Parliament No:	12
Session No:	1
Volume No:	89
Sitting No:	8
Sitting Date:	15-10-2012
Section Name:	Second Reading Bills
Title:	Personal Data Protection Bill
MPs Speaking:	[Mr Chen Show Mao (Aljunied), Mr Desmond Lee (Jurong), Assoc Prof Fatimah Lateef (Marine Parade), Mr Teo Siong Seng (Nominated Member), Mr Ang Wei Neng (Jurong), Mr Patrick Tay Teck Guan (Nee Soon), Mr R Dhinakaran (Nominated Member), Mr Lim Biow Chuan (Mountbatten), Mr Gan Thiam Poh (Pasir Ris-Punggol), Assoc Prof Dr Yaacob Ibrahim, Mr Speaker, Mr Zaqy Mohamad (Chua Chu Kang), Mr David Ong, Assoc Prof Dr Yaacob Ibrahim, Mr Speaker, Ms Jessica Tan Soon Neo (East Coast), The Chairman, Assoc Prof Dr Yaacob Ibrahim, The Chairman, Assoc Prof Dr Yaacob Ibrahim, The Chairman, Asst Prof Tan Kheng Boon Eugene, Ms Tan Su Shan (Nominated Member), Ms Low Yen Ling (Chua Chu Kang), Mr Chen Show Mao (Aljunied), Mr Desmond Lee (Jurong), Assoc Prof Fatimah Lateef (Marine Parade), Mr Teo Siong Seng (Nominated Member), Mr Ang Wei Neng (Jurong), The Minister for Information, Communications and the Arts (Assoc Prof Dr Yaacob Ibrahim), Mr Patrick Tay Teck Guan (Nee Soon), Mr R Dhinakaran (Nominated Member), Mr Lim Biow Chuan (Mountbatten), Mr Gan Thiam Poh (Pasir Ris-Punggol), The Chairman, Assoc Prof Dr Yaacob Ibrahim, The Chairman, Assoc Prof Dr Yaacob Ibrahim, Mr Zaqy Mohamad (Chua Chu Kang), Mr David Ong, Ms Jessica Tan Soon Neo (East Coast), Ms Low Yen Ling (Chua Chu Kang), Asst Prof Tan Kheng Boon Eugene, Ms Tan Su Shan]

PERSONAL DATA PROTECTION BILL

Order for Second Reading read.

3.10 pm

Assoc Prof Dr Yaacob Ibrahim: Mr Speaker, Sir, I beg to move, "That the Bill be now read a Second time." Sir, today, vast amounts of personal data are collected, used and transferred for a variety of reasons. This trend is expected to grow exponentially as infocomm technologies like high-speed computing and business analytics enable the processing of large amounts of personal data. A data protection regime to govern the collection, use and disclosure of personal data is necessary to address individuals' growing concerns over the use of their personal data and to maintain individuals' trust in organisations that manage data.

To date, Singapore has adopted a sectoral approach to data protection. There are numerous Acts within the public sector that contain statutory secrecy and disclosure provisions to regulate the collection, use and disclosure of information by public agencies and their officials in carrying out their statutory functions. Within the private sector, specific provisions in various sector-specific laws protect personal data, such as financial and health data. There are also industry codes of practice on data protection, such as the Model Data Protection Code released in 2002, for voluntary adoption by the private sector. However, as current sectoral frameworks are disparate, there is a need for a general data protection framework to ensure a baseline standard of protection for individuals' personal data across the economy.

Page: 828

The personal data protection law will safeguard individuals' personal data against misuse by regulating the proper management of personal data. Individuals will be informed of the purposes for which organisations are collecting, using or disclosing their personal data, giving individuals more control over how their personal data is used. A data protection law will also enhance Singapore's competitiveness and strengthen our position as a trusted business hub. It will put Singapore on par with the growing list of countries that have enacted data protection laws and facilitate cross-border transfers of data.

Sir, let me now elaborate on the proposed Personal Data Protection Bill. In formulating the Bill, we have sought to balance individuals' interests with the need to keep compliance costs manageable for organisations. We have also sought to ensure that Singapore's data protection regime is relevant and in line with international standards for data protection. To this end, my Ministry has studied the data protection frameworks in key jurisdictions, including Canada, New Zealand, Hong Kong and the European Union, to develop the most suitable model for Singapore. In addition, references were made to international guidelines, such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the APEC Privacy Framework.

The Bill has also incorporated relevant feedback and suggestions received from three rounds of public consultation conducted over the past year. Close to 1,900 responses were received from individuals and organisations, and we took them into consideration when reviewing the draft law. In particular, we have sought to address organisations' concerns about potential compliance costs, while maintaining a suitable level of protection for individuals.

Mr Speaker, Sir, I will now outline the key aspects of the Bill. The Bill provides a framework for the protection of personal data, which refers to data that relates to an identifiable individual, whether the data is stored in electronic or non-electronic form.

The framework will apply to all organisations, with certain exceptions. For example, the data protection rules in Parts III to VI will not apply to public agencies and organisations acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data. Some public agencies collect data where necessary to carry out their regulatory and statutory functions effectively. To ensure that the data is properly managed and protected, the public sector has its own set of data protection rules that are based broadly on the same data protection principles as the Personal Data Protection law. In some cases, these rules are even stricter than the requirements under the Personal Data Protection law. Some Acts also contain statutory provisions which regulate the collection, use and disclosure of information by the public sector. Together, these ensure that public agencies and officials are accountable for meeting strict requirements to ensure the confidentiality of personal data in their care.

Page: 829

Recognising that not all organisations have the same degree of control over personal data, the Bill provides certain exceptions for organisations referred to as "data intermediaries".

A data intermediary is an organisation that processes personal data on behalf of another organisation. The Bill provides for such organisations to be subject only to obligations for the care and retention of personal data that they process on behalf of another organisation, pursuant to a written contract.

The Bill is intended to apply concurrently with other laws and regulations enacted in Singapore. Organisations regulated by sector-specific laws and regulations today will thus continue to comply with the requirements under current laws and regulations as well as the Bill going forward. To avoid inconsistency between the Personal Data Protection law and sector-specific regimes, clause 4, subsection 6 of the Bill provides that Parts III to VI will not override other sector-specific laws and regulations, or anything imposed or expressly permitted by the law. The provisions of other written laws shall prevail where there is any inconsistency.

Part III of the Bill sets out the general responsibilities of an organisation for the personal data it holds or controls. Part IV sets out specific rules relating to the collection, use and disclosure of personal data, while Parts V and VI relate to access and correction, and care of personal data respectively. Sir, these rules are based on the principles of obtaining consent, specifying purpose, and reasonableness.

In general, an organisation can only collect, use or disclose the personal data of an individual with the individual's consent, and for a reasonable purpose which the organisation has made known to the individual. An organisation is also required to provide individuals access to their personal data and consider requests to correct the personal data it holds or controls. In relation to care of personal data, the Bill sets out obligations for ensuring the accuracy of personal data, the protection and retention of personal data, and the transfer of personal data out of Singapore.

Sir, I will now elaborate on the provisions governing consent. Clauses 13 to 16 provide that an organisation may only collect, use or disclose an individual's personal data if consent is given, or deemed to be given, by the individual for purposes specified by the organisation, unless exceptions apply. Consent is not considered valid if obtained by false or misleading means. In addition, organisations may not

impose terms and conditions requiring the individual to consent to the collection, use or disclosure of personal data beyond what is reasonable to provide the product or service to the individual.

Page: 830

While organisations are generally required to obtain consent, we recognise that it may not be practical for consent to be obtained in every situation. Clause 15 of the Bill provides for consent to be deemed when the individual voluntarily provides the personal data for a purpose, in a situation where it is reasonable for him to do so. For example, a person provides his personal data when registering with a clinic to seek medical treatment. It would be reasonable to deem that the person has given consent for the clinic to use his personal data for purposes related to his medical treatment at the clinic, and there is no need for the clinic to seek his consent in such situations. The provision for deemed consent enables organisations to collect, use or disclose personal data for reasonable purposes in situations where the individual need not give consent.

Even after consent has been given or deemed, clause 16 of the Bill provides that the individual may withdraw his consent, with reasonable notice provided to the organisation. It also spells out an organisation's obligations in relation to an individual's withdrawal of consent.

The Bill also provides for situations where collection, use and disclosure of personal data may take place without consent. These situations are listed in the Second, Third and Fourth Schedules respectively. These are typically purpose-based exceptions based on international practice. For example, personal data may be collected, used, or disclosed without consent where necessary for investigations or, where necessary, to respond to an emergency that threatens the life, health or safety of an individual.

Recognising that there is a legitimate need for artists and news organisations to be able to carry out their artistic or news activities without undue impediments, the Bill provides for collection without consent for artistic and literary purposes, and for news activities by news organisations.

Sir, at this juncture, I would like to highlight that I will be moving a Notice of Amendment after this in the Committee stage. The amendment will provide a clear definition for what constitutes "news activities" and "news organisations", to which clause 1(h) of the Second Schedule applies. The intent of clause 1(h) is to enable the legitimate collection of personal data without consent in the course of news gathering activities by organisations that are in the business of news. It is not intended to give all other organisations the unfettered ability to collect and publish a person's personal data under the guise of "news reporting". This is to provide members of the public some measure of protection from potential misuse and unwarranted publishing of personal data.

The Bill also permits the collection, use or disclosure of personal data without consent where the data is generally available to the public. This would include personal data that can be observed by reasonably expected means at a public location or event at which a person voluntarily appears. The intent is not to unduly limit activities performed in the public under reasonable situations, such as photography in public places.

Page: 831

There are also exceptions to the requirements in Part V for organisations to provide individuals with access to their personal data, as well as to correct their data. These exceptions, listed in the Fifth and Sixth Schedules, cater for situations in which the handling of access requests may be overly onerous or compromise confidential commercial information.

In line with the principle of keeping compliance costs manageable, the Bill adopts a practical approach to personal data collected before the data protection rules take effect. Recognising that it may be overly onerous for organisations to seek fresh consent for all previously collected personal data, the Bill allows organisations to continue to use such personal data as long as they are for reasonable existing uses, even if consent was not previously obtained in accordance with the Personal Data Protection law. However, organisations must seek consent if they wish to use the personal data for a different purpose from what it was collected for. Individuals may also withdraw consent that was given before the law comes into effect.

Sir, for cross-border transfers of personal data, organisations will be subject to the same data protection requirements in the Bill, regardless of whether the personal data was collected in Singapore, or collected overseas and subsequently transferred into Singapore. The Bill also allows an organisation to transfer personal data to an organisation overseas as long as it ensures a comparable standard of protection for the personal data provided under the Bill, such as through contractual arrangements.

Sir, let me now move on to the Do Not Call, or DNC, registry. In our public consultations over the past few months, we have received strong support for a national DNC registry to address the growing issue of unsolicited telemarketing calls and messages.

Part IX of the Bill provides for the setting up of a DNC registry. Organisations in Singapore will be prohibited from sending specified messages to any Singapore telephone number registered with the registry. A specified message, which is defined in clause 37, refers to any message for which one of the purposes relates to marketing. As long as a specified message is addressed to a Singapore telephone number, the relevant provisions in the Bill will apply, regardless of how the message was sent. Specified messages that are sent through smartphone applications, for example, will be covered if the telephone number was used as an identifier.

Exclusions from the definition of a "specified message" are provided in the Eighth Schedule. These exclusions are intended to focus the scope of the DNC registry to telemarketing calls or messages of a commercial nature targeted at consumers. Examples of messages that are not covered by the DNC registry include business-to-business marketing messages; messages that promote charitable, religious or political causes; as well as messages that promote public agency programmes of a non-commercial nature.

Page: 832

Clause 39 provides for the setting up of one or more registers within the DNC registry. Three separate registers will be set up: one for phone calls; a second one for text-based messages, such as SMS and MMS; and a third for facsimile messages. Organisations will be charged a fee to check against the DNC

registry to filter out numbers that have been registered. This and other fees will be prescribed in Regulations by the Minister.

Part IX also spells out the obligations on organisations that send a specified message. Such organisations will be required to check the DNC registry within a prescribed duration prior to sending a specified message. The intent, Sir, is to prescribe a duration of 60 days for the first six months of the DNC registry's operations, and 30 days thereafter. This is to allow organisations more time to adapt to the DNC registry requirements at the onset. Organisations will be prohibited from sending a specified message to Singapore telephone numbers on the DNC registry, unless the owner of the telephone number had given clear and unambiguous consent to the organisation to contact him or her for marketing purposes. Organisations sending a specified message will also be required to display clear and accurate contact information of the sender within the message, and will be prohibited from concealing or withholding their calling line identity as a "Private Number" when making a voice call. Failure to comply with any of these obligations will be an offence.

Sir, I have outlined the key requirements for organisations under the Bill. To administer and enforce these requirements, Part II of the Bill provides for a Personal Data Protection Commission, or PDPC, to be set up. The PDPC will serve as Singapore's main authority on matters relating to personal data protection and will represent the Government internationally on matters relating to data protection. Given the broad scope of the Bill, the PDPC is expected to work with relevant sector regulators in exercising its functions, and take into consideration other existing laws. The PDPC will also undertake outreach and communications activities to promote awareness of personal data protection in Singapore. An Advisory Committee will be appointed to advise the PDPC, and the Infocomm Development Authority (IDA) will be appointed as the Administration Body to provide administrative support to the PDPC.

The PDPC will be empowered to enforce the data protection rules effectively. These powers, Sir, are spelt out in Part VII of the Bill. The PDPC will be able to refer organisations and individuals to mediation with their consent. It will also be able to review certain actions of organisations in relation to the data protection rules, and issue decisions or directions for compliance where necessary. Where it is satisfied that an organisation is not complying with Part III to Part VI, the PDPC may direct the organisation to remedy the non-compliance, and financial penalties not exceeding $1 million could be imposed. The Bill also allows individuals to seek compensation for damages directly suffered from a breach of the data protection rules through private rights of action.

Page: 833

While the PDPC will be provided with strong enforcement powers to deal with serious contraventions, I would like to assure Members that the exercise of enforcement powers will be measured and reasonable. Clause 31 also provides avenues for organisations or individuals to request for reconsideration of the PDPC's decisions.

Part VIII of the Bill provides for appeals against the PDPC's decisions. Appeal Committees will be established from an independent Data Protection Appeal Panel to hear appeals against the decisions of the PDPC. Further appeals against the decisions of an Appeal Committee can be made to the High Court and Court of Appeal, but only on points of law and on the amount of the financial penalty.

Sir, to allow businesses time to adjust their data management policies and procedures, we will adopt a phased approach to implementing the personal data protection law. While members of the public have asked for the DNC registry to be set up as soon as possible, we recognise that organisations will require some time to adapt to the new requirements. We will provide a transition period of 12 months before DNC registry provisions come into force, and a transition period of 18 months before the data protection rules come into force. The DNC registry is expected to be ready for registration by members of the public in early 2014. During the transition period, the PDPC will focus on education and outreach, and issue advisory guidelines to help organisations understand the requirements of the law.

Although organisations are given some time to adjust their policies and practices, they are strongly encouraged to do so as early as possible. It is important to note that the Bill adopts a principle-based and technology-neutral approach, and it does not require that organisations put in place costly systems to manage and safeguard personal data. Compliance costs will also be reduced if organisations only collect and retain personal data that is necessary for their business purposes, and delete or anonymise personal data when it is no longer necessary.

Sir, in summary, the Bill sets out rules governing the management of personal data. It also provides for a national DNC registry to allow individuals to opt out of receiving marketing calls and messages. The Bill has been crafted to strike a balance between protecting the interests of individuals, and the need to keep compliance costs manageable for organisations.

Page: 834

The enactment of the Personal Data Protection Bill will strengthen Singapore's overall competitiveness, and enhance our status as a trusted hub and choice location for global data management and processing services. It will also address growing concerns over the misuse of personal data and provide much needed protection for individuals in Singapore. Sir, I beg to move.

Question proposed.

3.30 pm

Mr Zaqy Mohamad: Mr Speaker, Sir, thank you for giving me the opportunity to speak on the Personal Data Protection Bill (PDPB). I would like to thank the Minister for his opening statement explaining the Bill.

The PDPB marks a milestone, especially in this digital age and the era of the Internet, in which data is pervasively being transmitted – knowingly or unknowingly – by means of devices, applications or identifiers in hardware. Data is collected everywhere. As consumers or users, we may not have the necessary laws to govern its use or sharing.

I am heartened by the establishment of the PDPB that puts in place safeguards which were previously across several Acts concerning statutory secrecy and disclosure provisions. Thus, the PDPB provides an overarching regime to the right of privacy or protection of personal data for Singaporeans. This moves beyond a sectoral approach which previously only covered selected industries, such as financial services and healthcare.

Sir, I plan to address this Bill in several parts, but let me begin with queries and concerns pertaining to the definitions and coverage of personal data protection. The definition of "personal data" in this Bill means data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data or other information to which the organisation has or is likely to have access. In my view, this definition is vague and only concerns information and specific use of data that can identify a person.

If we compare it to the EU Data Protection Directive of 1995 on the protection of individuals with regard to the processing of personal data and free movement of data, "personal data" here is defined as information concerning an identified or identifiable person, such as identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

My primary concern is that the definition of our PDPB is vague in which personal data protection relates only to the identification of a person or his personal details. There are potentially other aspects in which a person's personal data that is reasonable to be kept private which also include details, such as salary information, or preferences with respect to religion, even social preferences, such as where I eat, what I buy and so on. Thus, I think that the Bill should delve deeper into the definitions of and to what extent personal data should be protected.

Page: 835

Sir, if I may use a simple example of one's monthly income or salary slip, such data being disclosed may not necessarily impact one's personal safety. However, this breaches one's right to privacy and potentially impacts one's "face value" in the Asian context.

The second aspect of personal data that is not covered in this Bill is whether data analysis on our personal data and acting on the analysis subsequently breaches personal privacy. And this concerns issues of whether business intelligence or data mining on behaviour or transactions over a period of time in which I can be identified is breach of access. So, I understand activities, such as data mining in the industry, are common, and I believe that most consumers are fine with this if their identities are not identifiable and if mining is done in aggregate form or with identities masked. However, if the situation is otherwise, should the use of data for mining be also declared upon collection of such data?

Overall, I am heartened with the extent of protection provided in sections 3 and 4 on the accountability of organisations and their intermediaries and the stipulated period in which the data privacy is enforced for living individuals and those who are deceased.

I would also like to put forth a suggestion for consideration. Should special groups of the society, such as children or minors, the mentally incapacitated, be singled out for special protection? Perhaps, in such situations, we should require legal guardians to assist with the consent. And, perhaps, we should consider that data of minors should be automatically protected without the need for consent.

In the application of the Bill, in section 11, subsection 1, it states that "in meeting its responsibilities under the Act, an organisation shall consider what a reasonable person would consider in the circumstances". I believe there could be greater room for clarity in this subsection, and it would be better if the Commission sets out to define what the meaning of reasonableness is or allows the industry the latitude to self-regulate by constructing a framework or a set of guidelines.

Section 18 explains the limitation of purpose and extent, whose reference to what "a reasonable person would consider appropriate in the circumstances" does provide a loophole for companies or organisations that may have different interpretations, given the latitude given.

Sir, on the impact of this Bill on Singapore as a global hub and a connected nation, many service providers, especially in the ICT sector and digital media business, are closely monitoring the developments in this space, as this has impact in the way information flows and how the businesses have evolved in this space. I believe that many will probably be heartened to note that one key point raised during the public consultation, which has been considered in shaping the tone of this Bill considerably, is that the focus and the responsibilities of the obligations are more on business-to-consumer (B2C) transactions rather than B2B.

Page: 836

As a global economic hub, we have to ensure that the implementation of this Bill must strive to balance Singapore's economic interests and, yet, provide sufficient protection for our citizens in their right to personal data privacy. Our compliance with foreign regulatory requirements should not impede our status and investments made for Singapore to continue as an economic and ICT hub, especially as digital media, Internet and mobile commerce, as well as cloud services, become more pervasive here. At the same time, we also need to ensure that individuals are effectively protected against loopholes in which organisations may exploit by using overseas channels to bypass the jurisdiction of our laws.

The Data Protection Act in the UK (1998) covers eight principles, one of which enforces that the data can only be transferred to countries offering adequate data protection. So, should Singapore consider extending the protection of individual data protection to include this coverage in which functions, such as disaster recovery, should be limited to countries that can offer similar or as good legal protection and undertaking as the PDPB?

Here in Singapore, we have many accounts and transactions – and the numbers are still growing – of consumers here using the Internet and various business platforms used on cloud or global shared services. In many of these cases, copies of consumer data reside on overseas servers serving as back-up, disaster recovery or alternative active mirror sites.

Taking reference from the UK Data Protection Act mentioned, is our data also as adequately covered and protected by similar laws and regulations overseas? To enforce data sovereignty in Singapore only will be too tight and may impede businesses, but we should also take due care that copies of data collected must be from a list of countries that provide adequate data protection.

In cases where companies also have copies of our personal data stored overseas, I think that they should be made to disclose upfront where copies of our data will also reside. In the event that the PDPB is not able to address adequacy, let the consumer make an informed choice at the point of consent by letting them know where the disaster recovery or alternative mirror sites reside, and this will enable consumers to make informed decisions on the risks at which their data will continue to be kept private.

Sir, with respect to section 26, relating to the transfer of personal data outside of Singapore, I have some queries on how the PDPB will apply in the following situations because these are increasingly

common, especially with the pervasiveness of IT and digital media: (a) firstly, service providers or cloud services that provide multi-country disaster recovery or high-availability options; (b) with duplicate data being resident overseas, will the organisation still be responsible if the data is accessed without proper authority or under legal warrant by a foreign entity or authority? Is the organisation obliged to disclose such a situation to its customers or users if they are legally required to disclose data on their servers overseas? (c) how can the Bill be enforced on a foreign company which may collect data from subscribers in Singapore with the data being outside Singapore? What is the recourse, if such data is subsequently transferred or sold back to a company to market in Singapore?

Page: 837

Sir, I know it sounds a bit complicated, but what powers does the Commission have to direct and determine damages on the above cases should the PDPB or subsequent Act be contravened? I think that these considerations should be clarified and perhaps FAQs be made available to companies and consumers to better educate each of the parties on their rights and obligations.

Sir, pertaining to section 10, subsection 4, in which the Commission may give an undertaking to a foreign data protection body that it will comply with terms specified in a requirement made, under what circumstances will the Commission agree to a foreign body? And what are the existing obligations that Singapore has undertaken in this respect? What change does the Ministry foresee if the Bill has an impact on the operating environment of our local business context?

On the Do Not Call (DNC) registry, I welcome the establishment of the DNC and I think it is a move welcomed by many Singaporeans who have been at the receiving end of repeated calls and SMSes for unsolicited services several times a day. I have just received two this morning, by the way. I am supportive of this initiative and it is about time we enhanced our framework to work in tandem with other measures, such as the anti-spam laws, that are in place.

The only concern I have is the implications it has on small businesses and agents in that they will have to find alternative means to promote their services or products. However, I am also certain that the inventiveness of the industry will mean that marketing will evolve and, hopefully, in a way that is more palatable to the ordinary consumer.

Technology, too, will evolve, and I see areas in which we will need to monitor. Alternative channels, such as social media and digital messaging such as WhatsApp or Viber, may then become alternatives for unwanted messages because personal data identifiers, such as mobile phone numbers or e-mail addresses, can be used to access and reach users in this area. I think this is an area of development that the Ministry and Commission should consider and continuously monitor to update the laws. I understand that these are early days for the PDPB, and it will take us time to understand the implications to the various business sectors and organisations.

Page: 838

Increasingly, we receive various calls from overseas numbers for purposes of telemarketing. These calls range from the marketing of investment products to various personal services. So, how does the DNC registry affect such companies? This may prove to be a loophole in which contacts can still be sold

to foreign marketing agencies whose source of information will be hard to trace legally. How can we prevent such loopholes from being exploited as foreign agencies are not affected by the DNC registry established under this Bill?

On regulation and enforcement, Sir, our laws are only as good as the resources in which we put in place to regulate and enforce them. The administration of the PDPB provides for a Commission, Advisory Committees, Administrative Body and other offices in which powers can be delegated. To these functions, how many resources will the Ministry invest into the machinery to regulate and enforce this Bill? Will these resources be sufficient to regulate the pervasive and vast use of consumer data across businesses and the Internet? If the resources are needed to prioritise their focus, what will their priorities be in dealing with electronic and manual data?

Sir, in the event of a dispute resolution, the Bill does not provide specific timelines in which the Commission established or the mediation parties should aim to resolve the dispute, especially in minimising any inconvenience or legal costs to the ordinary citizen. I hope that the Ministry will consider putting in place timelines in which dispute resolution should be made, so as not to cause lengthy inconvenience to businesses and consumers in resolving their concerns.

Given the benefits offered by this Bill in protecting one's data privacy, may I also ask what efforts will the Ministry put in place to educate and keep members of the public informed, and educate students in schools of the individual's rights to personal data privacy?

Moving on to a different segment, Sir, the implementation of the PDPB is more likely to affect the SMEs, and potentially load on them additional costs to maintain and secure their customer databases and information. Though I note that the Minister also mentioned earlier that there are many efforts being made to minimise this, small companies and proprietors may have difficulty setting up processes, in view of section 12 which states organisations are required to implement and develop policies and practices to comply.

So, given the complexity of the nature of data protection and the various legal and regulatory implications, will the Ministry or Commission set up an industry guide as a reference point to help organisations get up to speed on what are some of the best practices in implementing data protection policies, processes and systems?

To comply with section 24, which states organisations "shall protect personal data… by making adequate security arrangements...", given this new requirement on organisations, will the Ministry define security standards to ensure a minimum baseline is required? This will put consumers, companies and auditors on the same baseline and agree on an acceptable degree of compliance. But I also hope that these requirements will not be too onerous on smaller companies. Thus, to support the implementation of this section, are there also readily available funding which companies can access and be assisted to upgrade their systems and capabilities?

Page: 839

I foresee that companies will need to train employees to ensure consistent application across the organisation. So, I would like to propose that the Ministry or the Commission consider making funding

available for companies to tap on to develop their staff to obtain such training. Of course, existing frameworks, such as those by WDA, may be considered as suitable platforms to deploy such training.

Sir, I note that the industry will be given 18 months before the execution of the Bill, or, in particular, the PDPB. After which they will be able to continue to use such data which was collected prior to the implementation of the PDPB. I would have hoped that the notice period would be shorter at six to 12 months because this presents a loophole. Much data would have already been collected under the current regime without having obtained consent in section 16. In addition, the fact that an 18-month period is granted provides more than ample time for the industry to go on an aggressive approach in collecting personal data.

In this respect, I have a suggestion, when the Act comes into force in 18 months, to make it compulsory for companies holding on to personal data to re-obtain permission in accordance with section 14, or alternatively, all such companies should at least inform or declare upon the implementation date, on the terms defined under section 20, which relates to the notification of purpose in which data is used.

If possible, the notice should also inform their members or customers of their rights to personal data privacy, as well as to have the option to withdraw, access or update their personal data.

Sir, I would like to put forth one final recommendation in my speech before I end off. Beyond the existing scope of the PDPB, we have also seen various instances in which personal data is revealed or exploited to intimidate and embarrass individuals online. There have been many cases in which personal data, such as phone numbers, e-mail addresses, even home or office addresses, are disclosed online for the purposes of intimidation or embarrassment of an individual online.

I am personally in favour of a light-touch approach and self-regulation on the Internet. However, such acts are tantamount to cyber-bullying and intimidation. The PDPB has made significant strides in pulling together relevant laws across the various Acts to provide some protection to an individual's privacy. As such, why should such instances be excluded? While there may be laws that disparately cover these situations, there is no one consolidated framework with an established machinery, such as the PDPB, to handle such issues. The issue today is that such cyber-bullying and intimidation in disclosing personal data are also not high on the priority of the Police Force, and very likely a costly affair for one to pursue through civil litigation.

Page: 840

Sir, I would also like to seek clarity from the Ministry as well. In a situation where posting of personal data is made public, once made public, is the individual's data still covered by the PDPB?

Sir, in closing, I would like to commend the Ministry in implementing the Personal Data Protection Bill. The evolving business landscape, in which consumer data is key to sales and marketing, has led to undesirable use of consumer data, a practice which this Bill aims to curb. I hope that the Ministry puts in sufficient resources and protection to ensure the effective regulation of the Bill. The fact that data is pervasively being transmitted – knowingly or unknowingly – by means or devices and applications means that we will also need to put in place an education framework to educate the common person on the street of their rights. I also hope that the law serves to better protect those who are more vulnerable, such as

children and the mentally incapacitated, from being exploited. At the same time, while we do more to protect our people, we must also be mindful of the need to balance Singapore's economic interests as an economic and information hub. Sir, I support the Bill.

3.47 pm

Mr David Ong: Mr Speaker, Sir, thank you for allowing me to speak on the Personal Data Protection Bill (PDPB). The efforts to introduce a Data Protection Bill in Singapore had been on the backburner for years. Against the proliferation of data in the use by individuals, companies and organisations, many consider the introduction of personal data protection legislation in Singapore a timely move.

This brings the Singapore privacy and data protection laws in line with the global benchmark. In addition, legislation will also render adherence and observance mandatory. To raise social awareness or recognition of privacy rights in a civil society, the Government has to take the lead in creating awareness and in setting the standards and expectations of protection.

While the PDPB is intended to be a baseline law which will operate along with the existing sector-specific laws, the PDPB is fairly ambitious in proposing to extend its provisions to organisations which may not be physically located in Singapore but are engaged in data collection, processing or disclosure of such data within Singapore.

While MICA acknowledges there may be difficulty in enforcement against organisations with no physical presence in Singapore, it was thought that extending coverage to overseas organisations would act as necessary deterrence. This is especially so in the borderless world of e-commerce and the age of Internet proliferation.

Page: 841

The exponential growth of computers, hand-held mobile devices of all shapes and sizes, ease of access and connectivity, the thriving e-commerce economy, e-health, e-Government services and, now, the widespread use of cloud computing, have revolutionised how we live, work and play. There is a heavy reliance on data by companies, Government agencies and VWOs to function and perform optimally. The push towards better and more efficient customer relationship management practices places great emphasis on soliciting, management and use of personal data.

Whilst these have indeed brought us immense social and economic benefits, they have also generated greater public awareness and concerns on how our personal data, when collected, is stored, shared, managed, disclosed or used. With regular scam emails from people we do not know or unsolicited calls and SMSes from marketing companies to sell their products or services, there is no doubt that new rules for the protection of personal data must be put in place.

Sir, I rise in support of this Bill as it is about protecting our basic human rights to privacy. This should be guarded and enshrined in our Constitution, and when an item of business content is not solicited, consumers can have the right to refuse. Whilst I understand the need for commercial entities to resort to such persistent and, at times, aggressive sales tactics as they are the cheapest and quickest form of

outreach to potential customers, but if they are unwanted and objectionable, such aggressive telemarketing techniques tread on the fine line of harassment.

Sir, I am happy that this Bill would go a long way to protect citizens from unwanted sales pitches and would also help to protect personal data from being compromised and misused. With the growing number of senior citizens amongst our population, many may unwittingly give their personal details or sign away their rights, landing themselves in commercial deals that are not beneficial to them or which they do not need.

In recent years, individuals, multinationals and local businesses that operate in Singapore have jumped on the cloud computing bandwagon. Companies and individuals where these cloud data centres are based are mostly located overseas. Internet and cloud technology allow fast and easy transportation of data across national boundaries and technologies that facilitate the increasingly complex and cheap collection, storage, use and disclosure of data.

This means that personal information about individuals in Singapore may often be processed overseas, frequently without the explicit knowledge or consent of those individuals. This raises issues, such as the security of such data, who may have access to it, and for what purposes and what rights the individual may have to object. How many of us, when given a choice to read through our rights and its comprehensive terms and conditions of use, would simply scroll down through all the legal jargons and straight down to "accept"? Many of us are guilty of failing to take responsibility for ourselves and, when mishaps happen, it is hard to plead ignorance.

Page: 842

It is noteworthy to say that, with this Act, Singapore's regulation of personal data collection, management, use and abuse would be aligned with international standards. In the United States, this Act is as important as the First Amendment. Many facets of this Bill incorporates many common elements, such as notice, consent, access and data security common in many European countries, South Korea and, more recently, the Republic of China.

Equally noteworthy is that, in Taiwan, although the Bill on Personal Data protection was incorporated in 2010, the law was only passed most recently. The long delay was, in part, because of the need for more amendments and, in part, because of the need for extensive consultations with stakeholders from the business community. In many quarters, MICA's intent in proposing this Bill is perceived to help businesses and commerce to flourish rather than to stifle and impede. As such, communication with stakeholders is both necessary and vital.

It is, therefore, helpful that the PDP Commission can embark on an extensive education and outreach effort to help organisations better understand and embrace the new law. More importantly, it should engage stakeholders to bring about an organisation accountability approach to effectively implement sound data protection procedures. The need for extensive consultation with the business community cannot be overlooked, especially given the international business climate in general and the local Singapore economy in particular.

Sir, the business community, especially our SMEs, are already facing rising business costs brought on by many factors beyond their control, such as rental and manpower costs. Thus, the Personal Data Protection Bill (PDPB) must strike a balance between consumer protection and the need to keep compliance costs manageable for businesses. From feedback gathered during the recent consultation exercise, I am glad to note that several requirements have been relaxed, for example, business-to-business marketing calls and messages are now excluded from the Do Not Call registry requirements.

In a *World Economic Forum Report* in 2011, Singapore was named second, after Sweden, as the world's most digitally connected economy. Sir, all stakeholders – the Government agencies, the commercially-inclined service providers and the general public – have done much to put us where we are today. It is a reputation worth guarding in attracting fast-evolving information technology industries to set up shop here. We had benefited and would continue to stand to benefit when the cutting-edge IT industries do not bypass us because of stifling regulations.

Page: 843

In this regard, the passing of the PDPB law must not lead to a trigger-happy litigious society in Singapore against the business society. We are not a litigious society and must zealously guard against it taking root. The California Federal Court dismissing the class civil suit against social media, Facebook, is a case in point. Although the final verdict was in favour of Facebook, the latter was unwittingly forced to commit time and financial resources to defending itself. This, Sir, surely cannot be the intent of this Bill.

In passing the PDPB, we must strive to prevent a dent in our international reputation with the global IT companies from investing here in Singapore.

Sir, if there is anything that I would call on the Government to do more in relation to this Bill is to not over protect it till it stifles business creativity and innovation, increases business costs in compliance or deters companies from investing in Singapore.

While the PDP Bill will help put in place the necessary safeguards to protect consumers' personal data, it remains important for individuals to remain vigilant and take responsibility for their own personal data. With this, Sir, I support the Bill.

3.56 pm

Ms Jessica Tan Soon Neo (East Coast): Mr Speaker, Sir, thank you for allowing me to speak on this Bill. Before I begin, I would first like to declare my interest as I work in the infocomm industry.

With most privacy frameworks around the world, "notice and consent" either have, or are perceived as having, become the dominant means of data protection. The data ecosystem is more complex than ever before. The growth of e-commerce, the explosion of social media, the evolution of cloud computing, the emerging world of "big data" and analytics, have caused industry, Government and community stakeholders to look at the need for new governance models for the collection, use and security of data.

By understanding what it means to live in a highly-connected, technology-driven and data-rich world, we can craft principles that remain effective in protecting privacy but allow us to reap the benefits that only

big data can bring. There is an increasing realisation that while still important, relying heavily on individual notice and consent is not sustainable, given the huge increases in the sheer volume and flow of information. It also places too much burden on the individuals who may not have complete information or knowledge in making the choice or, as my colleague Mr David Ong has said, whether they actually do take the effort to understand what is required before consent is given.

To that end, we need to find a balance to allow for flexibility, transparency and confidence in these governance models; flexibility to the changes in technology, transparency around its collection, and confidence that the data will be used in a way consistent with our expectations. And this has never been more important to citizens, consumers, businesses and governments as we now live in a world where people are more connected and reliant on computing technology than ever before. We are all stakeholders in this data ecosystem, and balancing the competing and complementary interests of stakeholders is about striking the balance between opportunity and responsibility.

Page: 844

This Bill is about striking that balance and setting down a baseline of a set of rules to govern the way we can continue to enjoy the benefits of this data-rich environment in a predictable, secure and trustworthy way.

Privacy and data protection are not static. The longer we wait to create these governance models, the more we become policy followers than policy leaders.

While I think this Bill is necessary, I must emphasise that it is not sufficient to achieve the balance in a way that will secure data as well as our digital future as Singapore continues to strive to position ourselves as a data and technology hub.

The Bill, however, is an important step on a continuing journey to data protection as we look at how we modernise our laws to keep up with the changes and trends in data. Singapore has stood still for too long and others have set the rules of the game. We have seen our regional neighbours advance ahead of us in this area of policy or, worse, we have seen commentators position Singapore in a less than favourable light – either out of ignorance of the strong sectoral policies we have in place already, or out of mischief to drive a commercial advantage in the competition for data.

Singapore already leads the region and the world on so many key indices, from network readiness, prioritisation of ICT, efficiencies of our legal system, and global competitiveness. But our lack of a comprehensive data protection law has been an area where it has not kept pace with global regulatory trends and technology developments.

To underscore the impact that Singapore's lack of a comprehensive data protection law has had on the potential of our cloud computing and data analytics ambitions, the recent release of the Asia Cloud Computing Association's "Cloud Readiness Index" rated Singapore as third in the region for our cloud computing potential, after Japan and Hong Kong. And the key area holding us back from being first was data protection.

Make no mistake – we are still in a global marketplace for information and there is stiff competition for data. One could say that data is the new currency of the digital economy and, like currency, data is a coward. It will flow to where it is safe, secure and valued.

Page: 845

Singapore needs to think about our competitive position in this battle for data. Are we simply going to be an efficient and innovative hub for data for the world, or can we also be the world's most trusted environment for information. After all, there is no such thing as bad data. There is only the bad collection and bad use of data that we need to consider. It is, therefore, heartening to see the momentum that the Government has seized upon to promote a modern data protection regime and how the law will both govern technology as well as promote its use, especially in the area of next generation computing services.

Singapore has been an early adopter and driver of these services, most notably cloud computing and we have been setting our ambition to be a major global data hosting and processing hub. We are already home to many of the world's leading cloud service providers, so the need for a policy framework that balances the innovation and flexibility that underpin Singapore's vibrant ICT ecosystem while promoting good governance is essential. We are now in a unique position to develop not only a data protection regime that meets the privacy needs of our citizens, but develop a regime that embraces the realities of the 21st century computing and services to promote responsible information stewardship by data controllers and processors.

To achieve this balance, Singapore needs a "next generation" data protection regime to meet the needs and demands of next generation technology. What I mean by this is that we need to go beyond just regulating the collection and use of personal information, but we need to look at the data as a whole. Data, both big and small. Indeed, I see the development of Singapore's cloud computing ecosystem and the advancement of the data protection regime as mutually inclusive.

Singapore's growth and sustainability have long been linked to our comparative advantage of being a trading port and hub for goods, people and services. Geography had been on our side to a large extent but, in this new age, the ports of the future are not bound by geography but the policy environment that promotes them as a trusted home for data. While we are already endowed with an enviable ecosystem of cloud service providers, the competition is increasingly going to be the policy frameworks that provide certainty and confidence not just for these companies but the customers that they serve around the world.

Here in our region alone, we have recently seen privacy and data protection laws advance in Korea, Malaysia, New Zealand, Australia, the Philippines and Hong Kong, with legislation actively being discussed in Thailand as well. Our regional neighbours obviously see the potential for creating trusted environments for information and, not surprisingly, have high ambitions to drive the ICT sectors, especially around the cloud. The cloud provides new opportunities, new challenges and new responsibilities, and it is incumbent on Singapore to address these head on.

Page: 846

The Personal Data Protection Bill is a big step forward and I am confident that we will achieve the right balance between efficiency and privacy, but our job does not stop here. Continual policy refinement around core issues, such as data security, technology standards and the international trade in data, are essential for Singapore to retain our reputation as a policy innovator and, more importantly, to attain the trust and confidence of citizens, customers and cloud providers and achieve our ambition to be the leading technology hub.

An important area that we also need to consider is "what are the role and responsibility of Government beyond being the regulator and custodian of information?". In other words, what should Government have access to and what should it not have access to?

For those following the cloud computing debate over the last few years, a new term has taken hold – data sovereignty. This means that many governments, including Singapore, consider certain data to be of such importance that it should not leave the country, or, in some cases, the custody of the data controller.

Data sovereignty is not to be dismissed or misrepresented — it is founded on a belief that not all data is created equal and so we need to think differently about certain data sets. We have seen this most notably in the area of financial services and healthcare, as each regulator seeks to protect the information of depositors and patients alike.

This is understandable as all of us want our bank details and health records secured and protected. But, clearly, we need to be more innovative about how we govern the protection of this information while not shutting out the innovation and good that could be derived from more flexible and modern approaches to data protection – the balance between the individual's right to privacy and the good for society.

Let me give an example to illustrate this point. In today's data-rich world, much can be revealed about a person's past and even his/her expected future. This could present both risks and benefits for the individual and society. It is important to realise the power of data analytics. Analysing data may reveal that a person has an existing medical condition that can be treated, or is at risk of developing such a condition. That data, when combined with other data, may also enable insights and medical advances. This could benefit both the person and society as a whole.

Set alongside this is the need for governments to protect citizens and enforce the laws and access to data. This can be a powerful aid in preventing the wrong use of the data and responding to them when they do happen. To illustrate the point with the same example I used earlier, it is problematic if the medical history or information that suggests the risk of a future condition is used to deny employment or insurance to an individual.

Page: 847

Let me now touch on a related point. With the increase in cloud computing, both businesses and users of cloud services are seeking to understand how and when governments can have access to user data. Governments do have need to access data for legitimate reasons of law enforcement and national interest, but greater transparency of what constitutes legitimate access is now a major issue that we cannot ignore. I believe that a whole-of-Government dialogue is needed to assess this notion of transparency in Government access to information.

For Singapore, the importance of this is only further accentuated by our ambition to be the data custodian for citizens, businesses and even governments from around the region and the world. We need to consider not just what the private sector can and cannot do with data, but the public sector as well.

As I had mentioned, we are in a competition, a competition for confidence, and we need to ensure that we have transparent rules and principles that help drive the confidence of data customers that Singapore is the trusted hub for information.

So, as Singapore stands at the frontier of this new data world, what are the principles that we need to consider to help move us beyond just keeping pace with global regulation but enabling us to stay competitive as well?

I believe that we need to start to look at some new principles that will help shape this new data protection regime. This new regime must take into account a new world that is rich with new business models, new data usage models, new forms of technology, and individual privacy sensibilities. This may prove to be either remarkably resilient over time or quite fluid.

I support this Bill as a major step towards harmonising our data protection regime to interoperate with others in the region and the world. I think that it has been developed with the traditional privacy concerns, such as the "Do Not Call" regulations, but also the flexibility in looking at the cloud computing and data hub ambitions for Singapore.

Where I would suggest we make some changes is to fast track the implementation of the provisions, especially for large businesses. I propose that we have a sunrise period of 12 months for large business and two years for small business.

I would also recommend that the Data Protection Commission that is being set up under this Act, be charged with the task of establishing an expert taskforce consisting of Government agencies and businesses to look at how we can progress a true "data protection" regime. A regime that looks at the end-to-end data considerations, including Government access, data analytics, sectoral regulatory reform with the aim of establishing Singapore as the world's most trusted home for information.

Page: 848

Singapore has a history of innovation and reliability. One of Singapore's defining characteristics is reliability and confidence. We need to harness this reputation and seize on this momentum on privacy to lead the world in developing a truly comprehensive data protection environment for citizens and businesses here in Singapore and around the world.

While businesses will incur effort and possibly cost to adhere to the data protection requirements on the care and use of personal data collected, it will provide businesses certainty and clarity on how to manage the collection and use of personal data. It will also create confidence on how businesses operating in Singapore collect and use data. Mr Speaker, I support the Bill.

Mr Speaker: I propose to take the break now. I suspend the Sitting and will take the Chair again at 4.30 pm. Order.

Sitting accordingly suspended

at 4.11 pm until 4.30 pm.

Sitting resumed at 4.30 pm

[Mr Speaker in the Chair]

PERSONAL DATA PROTECTION BILL

Debate resumed.

Ms Low Yen Ling (Chua Chu Kang): Mr Speaker, I rise in support of the Personal Data Protection Bill. It is a positive move that not only protects consumers' interests, but it will also put Singapore on par with countries with data protection laws and strengthen our position as a trusted business hub and location for global data management and processing services.

With regard to the Bill, I would like to raise two areas of concern: firstly, the impact of the Bill on SMEs, a point also raised by hon Members who spoke before me; and secondly, the protection of children's personal data.

As we all know, SMEs are the lifeblood of our economy. Today, 99% of all enterprises in Singapore are SMEs. They employ 70% of our workers, and contribute over 50% of national GDP. The often-cited challenges by SMEs include manpower, financing and cashflow. In view of this, marketing activities that are key to enhancing an SME's brand and offering can become quite a load for these enterprises.

With the introduction of the Personal Data Protection Bill, SMEs would have to put in place more resources to navigate and understand the new law. For instance, they would need a staff to double up as a Personal Data Officer, to ensure compliance of marketing activities, have their data lists filtered and observe other requirements under this Bill. Many SMEs that are already under pressure with the labour crunch and economic uncertainty may have little capacity or capability to do so.

Page: 849

As SMEs do not have the scale and deep pockets of MNCs, we must be mindful that the Personal Data Protection Bill can pose significant challenges to their marketing and customer acquisition efforts. The fear of infringing the new laws may also weigh them down.

While protecting the interests of consumers, I hope MICA and the relevant Government agencies will also lend good support to the SMEs during the sunrise period to ease them into the implementation of the Bill. For example, it will take resources and time for SMEs to make sense of all the legal requirements and to also ensure compliance. There could be new or recurrent costs involved to ensure all requirements of the Bill are met.

Besides awareness and education, I hope the Government will consider providing free training, consultancy and support for SMEs that extend beyond the sunrise period, and also explore possible tax reliefs or financing incentives for SMEs on the costs incurred as a result of complying with the Bill.

(*In Mandarin*): [*Please refer to* ***Vernacular Speech*** on Pg 939.] I rise in support of the Personal Data Protection Bill. It is a positive move that not only protects consumers' interests, but will also put Singapore on par with countries with data protection laws and strengthen our position as a business hub and location for global data management and processing services.

With regard to the Bill, I would like to discuss its impact on SMEs. SMEs are the lifeblood of our economy. Today, 99% of all enterprises in Singapore are SMEs. They employ 70% of our workers, and contribute over 50% of national GDP. The often-cited challenges by SMEs include manpower, financing and cashflow. In view of this, marketing activities that are key to enhancing an SME's brand and offering can become quite a load for these enterprises.

With the introduction of the Personal Data Protection Bill, SMEs would have to put in more resources to navigate and understand the new law. For instance, they would have to have a Personal Data Officer, ensure compliance of marketing activities, have their data lists filtered and observe other requirements under this Bill. Many SMEs that are already under pressure with the labour crunch and economic uncertainty, may have little capacity or capabilities to do this.

As SMEs do not have the scale and deep pockets of well-recognised, global brands, we must be mindful that the Personal Data Protection Bill can pose considerable challenges to their marketing and customer acquisition efforts. The fear of infringing the new laws may also weigh them down.

Page: 850

While protecting the interests of consumers, I hope MICA and the relevant Government agencies will also lend good support to the SMEs during the sunrise period to ease them into the implementation of the Bill. For example, it will take resources and time for SMEs to make sense of all the legal requirements and to also ensure compliance. There could be new or recurrent costs involved in ensuring all requirements of the Bill are met.

Besides awareness and education, I hope the Government will consider providing free training, consultancy and support for SMEs that extend beyond the sunrise period, and also explore possible tax reliefs and financing for SMEs on the costs incurred as a result of complying with the Bill.

(*In English*): The second area of concern that I wish to raise is with regard to the protection of children's personal data. The fact that the Personal Data Protection Bill does not draw any explicit distinction between data subjects who are adults and those who are children introduces an important extra dimension that must also be addressed in the Bill.

An increasing number of children are now using the Internet. They are starting at a younger age, using smart phones and electronic tablets, and spending more time online downloading and uploading information. In 2010, according to the MDA, 39% of Internet users aged 7-14 years old get online once a day. The average duration of an Internet session for 41% of Internet users aged 7-14 years is one to two hours. While the Internet can be a channel for education, it also carries a spectrum of risks to children as they share more about themselves online as they view marketing advertisements, join social networks or even transact on the Internet through apps, games and contests. In the course of such activities, they can

be targets for unsuitable or aggressive online marketing for commercial gain, cybergrooming, online scams or even identity frauds.

As the Personal Data Protection Bill comes into place, I hope we can also provide suitable guidelines as to how children's personal data, especially data for those under 13 years old, should be treated. Several governments recognise that children need additional protection in this area. I understand that in 1998, the US enacted the Children's Online Privacy Protection Act (COPPA) to protect personal data of children below 13 years of age. The European Commission is reviewing its data protection law to offer greater protection to children. Like in the US, European companies have to get parental consent for all minors under 13 years old. The Commission also wants all communication aimed at minors to be clear and in plain language. This will ensure that young people can understand the implications of entering their data, the reason it is needed, and the protection it is afforded.

Children's personal data needs extra safeguards. The fact that personal information is becoming an online commodity applies to children as well as adults. We need to place parents in control over what information is collected from their young children online. We should require that "verifiable parental consent" should be sought whenever website operators and online service providers directed to children under 13 years old wish to collect, use, or disclose personal information from children. Parents should also be able to "opt out" of any further information collection from their child.

Page: 851

We have all a responsibility to ensure that our children are protected from potential risks or abuse that could result from unwitting personal disclosure. Due to the increased complexity of today's highly connected world, it is not enough to assume that laws to protect adults' personal data would do well for children as well. We need the Personal Data Protection Bill to detail the boundaries and guidelines that can ensure the safety of our children. In view of their limited understanding of risks and consequences, children need specific protection in this area.

Furthermore, laws alone would not suffice. Education – for parents and children – on how to protect and treat their personal data is needed to bring the public to a higher level of awareness and maturity that would reinforce responsible behaviour from individuals, companies and organisations. Industries can also be encouraged to self-regulate. Parents or children-related community groups can also play a part by providing and promoting healthy personal data protection practices and online behaviour.

We all know that regulation can only set the outside perimeters. We need education to set the inward indicators for safe and healthy sharing of personal information. On this note, I support the Bill.

4.41 pm

Asst Prof Tan Kheng Boon Eugene: Mr Speaker, Sir, I rise in support of the Personal Data Protection Bill. This comprehensive legislation is belated but I believe that the regulatory regime offered by the proposed law is better late than never. It provides a good start and will stand us in good stead as we develop and grow our system of protecting the personal data of individuals.

As the examples of Google, Facebook and Twitter demonstrate, consumer information and insights are currency in today's business world. This currency, in the form of digitised information, also means that personal data is now much easier to collect, store, use and disseminate. This also means that the protection of personal data is also much harder. Matters are compounded, given the lack of understanding and appreciation for online privacy. Legislation will always be playing catch-up with developments in the online world. Nonetheless, we must always endeavour to keep up. In Asia, the jurisdictions which already have data protection laws include Hong Kong, Taiwan, South Korea, Malaysia and the Philippines.

Sir, the role of data protection laws is significant in the Singapore context given that there is no common law protection for personal privacy here. But this does not mean that privacy is not important in Singapore. Yet, the definition of privacy is elusive in that any definition is easily open to the charge of being either too broad or too narrow. The common conceptions of privacy as "the right to be left alone" and "to have control over information about ourselves" are often inadequate. Instead, for the purposes of this Bill, which is concerned with personal data protection, the concept of privacy for me has to involve information and, in particular, the access of others to undocumented personal information.

Page: 852

In reviewing the Bill, my primary considerations are whether the proposed law provides sufficient recognition of the privacy principles of consent, control and care. Sir, I appreciate that the personal data protection regime envisaged by the Bill is a light-touch one – one in which a minimum data protection standard is uniformly applied across all private organisations and individuals.

Sir, let me just go on to my first reservation. The proposed law does not apply to the public sector. The public sector, collectively, has a lot of information about individuals living on this island. Further, given the range and intensity of surveillance technology at the disposal of the Government, the need to regulate how the public sector collects, uses, shares and disseminates personal information takes on greater importance.

Although there are specific legislations that govern the protection of data by the public sector, such as the Official Secrets Act and the Statutory Bodies and Government (Protection of Secrecy) Act, I am of the view that a unified regime is ideal and one that will provide more robust protection of personal data. If a dual regime is preferred, and which I sense is the Government's preference, I hope that the new Ministry of Communications and Information will seriously consider beefing up the legislation that governs the public sector's handling of information, which is primarily geared towards the protection of the secrecy of information.

I move on to my other concern, which relates to the "deemed consent" provision in clause 15 of the Bill. In general, actual consent should be encouraged both in law and in practice. While I am not so concerned with the need for explicit consent, there should be adequate safeguards for actual consent, whether expressed or implied. Similarly, while there are safeguards in the case of "deemed consent", I would like to suggest that stronger emphasis be placed on the connection between "purpose" and "consent". To adequately protect the individual, the Bill could go further and state that the connection between purpose and consent given must be clear.

A purpose cannot be so broad as to result in an organisation having the *carte blanche* to use personal information gathered for a whole host of other incidental purposes. Otherwise, what will result will be an abuse and misuse of the personal information gathered, which is seemingly protected by the law as deemed consent of a broad nature had been obtained.

Page: 853

On the Do Not Call (DNC) registry found in Part IX of the Bill, MICA has set a 12-month deadline for the implementation of the DNC registry. Could the Minister clarify whether it would consider moving towards a shorter sunrise period from the enactment of the PPD Act? Sir, the bulk of the compliance mechanisms that need to be put in place is under the responsibility of the authorities, that is, the Privacy Commission. The private organisations merely have to consult and observe the register in accordance with the law. My concern is that the longer a sunrise period there is, the greater the likelihood that some of the more entrepreneurial organisations will escalate their data collection and use the gathered information for direct marketing activities, in anticipation of the DNC regime coming into force.

Similarly, organisations may also attempt to collect personal data and use them before the law comes into force in order to gain an advantage from the deemed consent provision under clause 15 of the Bill as well as to engage in "stockpiling" of personal data to be in alignment with the requirements of clause 17 of the Bill. Sir, regardless of the duration of the sunrise period, I also hope that the Ministry will not provide a further grace period for compliance. To do so would only defeat the purpose of the sunset period, and will reduce the impetus for compliance as soon as possible.

I would also like to propose that the regulation of spam emails be incorporated into the PPD Act's Do Not Call registry regime. Sir, the Spam Control Act of 2007 has not addressed the problem of spam emails. If anything, the Act has probably not made any difference at all! Anecdotal evidence suggests that the incidence of abuse and misuse of email addresses is now greater than it was when the Spam Control Act was passed. By bringing emails under the DNC regime, we will not make an arbitrary distinction between emails and phone calls or phone messages. It is noted that SMSes and MMSes are also covered under the Spam Control Act but they are also included under the DNC regime. A person's email addresses are also personal identifiable information. By harmonising the regulatory regime, we will provide a more comprehensive and consistent approach to unwanted correspondence or communication regardless of the mode of communication.

Sir, another area of concern relates to whether the Bill covers non-Singaporean organisations if they are collecting or handling personal information with a Singapore nexus. I seek the Minister's confirmation of this, and hope that the scope of coverage to include overseas organisations will not be symbolic. More importantly, such a move will emphasise that it is the personal data of individuals with the Singapore link rather than the location or nationality of the organisation dealing with the personal information that is the primary focus of the legislation. Otherwise, the proposed law will provide an escape clause which will certainly be used, given the portability of digitised information.

Page: 854

Sir, surprising as it may sound, Singaporeans can do with a better and nuanced understanding of privacy and the need to protect undocumented personal information. Too often, we see people disclosing their personal particulars, including their National Registration Identity Card (NRIC) numbers, birthdays, without any care or concern that such information could be misused at a time when identity thefts are becoming a lot more common. Sir, I sincerely hope that the to-be established Personal Data Protection Commission, which is provided for in Part II of the Bill, will have a strong public education mandate and that adequate funding will be provided for this role. It is only when consumers value the protection of personal data and their privacy will the proposed law be effective.

Sir, I congratulate the drafters of the Bill for their thorough work on this important new law. The Ministry of Communications, Information and the Arts must be commended for seeing through this Bill which is at least a decade in the making. This is also MICA's last Bill. Such a Bill is demanding because of the need to balance the competing and, sometimes, conflicting needs of the different stakeholders. Some of these needs include: the need and perhaps even emerging right of privacy of consumers and individuals; the benefits of enabling information technology to boost marketing reach and capabilities given our aspirations to be a hub for Asian consumer insights; as well as the economic benefits that flow from allowing, within reasonable limits, organisations to collect and use personal data for their business endeavours. I think the Bill does strike an appropriate balance.

Sir, there is still a lot to be done for the protection of personal information. As many other Members have raised, should vulnerable groups, like children and the disabled, be provided with enhanced level of privacy protection? What about the prohibition of the trade and sale of personal information? In any case, the developments in this area mean that our laws will need to be constantly updated to keep pace with the changes and the ingenuity of people seeking to mine personal information for whatever advantage, pecuniary or otherwise. This underscores the centrality of personal data in today's world and its status as an asset. Sir, I warmly welcome this Bill and look forward to its robust implementation.

4.51 pm

Ms Tan Su Shan: Mr Speaker, Sir, thank you for the opportunity to speak on the proposed Personal Data Protection Bill.

In this Information Age, copious data is generated on our every movement, action or even preference, particularly in a digital society such as Singapore's, where one's location can be constantly tracked via phones, EZ-Link cards, CashCards, and so on. Abuse of data privacy could give rise to serious personal privacy violations which in turn could portend societal harm. Mr Speaker, Sir, this is a vital Bill, and one that is overdue.

Page: 855

That said, while it is indisputable that personal data privacy must be protected, the equally important questions of reach and enforcement may not have been fully considered in the proposed Bill. These are important areas which can be crafted in a more precise manner or it may leave too much open to interpretation. Allow me to offer three such examples from the Bill where, perhaps, more specific details can be offered.

Number one – clause 4. This clause relates to the application of the Bill. Yet, it says it will not impose any obligation on any individual, any employee or any public agency, acting in the course of employment. If this exemption is necessary, then, surely, they should only apply if these employees or public servants have accessed the data, whilst in the proper course of duty. This means they should exercise reasonable care in the handling of such data. A blanket exemption should not give these employees immunity from handling such data responsibly.

Secondly, clause 5 on the appointment of a Commission. Regarding this Commission, what criteria will be used in their shortlisting and selection? How do we ensure that they are independent and, related to that, what will be its tenure and maximum renewal? How shall we assess if it has discharged its duties in the best interests of Singapore and, given the importance of the role, will such information be publicly available in a timely and convenient manner?

Thirdly, clause 11 on the compliance of the Act. Clause 11 states that in meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances. This, however, leaves wide open the question of what might be deemed "appropriate", which significantly impacts the protection the Act might afford. Perhaps, there could be more clarity then on what may be deemed "inappropriate".

Clause 11 also allows for the delegation of authority. I quote, "an individual designated such may delegate to another individual the responsibility conferred". The question here is: is such second-degree delegation necessary? Does it aid or does it hinder accountability?

Lastly, as fellow Members have pointed out, let us just talk about the issue of NRIC numbers. It has become commonplace for NRICs to be used as a required field in forms, whether official or not. While contact information is necessary for tele-marketeers, is giving our NRICs always necessary? Have the authorities considered the risk of ID theft? Given the sensitivity surrounding such information, can the Minister consider ringfencing this data so that it absolutely cannot be shared, and should only be collected, if necessary, for administrative purposes – with the onus on the collecting agent to ensure it can meet the burden of proof.

Page: 856

I end with a suggestion for the Minister to consider improving the transparency of how the Government uses all the information it collects. After all, we are living in an era where we all carry chips with us. With security cameras in public areas, EZ-Link cards, cell phones, and so on, our whereabouts can be tracked all the time.

And if the Government is, indeed, the custodian of such data, then can the Minister address what is done with all this information, and how long is it stored? Who has access to this information, and under what circumstances is this information shared? Assuming this information is only shared in the course of public justice or security, then who determines what rationales are permissible, and what are the safeguards to ensure that such trust and privacy are not violated?

Mr Speaker, I am afraid I have raised more questions than answers. I hope the above questions and suggestions help our promulgation of a Personal Data Protection Act that is world-class, and delivers

solidly the personal data protection that our people fully deserve.

4.56 pm

Mr Chen Show Mao (Aljunied): Mr Speaker, Sir, the Bill before us has been a long time in coming. Back in 1990, the Law Reform Committee of the Singapore Academy of Law published the working paper entitled "Data Protection in Singapore: A Case for Legislation". And, today, we have a Bill that proposes a baseline data protection framework to regulate the way organisations in Singapore collect, use and disclose our personal data.

This Bill relates to the protection of personal data. It is developed based on principles derived from the OECD guidelines on the protection of privacy. These principles include, among others, accountability and openness. The data protection provisions being introduced will serve as a "baseline" law. That is, we legislate here for a minimum standard to be applied across the board. There are then expressed provisions within the Bill for various exceptions, particularly that any other written laws shall prevail over these data protection laws should there be any conflicting positions. So, this is, in part, how, as the Government stated, "a general baseline law will apply concurrently with existing sectoral regulations", such as for banking and telecommunications.

The Bill allows for various other exemptions. For example, an organisation may collect, use or disclose personal data without having to comply with these data protection laws if doing so is "necessary in the national interests". Or if the collection, use or disclosure of personal data is "necessary to respond to an emergency that threatens the life or safety of that individual or another individual". Or if those personal data is "publicly available". Or if the use or disclosure of personal data is "necessary for any investigation or proceedings". No need to comply with the data protection requirements in this Bill in these cases.

Page: 857

So, these exemptions would have been helpful in providing some flexibility to organisations, such as Government agencies, when dealing with the interests of the public in specific cases. But, unfortunately, this Bill will not apply to public agencies. It expressly carves out the application of personal data protection laws to public agencies that collect, use or disclose our personal data. These include Government Ministries, tribunals and, upon notification by the Ministers, statutory boards like the PA and the HDB. As an extension, the personal data protection laws will also not apply to private organisations when they act on behalf of a public agency. So, Sir, this is an area in which the Bill is lacking.

Like private organisations, public agencies that collect, use and disclose personal data of individuals should be required by law to comply with the minimum levels of data protection in this Bill. A reason given by the Government was that public agencies do not need to be included as they are already governed by their own set of rules and that these rules provide similar levels of protection.

Sir, to the extent that the Government's data protection rules are contained in our written laws, such as the Official Secrets Act, they would have continued to apply even if we were to extend the coverage of this Bill to our public agencies. This is because, as mentioned earlier, this Bill is set up as a baseline law that is not intended to affect rights and obligations under existing laws.

Sir, to the extent that the Government's data protection rules are not contained in written laws, then I do not know what they are. I do not know what these laws are, or, rather, what these rules are, because they are not made known to the public.

What I know is that, if these rules are not laws then they are not subjected to parliamentary scrutiny and oversight, and we do not know when or how they get created, amended or terminated. The people who are directly affected by these rules do not know what they are, much less have the chance to have their views on them heard.

To give an example, while individuals will be able to complain to the new Data Protection Commission relating to suspected violations of the data protection laws in this Bill, it is not clear if and how, under current Government data protection rules, individuals have similar rights for complaint against public agencies relating to the wrongful collection, use or disclosure of personal information.

The Government has also said that some of its rules are "more stringent in other areas." Well, that is good. That could continue to be the case, even if this Bill should apply to public agencies. And there is nothing in these laws stopping organisations, public and private, from having internal rules that afford even better protection for personal data, should those be deemed necessary or desirable.

Page: 858

The concept of accuracy, and individual access and correction are key provisions contained in this Bill. This means that individuals have the right to request access to their personal data held by an organisation and also to request that they be provided with information about ways in which their personal data have been used, and to be provided with the names of the parties to whom the data have been disclosed. Individuals also have a right to request that organisations correct any errors or omissions in their personal data.

So, it is just as important, if not more important, that these concepts of accuracy and access rights should also apply to public agencies that collect, use or disclose personal data. Public agencies, during the course of their duties, use personal data to make decisions, such as whether to grant somebody Workfare Income Supplement payments, which have a direct impact on the lives of individuals. Therefore, it is important that individuals should be able to access their personal data on the basis of which the Government makes decisions on and to ask for such data to be corrected if they are inaccurate.

Another reason that we have been given for why the public sector needs to be excluded is that public agencies often have to share information with one another or to deal with national emergencies. And, indeed, we do already have laws that allow public entities to share data. Examples include the Income Tax Act, the Medical Registration Regulations, the Immigration Act. As mentioned earlier, these will continue to apply as they are contained in existing written laws. Also, as mentioned earlier, we have broadly worded exemptions contained in this Bill relating to national interests and to emergencies, which may well be helpful through our public agencies looking to share information in a national emergency.

By ensuring that the public sector also falls within the remit of our personal data framework, individuals can be certain that there is at least a minimum baseline that applies the way the public sector treats their personal data, and they can take comfort from how the processes and the rules would be clear for them.

I also note that of the jurisdictions in the world that have a personal data protection framework, only very few do not have personal data protection laws that are applicable to the public agencies. Therefore, making this data protection framework applicable to public sector organisations, to our public agencies, would mean that Singapore will be truly in line with international standards, which is one of the three principles that the Bill is based on.

Sir, the protection of personal data is welcomed not only because of its expected economic benefits. It is welcomed also because it acknowledges an important principle that our personal data belongs to us, as persons, much like our cash or phones or wallets and other forms of property. And this property needs to be safeguarded and protected by law against misuse, including by the Government. We must remind ourselves that the proper function of a government and its associated bodies, first and foremost, is to provide essential services to the people. The Government collects our personal data in order to be able to provide us with various services, such as administering our CPF accounts for our retirement needs, or our Medisave accounts for our medical expenses. However, this information belongs to us, and our Government agencies must handle our personal data with care. Above all, they should be accountable to the people and to Parliament about the way in which they use and safeguard our data while they carry out various services for us.

Page: 859

Mr Lui Tuck Yew, as MICA Minister in 2011, said, "What we are doing, first and foremost, is to govern the proper processing of personal information, such as the collection, the use, the disclosure and the transfer of this data and to make sure that this is properly regulated." Sir, there is no reason why that should not apply to our public agencies.

5.08 pm

Mr Desmond Lee (Jurong): Mr Speaker, Sir, identity-related crimes cost the British public some £2.7 billion in 2010. In the US, a 2007 survey report estimated that some eight million people fell victim to identity fraud, losing close to US$50 billion.

The growth in identity-related crimes is closely associated with the rampant global black market in personal information. Just this month, for example, it was reported in the news that Japanese police had arrested two research firms' employees on charges of illegally obtaining private information from a broad network of information suppliers. These suppliers included mobile phone salesmen, staff at job placement centres, as well as police officers.

In the last four years, the pair allegedly made more than ¥850 million, or more than S$13 million. Quite ironically, they claimed that their business had turned profitable after Japanese data protection law kicked in and created a greater demand in the black market.

The current black market price list for sensitive personal and financial information was recently put up on the website of the US Office of the National Counter-Intelligence Executive (NCIX) to generate greater public awareness about data security. Apparently, it costs just US$3 to buy an American citizen's social security number, which the NCIX notes, wryly, is cheaper than a McDonalds' Happy Meal.

In a 2008 Australian government report, the growing incidence of identity-related crime in many countries was attributed to a number of factors, including globalisation, the rise in high-speed information flows, increase in the use of remote communications, greater sophistication in forgery techniques, as well as "the widespread collection and dissemination of data about individuals by private sector and other organisations, which provide opportunities for easier access to personal information".

Page: 860

Sir, I think these factors apply equally in Singapore. The introduction of an overarching data protection legislation is, therefore, critical, if a little overdue. It will complement existing laws, such as the Computer Misuse Act, the Penal Code and the Electronic Transactions Act, as well as other sectoral data legislation, to help increase protection around sensitive personal information.

But merely having such a legal framework is insufficient. Organisations and businesses must genuinely treat personal information of their customers and their employees with care and respect, and embrace data protection as an intrinsic and valuable part of business culture. Otherwise, if this is seen as just yet another cost to manage, then there will only be lip-service compliance or, worse, creative compliance.

The Personal Data Protection Commission should, therefore, focus its efforts along two main lines: (1) working with business and other federations to educate, help and incentivise organisations and businesses to adopt effective data protection protocols; and (2) devoting sufficient resources to enforce the rules firmly and fairly against organisations that flout basic data protection standards.

At the same time, personal data protection is not just something for organisations and businesses to do. It should really begin with you and me. We have a role to play in safeguarding our own personal information. Some of us may just be a tad too naive and trusting: dutifully filling in every request for sensitive information that is sought, for instance, on a lucky draw coupon, without thinking twice about potential consequences if the information is abused.

A healthy scepticism about the necessity of giving away valuable pieces of our own information to strangers who ask for it, is something that ought to be inculcated at home and in schools, and reinforced in the community. I, therefore, hope the Commission will consider working with schools, as well as community and grassroots organisations, to bring this message across to all Singaporeans, especially our more vulnerable groups, such as the young and our elderly, and to educate them about the data protection framework that we are putting in place to protect. They should understand what potential harm may be caused if they give away information, such as their NRIC numbers, their birthdays and other types of information.

Sir, let me now comment specifically on the Bill. First, I find it striking that there does not appear to be any substantive provision in the Bill that criminalises or otherwise penalises the deliberate and unauthorised disclosure of personal data, for example, by employees, officers or agents, or for procuring such unauthorised disclosures.

Page: 861

Contrast this with section 55 of the UK Data Protection Act 1998, which makes it a crime to obtain personal data from data controller without consent and to sell or offer to sell such information. While such acts may, under certain circumstances, be sanctioned as breaches under Part IV of the Bill or amount to offences in our Penal Code or the Computer Misuse Act, I would have preferred that the Personal Data Protection Act explicitly outlaw black market trading and trafficking in sensitive personal information.

In the Japanese case I just mentioned earlier, the companies concerned may well have collected and stored personal data appropriately and instituted measures to safeguard them but, unfortunately, rogue employees allegedly sold the information to the two individuals operating the black market.

Such an offence should be explicit and be backed by stiff penalties in the form of fines and jail terms, and be listed as a predicate offence under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) so that illicit profits can be confiscated.

Second, again on enforcement, I wonder if the powers contained in Schedule 9 of the Act are sufficient for the Commission and their officers to conduct full and thorough investigations into alleged non-compliance with our data protection laws.

There are powers in the Schedule to require organisations to provide documents and information, and enact powers of entry, search and seizure, but I note there are no expressed powers to compel attendance of persons and the recording of statements from individuals which are essential in discerning the exact nature of the breach.

For comparison, the Minister may refer to section 12(3) of the Private Hospitals and Medical Clinics Act and section 55A of the Infectious Diseases Act, both of which contain such powers to record statements.

Third, I notice that there is no obligation on organisations to promptly notify individuals or the Commission about significant data privacy breaches that may have occurred, for instance, when credit card numbers or sensitive medical records are stolen, lost or leaked. This was a suggestion made by a number of people during the public consultation phase, including notably by Professor Simon Chesterman, Dean of NUS Law School.

I think this is an important provision to consider having as it will allow the individuals affected to take timely and necessary precautions and remedial actions.

Four, while data protection is important, I think the provisions in Part VIII of the Bill, including the provision for reconsideration by the Commission and provisions on appeal, are a bit of an overkill. Let me describe the current process.

Page: 862

First, when an individual makes a complaint and the Commission investigates and makes a direction, the Commission may be asked under clause 31 to reconsider its decision or direction. An appeal may then be made to the Appeal Panel under clause 33, which will constitute an Appeal Committee to hear the appeal. The Appeal Committee's decision is not final. It is, in turn, appealable, under various circumstances, two more times – once to the High Court and, yet another time, to the Court of Appeal.

Sir, I think there may be too many layers of appeal. This creates uncertainty and delay in resolving disputes. The cost of such litigation may well be beyond the common man and put him at a disadvantage against corporations with time and deep pockets on their side. It is also disproportionate when compared to the number of levels of appeal available for other criminal and civil disputes that are heard before our courts.

Sir, I propose that appeals stop at the High Court, which is already a very high level. Go to the Court of Appeal for very important questions of law of public interest, and only then with leave of court.

Five, I would like to ask the Minister what effect the Bill is intended to have on the common law of confidentiality. Is the Bill intended to codify or to modify the common law?

For instance, Sir, let us look at clause 17(3) read with paragraph 1(m) of the Fourth Schedule. It states that an organisation, in this case a licensed healthcare institution, may disclose personal data about a current or former patient to a public body for the purposes of policy formulation or review.

Under the common law, the physician treating the patient, as well as the healthcare institution, is under an obligation to respect the confidentiality of the patient's information. Over and above that, the doctor has to comply with the Singapore Medical Council's (SMC) Ethical Code and Ethical Guidelines which also has stipulations about medical confidentiality. Such disclosure would therefore have required expressed consent or a legal requisition under the Statistics Act, under existing law.

Sir, to prevent confusion amongst professionals such as doctors and lawyers and other individuals who may be obliged to respect confidences under the common law and ethical codes, it may be helpful for the Commission to clarify and provide guidance on the interaction between the Data Protection law on the one hand, and common law and ethical obligations on the other.

Six, one of the questions posed by MICA during the public consultation was whether the Bill should only cover organisations in Singapore, or whether coverage should also extend to personal data collection and processing activities in Singapore regardless of where the organisation is located. MICA posed this question because it was concerned about the practical difficulties of investigating complaints and enforcing the law against organisations with no presence in Singapore.

Page: 863

I read through a sampling of the public responses on MICA's website and the majority of respondents, both corporations and individuals alike, felt that the law ought to apply regardless of where the organisations were located, so long as they were engaged in collecting, storing and using data here in Singapore.

I fully agree. This provides a level playing field, ensures even-handed protection of personal information, and is in line with the wider jurisdictional reach of legislation such as the Computer Misuse Act. In any event, the Commission can and should work with foreign data protection regulators and law enforcement agencies given how easily data flows across borders.

This seems to be the position taken in the Bill, as the term "organisation" is defined in clause 2(1) as including entities whether or not formed or recognised under Singapore law or resident or having an office

or place of business in Singapore. Could I seek Minister's clarification that this is indeed the position taken in the Bill?

And, finally, Sir, on the Do Not Call (DNC) registry, which I am looking forward to, I notice there is a defence in clause 43(3) of the Bill for those who send marketing messages without checking the registry. This defence applies when the person sending the message can prove that the subscriber or user of the number had given consent to the sending of the message.

Sir, I feel this defence may muddy and undermine the efficacy of the DNC registry. For instance, there could be a dispute as to whether the consent had come first, or whether the registration had come first, or whether there was even written consent in the first place. In my view, it would be much cleaner to just state that if a number is placed by the member of the public on the registry, then no calls ought to be made to disturb his peace and quiet, full-stop. Clause 43(3), Sir, therefore, ought to be deleted. Mr Speaker, Sir, with that, I support the Bill.

5.22 pm

Assoc Prof Fatimah Lateef (Marine Parade): Sir, it was not too long ago when I received a phone call from one of the staff of a local bank who told me, "Madam, are you currently in country X about to purchase a diamond and ruby Cleopatra necklace which costs about S$400,000?" Well, of course, I was not in country X. And, of course, he assisted in protecting my bank services, terminating the card and saving my money.

Sir, this Bill is a first in Singapore but represents a landmark one. It is timely, necessary and will only get more important with all the technology, telecommunications and IT development we are facing this century. It will assist with responsible use of personal data as well as guard customers' private details accordingly. Sir, I have no doubt our Government agencies will lead the way in doing this.

Page: 864

Now, a few clarifications. For section 4 on the applications of the Act, when it comes to foreign companies, private companies and MNCs, registered and operating here in Singapore, what happens when these foreign companies use the Singapore data and details overseas? How do we ensure the data is accorded the same level of protection when transferred overseas? Some of these companies may not have the appropriate contractual agreement as mentioned by the Minister. So, how do we have this added protection that we really need and also what about the data that has been collected prior to this Bill?

Pertaining to the global flow of information and cross border data abuse, what will happen in such cases? For example, in the numerous transactions done by Singaporeans such as booking of hotels overseas, signing up for conferences, filling up application forms and many other similar examples, how can Singapore citizens who have been affected seek redress?

Pertaining to the use of data on social networking sites such as Facebook, blogs, and so on, does this constitute "publishing" the information and data under this current Act?

Sir, the Bill also has no specific reference to children under the age of 12 years. In the United States, for example, there is a Child Online Privacy Protection Act (COPPA) enforced in the year 2000 for children under the age of 13 years. Should we, in Singapore, have some form of verifiable parental consent for the collection of personal data of children or could children or minors be given automatic protection in some ways?

On another issue, Sir. Electronic medical records are certainly an "in" thing in Singapore in the way we are going forward with one patient, one medical record. Patients seeking medical assistance from clinics and institutions are in their most vulnerable moments and will certainly automatically divulge information and data to those concerned. Now, healthcare data is, indeed, very intimate, very personal, very private and extremely confidential. We certainly need an utmost level of protection for these data. Can I ask the Minister whether there will be added layers or levels of protection for certain data which are managed in the healthcare sector besides those that are already available in the institutions?

Many organisations these days are requesting for data which include NRIC numbers and, for example, the People's Association, too, now has upscaled its criteria for awards and requires our grassroots leaders to collect information, including NRIC number, for entry into a system to gauge the outreach into the community. What is the Ministry's take on this, please?

Page: 865

Also, data of condominium owners which is often publicised on public notice boards by the MCST are easily accessible and available to people such as property agents and housing agents who can use this information sometimes even with very personalised brochures to residents living there. Will this Bill be able to look at some alignment with the Land Strata Titles Act?

Sir, assumed consent is quite different from formally taking informed consent. Clear delineation is crucial to handle short-, medium-, as well as long-term repercussions which may surface. At the same time, we need to have a balanced and equilibrium approach to this issue.

I commend MICA on putting forth this maiden Bill. There will certainly be some teething problems, but certainly we must move forward and continue to fine-tune as we progress into the future. It is not going to be smooth sailing. Certainly, data and information transactions have become a key part of our lives today and, indeed, we all must handle this with utmost integrity and ethics. Sir, with that, I support the Bill.

5.28 pm

Mr Teo Siong Seng (Nominated Member): Mr Speaker, good afternoon. I would like to first declare that I am the President of the Singapore Chinese Chamber of Commerce & Industry, representing 4,000 corporate members and 145 trade associations from a great diversity of trades, industries and service providers.

Today, I would like to speak about the Bill which is up for a Second Reading. There are two main sections in the Bill: the Personal Data Protection Act and the Do Not Call registry.

On the Personal Data Protection Act, firstly, the move to establish this is an important step to further enhance our position to build a trusted business and information technology hub. The Act would help to prevent companies from using personal data of individuals irresponsibly and without their knowledge or express consent. We understand that such a personal data privacy law has been enacted in the EU, Japan, Hong Kong, Malaysia and the Philippines.

On the other hand, the implications of this Act can be far-reaching. It would cover all industries because personal data also includes human resource records. Therefore, the Act would affect industries including, but not limited to, insurance, outsourced telephone marketing services providers, data storage service providers, property, banks, financial institutions, health, medical, security, and so on. All industries which need to refer to or make use of personal data to promote or expand their business would feel the impact. By the same token, industries which need to refer to HR records of individuals for recruitment purposes may face certain practical difficulties.

Page: 866

On Care of Personal Data, under Part VI, section 24, "An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks."

Companies would need to look for suitable security solutions to protect their data. Because the Act does not provide clear perimeters for what is meant by "reasonable security arrangements", it would be open to certain ambiguities. Multinational companies or large companies would most likely go for the best solution and sometimes costly solutions to protect their database, because they have the resources and can afford to do so, or may have done so already.

On the other hand, the incremental cost of compliance to the new Act, in terms of safeguarding the data and allocating the manpower to get it done, will be so much higher for an SME to manage. Under Part III, section 11(3), the Act states that "An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act." Under section 12(a), the Act also specifies that an organisation shall "develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Act."

Firstly, the cost of purchasing a highly secure data management system may be beyond their means. Secondly, with only a skeleton team managing administration and operations, it may not possible for SMEs to devote another headcount to handle compliance matters. Thirdly, in addition to the cost of buying the security solutions and the cost of compliance, SMEs have to worry about the consultancy and development costs to put in appropriate policies.

The compliance is not straightforward by any means. Organisations may also allow individuals from outside to access their data and accede to the request for individuals to correct their personal data. The organisations have to manage their database in such a way that they could provide information on which parties the individual's personal data had been disclosed to within the past year and be ready to communicate any corrections to them. At the same time, organisations have to provide information on the ways the data has been and may have been made use of. These are some of the onerous compliance

procedures that are not only time-consuming but also put undue obstacles in the way of an SME's operations. Over and above their daily operational matters, SMEs would now have to cope with compliance procedures to manage their database.

There is a proposed sunrise period of 18 months before the law on personal data protection will come into effect. The business community feels that 18 months is far too short for all companies and organisations to be ready. IT solutions companies may not have sufficient resources to customise and install suitable security measures for all Singapore companies within 18 months.

I would like to appeal on behalf of the business community for a longer sunrise period, especially for the SMEs. We could stagger the sunrise period, keeping the originally proposed 18 months for MNCs or large companies and selected businesses like headhunters, insurance brokers and marketing companies. Our proposal is to let smaller companies with less than $10 million in annual revenue use the 18 months to draft appropriate compliance policies, while the sunrise period can be extended by another 12 months. This would give them more breathing space for proper implementation. The SMEs and IT solutions vendors could also learn from the bigger companies on the implementation procedures and bring them up to speed.

Page: 867

At the same time, the financial penalty "not exceeding $1 million" for non-compliance is extremely heavy. This also gives rise to a certain ambiguity. There is this ceiling of $1 million for the heaviest penalty but no indication of what the lower range is likely to be. SMEs and MNCs are operating on different scales altogether and we hope the financial penalty would not be applied unilaterally irrespective of the size and scale of the company.

Next, on the Do Not Call (DNC) registry which I also welcome personally. While we are aware that the Do Not Call registry protects individuals against unsolicited calls like spa packages, bank loans, facials, and other marketing messages, we are concerned that this would become another additional cost for businesses. There are three separate registers: phone calls, SMS/MMS, and fax. Organisations would have to subscribe to the Do Not Call registry for each tier. A company wishing to send marketing messages would have to subscribe with each separate register – for phone calls, SMS/MMS and fax. No details have been given on the subscription fee or how it would be administered. We seek more clarity on this, especially bearing in mind that business cost is getting higher and higher in Singapore.

We also foresee that the cumbersome nature of having organisations make renewed checks with the DNC registry once in every "prescribed duration". Again, this compounds to the costs of doing business. In particular, the SMEs will be thrust into a difficult position of having to comply with such procedures, on top of their usual heavy workload and cost.

The penalties per breach for the DNC, capped at $10,000, may be acceptable for the big companies. But this is considered a very large amount for SMEs. We would appeal to the Personal Data Protection Commission to review this amount in all fairness to the SMEs. We also wonder if the penalty is commensurate to the offence.

While the business community understands the rationale for having a Personal Data Protection Act and the setting up of a DNC registry, it does introduce many areas of concern, in terms of overall compliance, additional costs, heavy penalties and an overarching impact on the SMEs.

We would also like to understand why the Personal Data Protection Act has now removed the Data Protection Fund which was originally intended to provide financing or incentives, including grants and scholarships, to any public authority, enterprise, education institution, or other person undertaking or facilitating any programme to promote data protection awareness or implementation and running costs of the Commission. This Fund could have been used to alleviate some of the operational and compliance costs for the SMEs. I hope that these relevant concerns will be heeded. In closing, I support the Bill.

Page: 868

5.37 pm

Mr Ang Wei Neng (Jurong): Mr Speaker, Sir, I rise in support of the Bill. I will commence in Mandarin.

(*In Mandarin*)*:* [*Please refer to* ***Vernacular Speech*** on Pg 940.] The Personal Data Protection Bill comes at the right time. In today's Internet world, personal data can easily be stolen or misused by unscrupulous people. Singapore is unlike the EU, US, Canada, Australia or New Zealand, where comprehensive consumer data protection laws are in force. Quite often, we receive uninvited calls, SMSes or emails trying to sell various products and services. The most annoying is a call like this: "xxx, you are our bank's valued customer; I call to recommend our newest insurance products/loans." Banks possess our personal data and they vow to keep the information confidential. However, the banks pass our mobile phone numbers to their agents and partners who in turn promote insurance products we usually do not need. I believe many Members of the House might have similar experiences!

Therefore, the Do Not Call registry will be welcomed by many people. Clause 40 of the Bill stipulates that customer can apply and register his telephone number with the registry or to have the number removed from the registry in the form and manner determined by the Personal Data Protection Commission (PDPC). I hope that PDPC can simplify the application process. It would be ideal if we could allow consumers to apply through phone, using any of the four official languages, after simple authentication of identity. If the consumer subsequently decides to pull out, I suggest the application to remove his number from the registry has to be made in writing. We do not want unscrupulous people or organisations to take advantage of illiterate Singaporeans by persuading them to withdraw from the registry, or to withdraw on their behalf.

While we protect the consumers, we also need to provide some safeguards to SMEs, so as to curb the cost of compliance. Section 3 of clause 11 mandates that an organisation must designate an individual to ensure that the organisation complies with the Personal Data Protection Act (PDPA). For example, EU Data Protection Law stipulates that organisations with over 250 staff must employ one dedicated data protection officer. However, considering SMEs' limited resources, perhaps the Commission could consider establishing a consulting service to help SMEs to comply with the requirements of PDPA at affordable fees.

Page: 869

In recent years, the technology of digital camera and video camera has improved drastically while the costs remain affordable. Consequently, more and more companies install surveillance camera on their premises to deter crime, help solve customer disputes, etc. At this point of time, I would like to declare my interest as I work in a Public Transport Organisation (PTO). We operate trains and buses that are installed with CCTV. I understand that video images recorded by surveillance cameras could be considered as personal data and come under the ambit of the Bill. I agree. Under clause 24 of the Bill, an organisation shall protect the video images which include taking steps to prevent the images from circulating on websites, such as YouTube, without prior authorisation.

(*In English*): In the last part of my Mandarin speech, I said I am glad that video images recorded by the surveillance cameras are considered as personal data as the video images can identify an individual. I understand that the PDPC will be issuing guidelines on the application of the PDPA to the use of CCTV and surveillance cameras.

I suggest that the PDPC could take reference from the data protection legislation in the EU when drafting the guidelines. For example, the guidelines can require organisations to inform their customers or members of the public about the presence of CCTV on their premises. They should also make provision to protect the CCTV video recordings in their possession or under their control by having reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal and similar risks, as stated in clause 24 of the Bill.

At the same time, it is advisable that an organisation should only release the CCTV recordings to public agencies, as defined in clause 2 of the Bill, and not to individuals, especially with regard to law and order issues such as allegation of thefts or assaults. This is because CCTV recordings, most of the time, may reveal images of other individuals which could be construed as personal data about these individuals and fall under the provision of clause 21, section (3)(c).

On the issue of transfer of personal data outside Singapore, I am disappointed that the Bill does not sufficiently protect the consumer. Clause 26, section 1, states that an organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the Bill. However, putting the onus on the organisations that collect the data in Singapore to ensure that a comparable standard of protection is accorded to the personal data transferred overseas is, in my view, asking a fox to mind the chicken coop. Organisations and businesses will be inclined to take the routes most beneficial to their own entities and bottom line. To this end, I would urge the Minister to consider allowing personal data to be transferred to a third country only if that country provides an adequate level of protection, that is, at the country level rather than at the firm level.

Page: 870

Lastly, I would like to ask the Minister whether the personal data and information collected during the house visits and walkabouts by fellow Members of the House, including myself, would fall under the purview of this Bill. I am of the opinion that the same standards and regulations should apply but I hope the Minister could elaborate.

5.44 pm

Mr Patrick Tay Teck Guan (Nee Soon): Mr Speaker, Sir, I rise in support of this Bill which will help to safeguard individuals' personal data against misuse, ensuring the interests of our consumers and putting us on par with advanced economies in terms of data protection laws. It is also good to note that most organisations and companies will be subject to this baseline law in ensuring compliance from the way customers' data is collected to establishing the accuracy of its data and defining its retention and usage within and outside of Singapore.

A difficult challenge that this new Bill has to address is to balance between satisfying the consumers' need for information and to prevent the infringement of their private space with spam e-mails, unsolicited SMSes and calls. It seems to me that the measure before and after Personal Data Protection (PDP) may sway to one or the other end for the caller and intended recipient. Before the PDP is proposed, the intended recipient will usually be hounded by sales or telemarketing calls often regarding banking, insurance or property marketing. After the PDP and the Do Not Call (DNC) registry option are implemented, will the majority of people list themselves on the register? It may be easier and faster to reject the call than to list the organisation or person under the register. If the calls are persistent, would enhancing harassment laws not be a more effective deterrent? While the DNC register is a good initiative, I ask whether it will entirely solve the problem of nuisance calls or it will just be a back-up option that is not fully utilised. The fact remains that people do not even know how their personal data is compromised in the business-to-business transactions of customer database.

I would like to provide the classic case of cold calls from property agents to illustrate how seeking a balance for consumers can be tricky. The context of the intended recipient will blur what should be considered as a breach of personal data or what can be considered to be a normal market transaction. For a property owner who is looking to sell or rent his or her property, he or she would welcome as many calls as possible by property agents, solicited or unsolicited, to get the best price or quotation. He or she may even encourage personal data to be passed on from one property firm to the other. Having sold or rented the property, would the individual therefore regard further calls by interested agents to be with or without "consent"? It may be difficult to apply the DNC regime in such a broad stroke for the customer or consumer. From another perspective, the new privacy laws will also add on to the burden of businesses having to manage their clients' ever evolving needs.

Page: 871

Under the new Bill, it is stated that organisations shall not attempt to obtain consent for collection or using personal data by deploying deceptive or misleading practices. We know how easy it is to bypass this by dangling a lucky draw to obtain personal details from the customer. By sharing my personal particulars for the lucky draw, I may have only consented to its usage for the lucky draw alone. I may not have agreed for the business to share these details with other business associates. However, from the company's perspective, they may have already regarded this as a broad consent, which in most cases are explicitly stated upfront in a lucky draw coupon, and for any of its intended commercial purposes such as promotion of products through e-mails, tele-marketing, and so on.

So, when the sales mechanism is activated, one may find oneself unwittingly applying for a credit card or, in the worst case, signing away one's right for our personal data to be used in any way that the company wants. While consent can be withdrawn, it leads to much personal hassle which could have been prevented with better consumer knowledge. How do we ensure consumers understand the terms and conditions that they may have unwittingly agreed to? How about those who are not able to read and understand the fine print well? How does the new law draw the line in this case between promoting commerce and protecting the interests of consumers? What would be considered as deceptive and misleading practices? By putting forth these questions, I would like to highlight that the challenges will be in the execution, implementation and enforcement. This will include the criteria and the interpretation of the law and rules even though consumers can apply to be in the DNC register or carry out withdrawal of consent.

From the business perspective, the new legislation may have adverse effects on the business if they are unable to handle the new privacy demands of their customers well. I am equally concerned on the impact on the livelihood of the many insurance and property agents as some of them may be freelance professionals themselves. With the new Bill, it would be useful to have supporting guidelines or guides in a succinct format, as to how these industries, their stakeholders and individuals are to act in compliance with the new laws and still be efficient and profitable. Perhaps, even the standard form or format which is in legal compliance with the new law is circulated or shared by the Ministry.

In terms of the exclusion list for this new Bill, public agencies do not have to be subject to the rules under PDP. The apparent inconsistencies in the application of rules are an immediate concern. We know that the Government has its own set of data protection rules that public officers have to comply with. These rules are said to be like the PDP itself and therefore an additional layer of law is not needed.

Page: 872

In a similar vein, I put forward, would a not-for-profit organisation, such as the National Trades Union Congress (NTUC) and 61 affiliated unions, with the interests of workers in mind, not qualify to be exempted from the PDP? Currently, for NTUC and our affiliated unions, we already have strict internal controls as to how we manage the database of our members to protect their privacy. My concern is whether the new laws will affect our outreach and communications to our workers and members. At the same time, will the Unions' organising efforts to engage more non-members in the public domain be affected?

NTUC's membership efforts need to be as wide-ranging and pervasive as possible. While we understand that there is freedom of association, NTUC and our affiliated unions would like to share our benefits effectively to the working populace. It would be far easier to carry this out without the onerous requirements now set out. NTUC as an inclusive Labour Movement can only play the role of bringing different communities closer together. NTUC and our affiliated unions are driven by a social cause and not for profits. Hence, I submit that we should not be subject to these additional regulatory measures intended for the private sector. I would like to strongly appeal for organisations such as NTUC with a keen interest in workers' welfare to be exempted from this new Bill and Act.

Having listed the effects that PDP has on various stakeholders, it would be good to consider the overall impact that PDP will bring to our society. The establishment of the Personal Data Protection Commission (PDPC) is meant to implement the law. However, with its wide-ranging powers, I am concerned about the impact that it has on the civil rights of our people and commercial rights of our businesses. Herein lies the challenge of the balancing act again – how do we establish the genuine intention of fair business practices versus the indiscriminate selling of customer databases from business to business. It is important that while we will vest PDPC with its investigative powers such as search without warrant, the composition of PDPC should reflect the diverse perspectives of not just the Government but of businesses and civil rights leaders. There should also be significant public and consumer education about the appeal mechanism and grounds for appeal.

It is important for us to be able to establish the desired outcomes that we would like to see from the implementation of the PDP. The desired outcomes should be inclusive to ensure win-win for consumers, businesses and protection of the individual's privacy. Once again, on behalf of the Labour Movement, I would like to seek the exemption of NTUC and our affiliated unions from this Bill. Notwithstanding, I support this Bill to tighten the protection of our personal data.

Page: 873

5.54 pm

Mr R Dhinakaran (Nominated Member): Mr Speaker, Sir, today, we are on the verge of passing a landmark Act, which will make personal data more confidential and safe. While I understand the need for such a Bill arose from the plight of several unhappy residents of Singapore having being accosted by strangers offering various unsolicited services, and the need for the law to take a tough stand to dissuade such nuisance creators, it is important to understand and think through the needless collateral damage we may be causing with this Bill.

The Bill has tried to define personal data, its usage and various obligations for the party holding on to this data. While the attempt has been towards clarifying the usage and their implications, it will weave in a maze of legal complexity into the subject. I wish to bring to highlight certain types of challenges we are likely to face after this Bill is passed.

Firstly, I would like to illustrate the example of signing forms with disclaimers like in the case of credit cards, and so on, where most people sign on the dotted line without going through the page full of clauses in detail and in very, very small letters. You need a kind of binoculars to go through the details. They may have unknowingly permitted usage of their personal data for marketing purposes, which the company is within legal bounds to use.

However, the customer may take offence under the present law claiming the calls as violation of privacy and the business forced to prove that its calls were legitimate. For small businesses, the legal and operational costs incurred to prove that it was legally accorded the right to use the data by the customer will be an over burden.

In addition, the businesses always grow in size and scope and it is very natural for new add-on services to emerge, keeping in view of its relevance to its customer base. This results in the creation of newer business divisions, entities and subsidiaries within the same parent group.

The Bill forbids usage of existing customers' data between subsidiaries or group companies unless explicitly collected for the use. This will lead to severe duplication of efforts and maintenance of separate databases, marketing team, etc, and may even kill cross marketing efforts which drive increasing productivity and even customer satisfaction. Of course, it leads to higher costs for businesses in duplicating the marketing efforts.

Furthermore, wilful wrong submissions of data by customers who want to protect privacy but are also keen to have businesses reach out to them on offers is not uncommon. Some people may be filling mandatory fields in an online form, with fictitious email, IDs and phone numbers. While these numbers may not be theirs, it may be existing numbers of other people who have shown no interest in the company's products or services but are now exposed to marketing calls unwittingly. Is the business guilty on the count of breach of privacy?

Page: 874

The Bill states the need to preserve logs and usage of personal data for a minimum period of one year. Is it practical to expect SMEs to maintain logs for every marketing call they make if they do not use the services of a sophisticated call centre? I am sure some small businesses may not have the resources to engage such professional services for peripheral reasons or spending additional resources in maintaining the data internally.

While the Bill requires data users to preserve sources of data, it allows already available public data for use. What about customers who have detailed online profiles giving personal contact particulars while also seeking privacy or selectively signing consent for certain use? Does the public information available overrule all the selective consent given? What if visiting cards shared in business forums or meetings are used as a consent and implicit interest in the company's products and services?

I would like to draw attention to the DNC database. This is the most direct redressal of key grievances leading to the Bill. I am sure most of us receive unsolicited calls typically trying to market unsolicited financial instruments. We may want to join the DNC list out of frustration and irritation. Having joined the list, it does not preclude any of us from being enamoured by some exciting things we see or offers we like and therefore we may register our interest for these services or goods.

However, if the business does really check the DNC registry, we should be getting no communication. Is this what we want? Is this acceptable? Will we not charge the retailer for not providing good services and not receiving the communication despite registering for it? The fact that we have chosen to enlist in DNC may have occurred in a different context and timeframe.

The DNC, being dynamic in nature, makes it even more onerous for businesses to follow. Businesses may make a decision based on the status at a point in time, only to be unwittingly violating it at the point of making the call should the customer opt out of the DNC list by then. These are practical realities and complexities. Moreover, the call roster to make calls at call centres is made in advance.

Having spelt out a few instances of complexity and additional costs we may be weaving into the existing practices, I would like to imagine brief immediate recourse by businesses to avoid the maze of legal complexities the Bill may bring about.

Today, in many western countries where a DNC registry is in place and personal data protection law is in force, unsolicited calls are almost non-existent. Businesses have adapted to use other communication channels to reach out to their customers. These methods are largely generic and public channels. The use of flyers is extremely high in these markets. Perhaps, while we would have addressed the menace of unsolicited marketing approaches with a tedious-to-implement data protection law, we may be unwittingly inviting more flyer menace in our mailboxes. We may want to look and think about this well in advance, especially when we are spending large amounts of resources to control littering in our country!

Page: 875

At a time when we are looking at customised services and customised marketing, the new Bill will increase costs significantly for database handling and administration, making more of the smaller businesses to go back to blanket marketing methods which will be easier and less costly.

The irony of this subject is that while we are annoyed by unsolicited approaches, we are still keen to have the best offers to selectively reach us. It is a choice to make between wants for better deals and offers, and the need for privacy. A costly choice for the businesses, it is the price we are trying to assign for the legal complexity we may be weaving into our lives which may not address the real issue of breach of privacy as it may eventually lead to other kinds of unsolicited approaches. Marketing, after all, is to create a need where there is none, and it is the best possible when you reach out to a target segment beyond your existing customer base.

Having made my point through the speech, I would like to acknowledge that there is indeed a need to protect the privacy of our people and it should not be abused by cold calls and unsolicited approaches. But I feel the approach we are taking is perhaps more theoretical than keeping it simple, practical and perhaps clinical. Some possible ways will include those I will list.

If there is indeed clamour in the market on unsolicited communication, it would be perhaps best to analyse and segment the noise and address the specifics alone. For instance, if financial marketing of loans and credit lines are the majority of the breach of personal privacy, then an opt-out option could be made compulsory before making the call.

To ensure that customers' privacy is respected but at the same time he is exposed to new products and services that may be of interest to him or her, we should allow a less direct but personalised approach. A SMS to an intended customer seeking permission to call for discussing an offer can be sent together with an option to unsubscribe future messages and calls on a toll-free basis will clearly avoid nuisance while giving the customer a choice with minimum intrusion. A call should follow only having a reply from the customer rather than a message where silence is implied as acceptance to the offer.

Imagine, if offers in supermarkets are not to be communicated to regular buyers, how would the customers react to their favourite retailers not communicating to them on bargain buys? Clearly, there is a

distinction on what we would want to hear and what we do not want to hear from the marketers. A blanket approach may not be a good solution.

Page: 876

Besides, in case of disputing the intrusion by both parties, the resolution would become an expensive and needless affair for both parties. What we need to build in here is more a sense of responsibility to marketers and a clear option for customers to opt out after having been given a chance to understand what is being offered.

This will ensure that the customer later does not cry foul that he was never informed, while the fact would have been that he had opted out of all marketing calls because he was irritated by one stray call for something he did not want. A simple and balanced approach is the way to go forward, than to weave complexity and create more work for all parties, including the judiciary. The cost-benefit analysis may also prove the complexity is unworthy. On the whole, I support the Bill, Sir.

6.07 pm

Mr Lim Biow Chuan (Mountbatten): Sir, I rise in support of the Bill. Over the last few years, many consumers have complained about the proliferation of unsolicited calls and SMSes which they received. These calls and SMSes generally try to sell them a service or product which they did not ask for. For example, I am not looking for a house. Yet, each month, I receive several SMSes promoting the sale of houses and the launch of new housing developments. In addition, I also receive cold calls from advertisers trying to sell me hotel packages, financial products and timeshare package.

Sir, some of these calls were made at odd hours and some calls were made whilst consumers were overseas. Many consumers complain that they get very irritated each time they are overseas and received unsolicited calls or SMSes from advertisers. They then may have to bear the extra overseas telecom charges for these unsolicited advertising calls and SMSes. It is a waste of their time and disruptive to their work to have to answer to such calls or to read SMSes when they are busy or at a meeting.

I have also heard from a friend that once, when he tried to cut short the telemarketer and said that he was not interested in the product, he received a string of expletives and the caller then hung up the phone. Unfortunately, the marketing call was made from an unlisted telephone number and he had no recourse to complain.

Sir, the general consensus is that much of the information which is available to commercial advertisers is derived from data which consumers innocently gave whilst filling in forms for lucky draws, for some VIP or privilege cards or completing survey forms. These data are then compiled and then traded for sale. Thus, if we search the Internet, we will find that some 5,000 names can be sold for as little as $250. In this computerised age, it is so easy to replicate and sell the data list again and again to different organisations trying to launch their new products or services. In fact, feedback from many consumers suggest that their details are being circulated amongst timeshare companies as these consumers receive repeated marketing calls from different timeshare companies.

Page: 877

For these reasons, Sir, I strongly support the introduction of this Personal Data Protection Bill. It is the right thing for the Government to regulate the collection, use and disclosure of personal data and to ensure that once collected, the data cannot be used for different purposes or reasons unless express consent from the individual has been obtained.

I also support the setting up of the Do Not Call registry at Part IX of the Bill. I accept, Sir, that there is a need to balance the social benefits and economic advantages of some form of electronic advertising. It is also not in the interest of society to absolutely ban all forms of electronic advertisement, some of which may be educational in nature, some of which may promote a charitable cause and some of which may be for research. Thus, the definition of specified message at section 37 of the Bill with the exclusions at the Eighth Schedule is acceptable for the moment. These may have to be reviewed at a later date as technology and the norms of the world change.

Sir, allow me to seek some clarifications on the Bill from the Minister. Section 13 of the proposed Bill provides for the organisation to seek consent from individuals before collecting, using or disclosing the personal data. Section 20 provides for the organisation to notify the individual the purpose for collection of the personal data and any other purpose for the use or disclosure of the data.

Sir, supposing an organisation buries details in small print in its lucky draw or survey forms, that they are collecting the personal data for sale to third parties and that the individual, by completing the form consents to the disclosure and sale of the personal data, is that allowed under this law?

My concern is that many consumers do not actually read the small print which may be found at the back of the page or that it is simply too small print.

Some years ago, when I bought a sofa set, I was given 15 lucky draw forms to complete. At that time, my focus was simply to quickly fill in the forms, much less read the small print terms and conditions. I have since stopped filling in lucky draw forms.

Sir, section 22 of the Bill provides that an individual may request an organisation to correct an error or omission in the personal data. May I ask whether that individual can also request that his data be deleted?

Page: 878

Section 26 of the Bill provides that an organisation shall not transfer any personal data to a country or territory outside Singapore except in certain circumstances. Suppose a rogue organisation breaches this section and sells all the personal data to another organisation outside Singapore, how would such a breach be established? Secondly, if the buyer of such personal data were to operate from overseas to trade in the data, what would the Government do? With the current Internet technology, it is really not too expensive to call from overseas using Internet platforms like Viber.

Sir, I do express concern about how proactive the Government is in enforcing the law because when the Spam Control Act was introduced in 2007, I spoke on it, and I had some hopes that spam e-mails

would be reduced. However, quite honestly, I have seen little improvement to the situation. My e-mail and many of my friends' e-mails still receive a large amount of spam e-mail weekly.

Next, Sir, section 28 of the Bill provides for the power of the Commission to review certain complaints. Could the Commission's power to review be extended to investigate a complaint by an individual that an organisation has required the individual to consent to the collection, use or disclosure of personal data beyond what is reasonable, or to review a complaint that an organisation has not made reasonable security arrangements to prevent unauthorised access or disclosure of personal data.

Section 32 of the Bill provides for a person who suffers loss or damage to have the right of action for relief. Could the Minister clarify what kind of loss or damage is envisaged before an individual may commence such an action?

Sir, finally, Part IX of the Bill, the Do Not Call registry, Minister had earlier stated that there would be a separate register for facsimile messages. May I know whether businesses can ask to be included in this Do Not Fax registry so that they do not receive spam faxes? What about e-mails? If e-mails are not included, would businesses resort to sending e-mails since they are no longer allowed to make voice calls, SMSes or faxes?

Finally, Sir, I would urge for this law to be implemented as early as possible. Otherwise, personal data collected may be traded before implementation of the law, or may be transferred out of Singapore before the implementation date. Sir, I support the Bill.

6.15 pm

Mr Gan Thiam Poh (Pasir Ris-Punggol): Mr Speaker, Sir, I rise in support of this Bill. I appreciate the Ministry's sincere efforts to take into account the concerns of all stakeholders regarding personal data protection. Not less than three rounds of public consultations were conducted between September last year and this April. Members of the public and industries had contributed close to 1,900 feedback regarding this protection framework, the Do Not Call (DNC) registry and the proposed legislation. I would just like to add a couple of points.

Page: 879

Firstly, with 97% of the respondents in the MICA poll supporting the idea for a DNC registry, perhaps we should consider changing the registry to an opt-in list of phone and fax numbers instead. That is, only individuals who do not object to being contacted by organisations seeking to provide goods and services have to register for the list. The assumption is that the rest of the population does not desire unsolicited calls, SMSes and faxes. I think this is a more cost effective and efficient way. In addition, such a registry is more considerate of the needs of the vulnerable members of our society, including many elderly folks. Why should they be inconvenienced with the requirement of opting-out registration? In fact, I suspect after the passing of the Bill, telemarketers will end up targeting this group after the more savvy residents had submitted their opt-out applications.

Secondly, we have this problem of calls originating from call centres overseas. May I ask the Minister to share with the House the legal implications and enforcement measures for businesses with multiple call

centres in other jurisdictions, as this Bill only addresses organisations in Singapore.

6.17 pm

Assoc Prof Dr Yaacob Ibrahim: Thank you, Mr Speaker. First, I thank the many Members of this House for their support for this Bill, and for sharing their thoughts on important issues that this piece of legislation seeks to address. Sir, Members have raised many different scenarios about the protection of individuals and the concerns of organisations. The Bill is drafted to apply to all sectors in the economy and necessarily contains broad and general principles. It will therefore not be possible to give a definitive answer to each and every scenario, as this would require an assessment of all the facts of the specific case.

Sir, with this in mind, let me address the key themes and questions that Members have brought up. One of the key issues that Members have brought up is the issue of compliance costs, especially for SMEs. This is a key consideration for us in developing this Bill. We have sought to mitigate compliance costs for businesses where possible. Several requirements have been adjusted to take into account the feedback and suggestions received from the businesses during the public consultations period.

[Mr Deputy Speaker (Mr Charles Chong) in the Chair]

For example, Sir, the law will impose fewer obligations on organisations known as "data intermediaries", which process personal data on behalf of other organisations. Measures are also in place to mitigate organisations' costs for handling access requests. Business-to-business marketing calls and messages are also excluded from the Do Not Call (DNC) registry so as not to unduly hinder business-to-business marketing.

Page: 880

Sir, I would like to assure Members that we have been mindful to ensure the Bill does not impose overly onerous requirements on our businesses, while maintaining an adequate level of protection for our consumers. Nonetheless, Sir, some costs are inevitable in complying with any new piece of legislation or regulation.

Both Mr Zaqy Mohamad and Ms Low Yen Ling asked about training and financial assistance to help our SMEs comply with the Act. Sir, to ease organisations into the new law, the Bill provides a transition period of 12 to 18 months for organisations to adjust their practices to comply with the DNC registry and data protection requirements, respectively. During this period, the Personal Data Protection Commission (PDPC) will focus on building up the capabilities of organisations to comply with the Act. The PDPC will issue advisory guidelines, provide educational materials as well as conduct education and outreach activities to help both organisations and individuals better understand the Act. These education and outreach activities will continue beyond the transition period because it is in our interest to ensure that everybody knows the Act well so that they can comply with it effectively and efficiently.

Sir, there are also existing industry assistance schemes, such as IDA's iSPRINT scheme and SPRING's Innovation and Capability Voucher scheme, that companies can potentially tap on to help defray costs in upgrading their systems or processes to comply with the Act.

Sir, both Mr David Ong and Ms Jessica Tan rightly pointed out the need for a framework that balances innovation and flexibility with the need to ensure good data governance. A data protection regime can help promote business innovation and enhance competitiveness. It was also observed that consumer data, if appropriately used, can lead to better services and products that help local businesses become more competitive. The Bill also supports Singapore's development as a global data hub by providing a conducive environment for global data management industries, such as cloud computing and business analytics, to operate in Singapore.

Sir, Mr Desmond Lee asked how the Bill is envisaged to operate in relation to common law principles. The Bill does not seek to change any right or obligation conferred by or imposed under the common law, including the common law principles of confidentiality and consent. The Bill does address a number of issues that are not covered under the common law today. For example, the common law does not have a general requirement that consent must be obtained for the purpose for which personal data is collected, used or disclosed.

The Bill, as we have mentioned, is a baseline legislation that will operate concurrently with other legislative and regulatory frameworks. Taking the example of the health sector, medical records that contain personal data are covered under the Bill. This includes personal data contained in electronic health records. Doctors will need to follow the rules for collection, use, disclosure, access and correction, and care when dealing with personal data in medical records. In addition, Sir, other relevant laws, such as those under the purview of the Ministry of Health, may also apply.

Page: 881

Several Members also commented on the definition of personal data. Mr Zaqy Mohamad raised the concern that the definition is broad and vague and may not cover information such as a person's salary and religious preferences. As one can tell from the different situations that Members have raised, it is necessary for the definition to be sufficiently broad to allow the Bill to apply to differing circumstances. The definition adopted in the Bill encompasses any data that can identify an individual, and it will cover the examples cited by the Member. The definition also covers personal data recorded in both electronic and non-electronic formats.

Mr Ang Wei Neng spoke about CCTVs. The Bill covers CCTV recordings to the extent that images of identifiable people are captured. However, imagery captured by CCTV in public places may be considered as "publicly available" personal data, and can be collected, used or disclosed without consent. However, for CCTV surveillance at private premises, consent would generally be required unless other exceptions apply. In such cases, it may suffice to notify individuals through the placement of signs that CCTVs are monitoring the premises. The PDPC will provide more detailed guidance on the use of CCTV and surveillance cameras in due course.

Sir, several Members asked how the Bill will apply to personal data posted online, such as social networking sites and blogs. Online sites, including social networking sites and blogs, may be considered "publicly available" sources depending on the circumstances. The collection, use or disclosure of "publicly available" data will not require the consent of the individual concerned.

On Mr Zaqy Mohamad's suggestion to cover cyber-bullying and other undesirable online behaviour, the Bill is concerned with regulating the management and the protection of personal data. It does not govern other actions of individuals online. This would be more appropriately addressed by other laws.

Sir, several Members asked about the application of the Bill to foreign organisations operating in Singapore, and ensuring personal data transferred overseas are accorded the same level of protection. The Bill will apply to any organisation that collects, uses or discloses personal data in Singapore. This includes foreign companies operating in Singapore.

We are not adopting a prescriptive approach of restricting transfers of personal data to countries that have an adequate level of data protection. Instead, the Bill adopts a "principle-based" approach, where the onus will be on the organisation in Singapore to put in place measures, such as contractual arrangements, to ensure a comparable standard of protection is accorded to personal data transferred overseas. Therefore, there is no need to further burden our organisations with disclosing to consumers where copies of their personal data will be transferred to.

Page: 882

Sir, the Bill applies to all organisations across the private sector, regardless of whether they have commercial or non-commercial aims, such as NTUC. This is important as it will assure the public that there is a minimum set of data protection rules applied consistently across the private sector and foster greater trust.

The Bill does not cover the public sector as it already has its own set of data protection rules that all public officers must comply with. These rules are guided broadly by the same principles under the Bill. Statutory provisions in several Acts also regulate the collection, use and disclosure of information by the public sector. These ensure that public agencies and officials are subject to responsibilities to maintain confidentiality and protection of personal data, while enabling them to carry out their statutory functions in an effective and accountable manner.

All Ministries, Statutory Boards and Organs of State are required to comply with the public sector rules with regard to Data Protection. The Government takes steps to ensure that officers comply with Government policies and regulations, including Data Protection, for example audits may be carried out, and where there are cases raised to the Government, these will be investigated and officers who are found to have violated these regulations may be disciplined according to the Public Service Disciplinary Regulations. Agencies have mechanisms and processes in place to receive and address complaints or enquiries about Government's policies and procedures relating to the handling of personal data. In relation to individual's access and correction rights, individuals can also request.

Sir, I understand that individuals may also request Government agencies to correct inaccurate personal information held by the agencies. I would also like to reiterate that personal data held by Government agencies are protected by appropriate security safeguards against accidental or unlawful loss, as well as unauthorised access, use or disclosure. This is regardless of the format in which the personal data is kept.

Mr Ang Wei Neng touched on how the Bill will apply to Members of Parliament. In general, Sir, Members are required to comply with the requirements under the Bill when collecting, using or disclosing personal data in the course of their work. In certain cases where an individual voluntarily provides his personal data to the Member for a purpose, such as for the Member's assistance, consent may be deemed to be given for the Member to pass the personal data to a relevant organisation for the purposes of providing assistance. Where the Member is acting on behalf of a public agency, the public sector rules will apply.

Page: 883

Sir, Mr Desmond Lee asked about the exceptions provided in the Second to Fourth Schedules. These are based on the overarching intent of ensuring adequate protection for individuals without placing onerous burdens on organisations to comply with the law. They also take into account international practice and Singapore's context. For example, exceptions apply in certain circumstances or situations where obtaining consent for the collection, use or disclosure of personal data may not be feasible. Such situations include collection of personal data for life-threatening emergencies. Exceptions are also necessary to enable certain organisations to effectively perform their functions, such as investigations or legal proceedings.

Sir, let me now address some of the queries on specific situations. Sir, as I mentioned earlier, how the Bill applies will depend on the facts and circumstances of the case. In the example of the lucky draw forms, mentioned very often today, including by Mr Patrick Tay, that if the organisation had clearly stated on the lucky draw form that the personal data provided would be used for the purposes of contacting the individual to market certain products, then the organisation would be able to use it for those purposes. So, I advise that you read the fine print in future. If, however, there was no mention of the marketing purpose, then it is likely the organisation will be in breach of the provisions if they use the data for marketing activities.

Likewise, for the example of the use of the NRIC details raised by Assoc Prof Fatimah Lateef, organisations should consider if collecting a person's NRIC number is reasonable for the purpose, and obtain the individual's consent. For example, if the organisation needs to verify the individual's identity to provide certain services, such as for admission to a hospital or to check on his health insurance, it may be reasonable to require the individual to provide his NRIC details to prove his identity.

Sir, several Members raised the need to provide for special groups of people such as children and the mentally incapacitated. Members may wish to note that the details of persons who may act for minors and the extent to which they can exercise their rights or powers of such individuals will be set out in the subsidiary legislation subsequently.

The Bill is designed to allow sectoral legislation to provide higher level of protection on top of its baseline requirement. Additional protection for other special groups that is required can thus be catered for by sector-specific laws. I take Ms Low Yen Ling and Assoc Prof Fatimah Lateef's point that children's personal data will be an increasingly important issue, as tools and platforms for collecting children's data become more prevalent.

Page: 884

The Bill, Sir, is a first step in putting in place a basic personal data protection regime for Singapore. We will continue to review and adjust the legislation to address additional areas of concerns where necessary.

Sir, several Members raised queries about the Do Not Call or the DNC registry. Allow me to clarify some of these concerns. Mr Dhinakaran raised concerns about the DNC registry's impact on organisation practices. Today, nothing prevents organisations from freely collecting, using, sharing, or selling consumers' personal data without consent. The Bill imposes the necessary requirement on how organisations may collect, use or disclose personal data so as to protect individuals from the misuse of their personal data.

To clarify a point mentioned by Mr Dhinakaran, the Bill does not prohibit the sharing of personal data between entities, as long as consent is obtained. This approach strikes a balance between allowing organisations to share personal data and allowing individuals to decide how their data may be used. The Bill also does not prescribe a retention period for personal data. It only states that organisations should not retain personal data when such retention no longer serves the purposes for which the data was collected. It does not make business sense – if you do not use it, delete it. This is in recognition that the appropriate retention period will vary according to the legal or the business needs of each organisation.

Requirements of the DNC registry are not as complex as some Members may perceive. Organisations that send marketing messages must check their contact list with the DNC registry within the prescribed period before sending the message. A 60-day checking interval will be prescribed for the first six months of the DNC registry's operation. Thereafter, we will reduce the checking interval to 30 days. An organisation will not be in breach of the rules if it sends marketing messages to individuals who register their numbers within the interval period, after the organisation has checked with the DNC registry. So, if you check on day one and his number is not there on the registry, you can send a marketing message to him. On day two, he enters his number in the registry. This is still within the prescribed period. However, this individual should not receive any marketing messages after the 60-day or 30-day interval. Organisations may still send marketing messages to registered members if they have obtained clear and unambiguous consent to do so, in written or other accessible form.

In the examples raised by Members, seeking consent to use personal data using general or vaguely-worded clause, buried within pages of other terms and conditions, is unlikely to be considered clear and unambiguous consent. This may not comply with the requirement to notify individuals of the purposes of collecting, using or disclosing their personal data and could also be considered a misleading or deceptive practice prohibited under the Bill. Organisations should also retain the records of consent that its customers have given, to indicate that they can be contacted for telemarketing. This is a practical way for organisations to demonstrate that they are compliant with the law.

Page: 885

Sir, Mr Zaqy Mohamad and Mr Lim Biow Chuan made a valid observation about telemarketing calls originating overseas. Similar concerns of the abuse of personal data by overseas organisations were also raised. While the PDPC may seek to enforce the Act against overseas organisations, in reality it may be

difficult to investigate and proceed with any enforcement action against such organisations. Recognising this limitation, clause 37 provides the ability to enforce against any local organisation that authorises sending of the marketing message. So, this will mitigate the problem as marketing messages targeting Singapore telephone numbers are likely to involve goods and services by organisations with a local presence. The Bill also contemplates that the PDPC may establish arrangements with foreign data protection regulators, which may include cross-border co-operation.

Sir, Asst Prof Eugene Tan asked about covering e-mails under the scope of the DNC registry. We have decided not to include e-mails as unsolicited e-mails can be blocked through e-mail filters and cause less of a nuisance to delete when received as compared to phone calls in the wee hours of the morning, SMSes and fax messages which are more difficult for the individuals to filter out. A significant proportion of spam e-mails also originate from overseas, which makes it difficult for any enforcement action to be taken, even if the e-mail messages were to be included.

Sir, I take the point raised by Mr Dhinakaran that the DNC registry may lead to more organisations using mass marketing channels such as direct mailers and flyers. Sir, I would suggest that the DNC registry will better focus organisations' telemarketing efforts. This is because the DNC registry allows them to effectively target a group of consumers who are genuinely interested in receiving information on products and services, and eliminate time and resources wasted on those who do not wish to receive such information. It should drive more positive behaviour rather than negative behaviour.

Individuals who change their minds can withdraw their numbers from the DNC registry using a similar method as registration. The process could be as simple as calling a number, using the phone of which the telephone number is to be registered or deregistered, or filling up an online form.

Sir, several Members raised the possibility of organisations taking advantage of the transition period to collect and use personal data. Do not forget the public also know that the Bill is coming. So they should be more cautious.

Sir, the Bill has taken the approach of protecting individuals' personal data without imposing overly onerous requirements on organisations. Requiring organisations to notify or deem consent from individuals for all personal data previously collected, would be too onerous. The Bill, therefore, takes a balanced approach by allowing organisations to use the personal data collected before their appointed date for the purpose for which it is collected, provided the purposes are reasonable. After the law comes into effect, individuals can withdraw consent that was previously given. These measures will help protect consumers from those who seek to use the transition period to misuse personal data before the law comes into effect.

Page: 886

Sir, several Members also requested for staggered transition periods. Ms Jessica Tan proposed different sunrise periods for 12 months for large businesses and two years for small businesses. We have proposed a single sunrise period for at least 18 months for all organisations, regardless of size, in order to minimise confusion and perhaps keep implementation simple and effective.

Differential treatment for small companies in some jurisdictions was found to have added to the complexities of implementation. During the sunrise periods, the PDPC will conduct awareness-building activities for both businesses and consumers, in relation to their rights and obligations under the regime. These activities will be targeted at enhancing organisations' ability to comply with the PDPA when it comes into effect.

Sir, several Members touched on the issue of enforcement and implementation. The Bill provides the PDPC with a range of powers to enforce the Act effectively. It adopts what we call a complaints-based approach to enforcement and the PDPC will have the powers to initiate investigation or investigate if a complaint is lodged. It will have the power to investigate potential non-compliance and the power to issue directions to organisations to correct their non-compliance. In enforcing the law, the PDPC is expected to act on cases in a timely manner and may issue advisory guidelines on its procedures and associated timelines in due course.

Mr Desmond Lee expressed concern about the dispute resolution and the appeal process being cumbersome. The approach, Sir, takes into consideration that a large majority of cases are likely to be resolved early, which may not require a decision by the PDPC. However, in instances where the PDPC is required to investigate and take enforcement action against an organisation, the appeals process allows for a quicker resolution through reconsideration while providing aggrieved parties the appropriate avenues to appeal to an independent appeal body. Further appeals to the High Court and the Court of Appeal are allowed on points of law or on the amount of the financial penalty imposed. Sir, this is in line with other laws such as the Competition Act.

Sir, Mr Patrick Tay and Ms Jessica Tan spoke on the role of the composition of the PDPC. As mentioned in my earlier speech, the PDPC will serve as Singapore's main authority on matters relating to personal data protection. It will also undertake education and outreach activities to promote public awareness of personal data protection in Singapore. An advisory committee will be appointed to provide advice to the PDPC. It will comprise members of the industry, members of the public and civil society. The exact composition of the PDPC and the advisory committee will be firmed up and announced in due course, if the Bill is passed.

Page: 887

Sir, the Bill is not intended to be overly prescriptive as it applies to all sectors of the economy. To provide greater clarity on the interpretation and the application of the Act, the PDPC will issue advisory guidelines which will be developed in consultation with the industry. Public education will also be key as some Members have highlighted and, in this regard, the PDPC will reach out to the public, including our young children and schools, to raise awareness to the importance of personal data protection. So, while the Bill puts in place safeguards to protect consumers' personal data, ultimately, individuals will have to take responsibility for their own personal data.

Sir, as you can see from the broad range of issues raised by Members of the House, from consumers and business interests to national and international considerations, we can appreciate the complexities of the issue of personal data protection and the importance of striking a balance within the various considerations. Sir, the issues that Members have raised are among the myriad issues we have

considered in formulating a model that takes into account the interests of different stakeholders and Singapore's needs. We also recognise interests and circumstances may change. We will, therefore, need to continue to review and adjust the law to address new and emerging issues. As the Chinese proverb says – I will have to say this in English, Sir – "The journey of a thousand miles begins with one step." Members of this House will agree that this is an important legislation and a significant step forward for Singapore, and I hope they can support the Bill, Sir.

Question put, and agreed to.

Bill accordingly read a Second time and committed to a Committee of the whole House.

The House immediately resolved itself into a Committee on the Bill. – [Assoc Prof Dr Yaacob Ibrahim].

Bill considered in Committee.

[Mr Deputy Speaker (Mr Charles Chong) in the Chair]

Clauses 1 to 68 inclusive ordered to stand part of the Bill.

First Schedule ordered to stand part of the Bill.

Page: 888

Second Schedule –

The Chairman: The Second Schedule. Assoc Prof Dr Yaacob.

Assoc Prof Dr Yaacob Ibrahim: Sir, there are two amendments to the Second Schedule, as indicated on the Order Paper Supplement. As both amendments are related, may I seek your leave to move both amendments together?

The Chairman: Please do so.

Assoc Prof Dr Yaacob Ibrahim: Sir, I beg to move,

(1) In page 57, line 20, before "the", to insert "subject to paragraph 2,".

New Paragraph (A):

(2) In page 58, after line 27, to insert –

"2. In this paragraph and paragraph 1(h) –

"broadcasting service" has the same meaning as in section 2 of the Broadcasting Act (Cap. 28);

"news activity" means –

(a) the gathering of news, or the preparation or compilation of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public; or

(b) the dissemination, to the public or any section of the public, of any article or programme of or concerning –

(i) news;

(ii) observations on news; or

(iii) current affairs;

"news organisation" means –

(a) any organisation –

(i) the business of which consists, in whole or in part, of news activity carried out in relation to a relevant broadcasting service, a newswire service or the publication of a newspaper; and

(ii) which, if the organisation publishes a newspaper in Singapore within the meaning of section 8(1) of the Newspaper and Printing Presses Act (Cap. 206), is required to be a newspaper company within the meaning of Part III of that Act; or

(b) any organisation which provides a broadcasting service in or from Singapore and holds a broadcasting licence granted under section 8 of the Broadcasting Act;

"newspaper" has the same meaning as in section 2 of the Newspaper and Printing Presses Act;

"relevant broadcasting service" means any of the following licensable broadcasting services within the meaning of the Broadcasting Act:

(a) Free-to-air nationwide television services;

(b) Free-to-air localised television services;

(c) Free-to-air international television services;

(d) Subscription nationwide television services;

(e) Subscription localised television services;

(f) Subscription international television services;

(g) Special interest television services;

(h) Free-to-air nationwide radio services;

(i) Free-to-air localised radio services;

(j) Free-to-air international radio services;

(k) Subscription nationwide radio services;

(l) Subscription localised radio services;

(m) Subscription international radio services;

(n) Special interest radio services.".

Sir, as mentioned in my speech earlier, this amendment will provide a clear definition of what constitute news activities, the news organisations, to which the exception from the requirement to obtain consent for the collection of personal data will apply to. The intent of this exception, provided in clause 1(h) of the Second Schedule, is to enable the legitimate collection of personal data without consent for news gathering activities by organisations that are in the business of news, while providing some protection to members of the public from potential misuse and unwarranted publishing of personal data by other organisations.

Amendments agreed to.

The Chairman: Consequential amendments will be made.

(1) In page 58, line 13, to renumber paragraph 2 as paragraph 3.

Page: 890

(2) In pages 58 and 59, to renumber paragraphs 2 and 3 as paragraphs 3 and 4, respectively.

The Second Schedule, as amended, ordered to stand part of the Bill.

The Third to Ninth Schedules inclusive ordered to stand part of the Bill.

Bill reported with amendments; read a Third time and passed.

Page: 890
