paragraph cancels out all the good the rest of the data protection regime hopes to achieve.

Paragraph 3.52
The concerns raised earlier with respect to paragraphs 3.42 to 3.48 are also applicable here.

Paragraph 3.55
At the top of page 19 of the Consultation Paper, there is an exception for information disclosed "for research purposes, and including statistical research". This exemption for disclosure is far too broad, and far too vague. There is not even a tempering through requiring that the research be in the public interest, or for the public good. Nor are there any requirements that the information be de-identified or anonymised. Further, the proposal here gives a clear mandate for personal data to be sold. This exemption may be

acceptable for medical purposes only but since “research purposes” is so broad, it would easily encompass market research.

In the specific scenario referred to in the paragraph, the various sentences seem to contradict each other, thus it is unclear what is the exact scope of this exception. In the second line from the top of the page, the sentence begins with “in situations where” thereby limiting the exemption to where it is impractical to obtain consent and the research purpose cannot be accomplished unless the individuals are identified. In this scenario, no consent is required from the individuals as long as “the personal data is not linked to other information that could be harmful to the individuals”. However, the sentence finishes by stating that “the benefits to be derived from the linkage are clearly in the public interest”. So, on the one hand, the proviso is that the data is not linked to other information that could be harmful to individuals, however, in the next breath, it allows for the linkages if they are clearly in the public interest. So what happens if the linkage is harmful to the individuals but in the public interest?

This exemption also appears to take the exception one step further to allow not just disclosure of personal data for research purposes without consent, but also to allow data matching. Data matching is one of the worst evils as it allows organisations to collect, hold and process large amounts of data about any given individual thereby threatening the physical and financial security interests, as well as privacy interests, of individuals. Data matching should not be permitted unless it is for health, safety or security purposes.

The exemption presented here is far too broad. At the very least, rather than “public interest”, it should be amended to something narrower, such as, public health, safety, or security.

The requirement that organisations using the personal data for research must remove or destroy individual identifiers “at the earliest reasonable opportunity” is very weak. For all research purposes, individual identifiers should be removed before the research is conducted, except for health, safety, or security research where this may not always be possible.

Paragraph 3.56

As already mentioned, research purposes can include market research, and since the identity of the consumers are known to the market research companies, such companies have a vast amount of information on individual consumers. Whilst at some levels, this may seem harmless, it may lead to harmful outcomes. Take the example of a credit card company which discloses the full statements of its customers for the past five years for so-called market research purposes. It may be that an individual will holiday at the same destination at the same time every year because of work constraints. This information, being available to third parties who may not always be law-abiding, may result in thieves committing crimes at the individuals' homes while they are away on holiday. Consumers should be free from this type of surveillance, tracking and intrusions upon their private affairs.

Paragraphs 3.60 to 3.61

It seems the proposal here is inconsistent with previous principles in the proposed data protection regime. There should be a single rule that extends to activities outside of Singapore. Then, there would be no need for a separate rule to cover organisations that transfer personal data outside Singapore. The proposal in these paragraphs simply require that appropriate measures are taken to protect personal data where such data is transferred outside Singapore. There is no definition of appropriate measures. What would satisfy appropriate measures? Little processing? No processing? Are disclosures permitted? Disclosures to whom? As already mentioned above, a company based in Singapore can simply **sidestep** the whole data protection regime by sending personal data offshore to be processed and disclosed.

Rather than following the stringent requirements under the EU principle of adequacy in Articles 26 and 26 of the Data Protection Directive, the rule could be as simple as requiring the transferred data to be protected at the same or equivalent level as in Singapore. This is at least clearer than simply stating the requirement to be that the measures are “appropriate”.

Paragraphs 3.62 to 3.66
All the proposals presented here are sensible.

Paragraph 3.67
Organisations ought to be required to specify the retention period at the point of collecting the personal data. This will prevent data from being kept indefinitely – from my professional experience in conducting privacy audits for large multi-national companies, there have been instances where personal data is kept for 30 years!

Having such a requirement will also assist individuals when they wish to correct and control their data as they would not need to worry about those data which have already past their “expiry date”. For example, if an individual's home address is collected and she is informed that the information will be deleted after the goods are delivered (or after a few days after delivery), the individual need not worry about that piece of information being abused after the goods are delivered. A case in point here may be businesses such as Pizza Hut. Pizza Hut delivery will collect the consumer's name, telephone number and home or delivery address and if the person paid by credit card, their credit card number. This information appears to be kept in the Pizza Hut company system indefinitely, as the next time the person calls and gives the telephone number, the Pizza Hut staff is able to recite back to the customer all the information. There are two concerns regarding this. First, any Pizza Hut staff answering the telephone will have access to an individual’s full details including delivery/home address once they type in the telephone number. There are opportunities for rampant abuse. Secondly, if one knows the telephone number of one’s enemy, to find out that person’s home address, they simply ring Pizza Hut and pretend to place an order using the enemy’s phone number and Pizza Hut will disclose the enemy’s home address. There is no security, nor privacy. It would be better if Pizza Hut would delete all my details once the delivery has been made.

Paragraph 3.68
As already stated above, for the purpose of hiring only, employers should be granted exemptions from access by the data subject. In addition, there should also be an exemption from access for entry into universities and other higher educational institutions. Access to an individual's personal data should be granted for all other functions of employers and higher educational institutions. The reasons for this is to ensure there is no misinformation being held and further disseminated by organisations and to assure individuals of the right to control their data.

An example may illustrate the point better. An ex-employee who may have left an organisation on bad terms may wish to ensure that her superiors do not unfairly and without cause alter records pertaining to her and to paint her in a negative light. This may be important for the ex-employee as current and future employees, especially those working in human resources department, will have access to her records, and also, enquiries by government departments and instrumentalities may be made on the ex-employee's record.

Otherwise, the general right given to individuals to request access to their personal data and to correct inaccurate data is to be commended.

Paragraph 3.71
The exemption where it is "impractical for organisations to grant" access is unclear and too broad. The examples given in the paragraph are non-contentious examples such as legal privilege or data that was collected or created through mediation or arbitration processes. However, the test of "impractical" is too vague and too general. Something could also be argued as impractical if it is too troublesome or if the organisation simply does not wish to disclose the information. If the examples given in paragraph 3.71 represent the scope of the exemption, then the wording of the exemption should be limited by those examples. For example, the exemption could be simply worded as: where the data is confidential or where the data was created or collected in a course of mediation or arbitration.

By having the test for exemption to be "impractical", this can be mis-used in a very wide range of scenarios and would render the right given to data subjects completely useless.

Paragraph 3.72
Many of the exemptions elaborated here are sensible. However, there may be questions of overlap between tort law and the proposed exemption covered in the last sentence. There may be cases where under tort law, there is a duty of care to inform another, but under the exemption in the last sentence, this would be prohibited.

A case in point is a case from a New Zealand court some 15 years ago. A husband had contracted some sexually transmitted disease, and failed to inform the wife. Both the husband and wife were treated by the same general practitioner. When the wife grew suspicious, she questioned the general practitioner who declined to disclose any information. Subsequently, the wife

contracted the sexually transmitted disease and took legal action against the doctor for not exercising his duty of care to protect her.

Perhaps the last exemption in this paragraph should be clarified so that it is subject to existing duties of care or other laws or regulations.

Paragraph 3.73
The last exemption in this paragraph regarding references given for the purposes of education or employment touches on the very points I have made already. Rather than a specific exemption expressed in such a limited and narrow manner, a more general exemption from the entire data protection regime should be created for any activities related to entry into tertiary educational institutions as well as activities related to the hiring processes.

Paragraph 4.4
The proposed penalty regime, that is, one by tiers, is an appropriate one. Large scale blatant breaches by large organisations ought to be penalised on a much greater scale than small inadvertent breaches by individuals or SMEs. In this vein, the proposed ceiling of $1 million is not high enough. This number appears to be pegged to the UK maximum of GBP500,000. However, in France, legal entities can be fined up to €1,500,000 for data breaches.

In addition, it needs to be taken into consideration whether the penalty is expressed as “per breach” or not.

Furthermore, financial penalties should be levied where there are obvious disrespect or disregard for data protection laws, *irrespective* of whether significant harm is caused or not.

In addition to the rectification of non-compliance with the data protection law, and the payment of penalties, the DPC should also have the power to order apologies or notices to be placed in the media by those who breach the data protection law. This would be an added deterrent.

The extra sanctions in the event of organisations or individuals who obstruct those charged with the performance of their duties or powers under the data protection act is highly commended. Similarly, criminal penalties for misleading or attempting to mislead the DPC are also appropriate.

Paragraph 4.6
The idea of an independent appeals board is excellent, as is the availability of judicial review of the appeal board's decisions.

The right given to individuals to separately seek redress by civil proceedings in court is also to be applauded – this would render the remedies given to consumers more comprehensive than many jurisdictions in the world.

Paragraph 4.8
Whilst it is helpful for the DPC to initiate investigations, as already mentioned above, it should also be empowered with the right to conduct irregular or

regular audits, more for deterrent purposes than anything else.

The overall tone of the approach to settling disputes through requiring the parties to mediate first is positive and definitely a step in the right direction.

All the circumstances for not pursuing investigations outlined here are sensible and appropriate.

Other possible remedies

As a matter of security, fairness and efficient protection of personal data, there ought to be breach notification requirements. Although there is currently no breach notification requirement in the EU Data Protection Directive, the Vice-President of the European Commission and EU Justice Commissioner, Vivien Reding, has in June 2011 outlined updates to EU legislation for the protection of personal data, following a public consultation throughout 2010. Mandatory requirement to notify data security breaches will be introduced. Mandatory requirement to notify data security breaches has already been in effect in the telecommunications and ISP sectors for a number of years (see DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009).

For the purposes of a light–touch regime such as that being proposed for Singapore, a breach notification requirement to the DPC *at the very least* should be mandatory. There is very little cost involved for the organisation to do this, but yet, the benefits are great to the consumer. In addition, in the event of serious breaches, there should also be mandatory breach notifications to affected consumers. This would greatly enhance consumers' confidence in data security and oversight mechanisms.

The time period for the breach notification to occur should be as soon as possible after the discovery of the breach. Earlier this year, it took Sony one whole week to notify breaches to its online gaming system which resulted in the theft of customers' direct debit details, credit card details, names, addresses, email address, birth dates, usernames, passwords, logins, security questions etc. A second similar breach earlier this year of customers' personal data at Sony took over 2 weeks to be notified as Sony did not discover the breach until about 11 days after the breach. All these time periods are unacceptable as customers do not even have a fighting chance to protect their own bank accounts.

Another major breach this year was that of credit card details from Citibank in the US. Citibank waited over one whole month before making the extent of the breach public. This is simply unacceptable.

Paragraph 4.13 - Sunrise" period

One single sunrise period for all provisions will be simpler to implement. However, there may be advantages in having staggered sunrise periods to encourage early thought to data protection, rather than having a long sunrise

period clause with all parties scrambling to implement compliance at the very last minute.

A sunrise period of two years is, in my view, too long. Organisations will be complacent for the first year or more, and only begin to start springing into action six months before the sunrise period ends. In my view, a sunrise period of 12 months would be ideal. After all, most if not all the proposals contained in the Consultation Paper are simply business best practices which all organisations should have already been adhering to. If however, the government adopts higher principles than those currently proposed, then perhaps a period of 15 to 18 months might be appropriate.

Paragraph 4.15
It would be totally unworkable if existing personal data is exempt from the data protection regime. It would be too difficult, if not impossible, to trace back when a piece of personal data was collected.

Paragraph 4.17
Whilst the suggested solution by MICA is a practical and workable one, however, it would be much better if individuals are given the right to withdraw their consent, or to have their personal data deleted during the sunrise period. To make this manageable for organisations, the onus should be on the individuals to inform the organisations that consent is withdrawn and to request that their personal data be deleted. Obviously, this would be subject to whether or not it would be legally possible for the organisation to delete the said data as there are obviously areas where laws and regulations require retention.

This will also serve as a "wake up" call to organisations that they need to tidy up their collection and use of personal data, and, that data protection will be a reality in Singapore very soon.

Part V
This is a wonderful initiative and a bonus to the data protection regime. However, as already documented earlier, many marketers and even fraudulent marketers, are calling from China and India. Most of the time, the phone numbers have been sold to them and consumers have never given consent.

Whilst the difficulty of the extraterritorial application of laws in Singapore is appreciate, there are pieces of legislation such as the Computer Misuse Act (section 11) which have enacted extraterritorial reach. Hence, it would be helpful for the coverage of the Do Not Call Registry to apply also to callers outside Singapore.

General Comments

The EU gold standard of only allowing data to be collected for specified, explicit, and legitimate purposes, and to only collect that is relevant and necessary should

apply. Similarly data should only be processed fairly and lawfully.

There does not appear to be any requirement that data is processed on a confidential basis, which means there is not imposition of any positive requirement on the data processor to limit access to and protection of the personal data when conducting processing.

There should be specific provisions concerning NRIC numbers. Two specific prohibitions are essential. First, no private organisation should require persons to disclose their NRIC numbers unless it is required by law. Second, no private organisation should be allowed to use the NRIC number as the means of identifying the individual.

The NRIC number is a unique number and an important number in the life of the Singaporean, especially vis-à-vis dealings with the government. It should be guarded and protected and not be freely given away to private entities. It should be protected in case the simple knowledge of the NRIC number is misused. When a party has a person's NRIC number, this number, when combined with other pieces of personal data about the individual, can be easily used to perpetrate identity theft and other crimes.

The collection and processing of the NRIC number also greatly assists data matching and sharing across databases by private organisations which can also lead to identity theft and other crimes. The profiling that is possible with data matching is also against the interests of individuals.

It is totally inconceivable why a cosmetic counter at Tangs would need an individual's NRIC number just to send out marketing materials. Similarly, why would a bookshop need the NRIC number just to issue a discount/loyalty card to a customer?

Similarly, organisations should be prohibited from using the NRIC number to identify the individual. An example might illustrate the point better. At some educational institutions, the staff number used for staff is the same as their NRIC numbers. Furthermore, the library card also uses NRIC Numbers. This means that everybody who works in the library also has access to employees' full name and NRIC Numbers, and possibly other details about the staff member such as their date of birth, home address etc. The NRIC number should be kept private