Closing Speech by Mr S Iswaran, Minister for Communications and Information, at the Second Reading of the Personal Data Protection (Amendment) Bill 2020 on 2 November 2020

Introduction

1. Thank you, Mr Deputy Speaker.

2. Let me start by thanking all 13 Members who have spoken and for their support for this Bill. To be precise, actually, 11 Members have given explicit support and Mr Leon Perera and Mr Louis Chua, I am assuming, I have their deemed consent since I do not think that there is adverse effect on any individual. I also want to thank them for raising important issues this Bill seeks to address. And I think the comments of Members fall broadly into a few areas about: protecting consumers' personal data, endowing consumers with more control and a greater sense of autonomy and confidence while supporting organisations' legitimate use; and supporting businesses in the use of data for growth and innovation.

3. I think in the comments that have been made by Members, it is clear that we all appreciate and recognise that there is an inherent tension between these objectives, and the proposed amendments seek to strike a judicious balance between them.

4. In thinking about these issues and I do propose to address the specific questions raised by Members, it is important that we first recognise that this is a delicate and dynamic balance. It is delicate because if we over-correct in one direction, consumers may not retain their confidence and trust in the system. If we swing the other way, then we shackle our businesses and the very benefits that we seek for our consumers and for our economy will diminish. It is dynamic because technology is changing and the ways data is being generated and being put to use are also changing. And therefore, it is imperative that we find our own balance in the way we regulate the collection and use of data in Singapore.

5. And there are different jurisdictions with different models. GDPR has been cited by several Members. There is also the APEC CBPR. I do not think any one of these is universally acclaimed because each has its strengths and its weaknesses. And that is why, in this endeavour of moving this legislative amendment, we have sought to understand the different regimes and to ensure that Singapore is able to remain best-in-class and also ensure that we are nimble and remain interoperable, which is key to our positioning as a node in the international flow of data and digital transactions.

6. And that leads me to the second overall point I want to make, which is we must recognise that whilst legislation and regulation is important, it is not a panacea and neither is it foolproof. And therefore, what it means is whilst we can put in place rules that will govern the data practices and ensure that data is safeguarded to the best of our ability, we cannot eliminate the risk of data breaches.

7. So, it is important that we recognise that whilst the rules must be formulated and enforced, it must be complemented by good practices and that has to evolve over time so that we understand, as an overall economic system and as a society, our respective responsibilities and roles.

8. And that brings me to my third overarching point, which is that it is essential that we recognise all of us have a role to play and a responsibility to discharge in maintaining the security and the usability of our data regime and, in a sense, safeguarding the public commons.

9. So, Government formulates the rules and regulations, enforces, provides guidelines and adapts to changing market situations to ensure that we remain abreast, to the best of our ability, of the developments and ensure that we keep Singapore relevant in the context of a new digital economy.

10. Businesses must recognise that this is in their self-interest. It is not just about complying with rules or regulations. At the end of the day, in any competitive domain, businesses will be able to differentiate themselves by their data policy and they will be able to signal the quality of the institution by the kind of approaches they take to safeguard their customers' data. So, they must be accountable and responsible, recognising ultimately that it is in their self-interest.

11. And finally, individuals. I think all of us have the responsibility. Whilst some Members have talked about the so-called power asymmetry, ultimately, I would argue that consumers – individuals like you and me – we are not powerless by any stretch of the imagination. We can choose to decide whom to do business with or whom to give our custom. We can choose to decide what data we want to share. We can choose to decide whether we want to give consent and when we want to withdraw that consent. And, ultimately, we can decide when to sever the relationship if that is what we want.

12. So, I think we should not lose sight of that aspect as well. Ultimately, the legislation must be seen in that perspective. It is one part of an overall architecture that will ensure a vibrant digital economy, but also one where data is respected, it is safeguarded, but also used for appropriate purposes.

Consumers

13. Let me now turn to some of the specific questions that have been raised by Members.

14. First, on protecting consumers and the data. I think it is important to emphasise PDPA recognises organisations' need to use personal data for legitimate purposes. And today, that is accommodated through exceptions to the consent requirement, or as deemed consent. For all other purposes, organisations have to obtain consent from the individual.

15. Current exceptions to consent cater for scenarios such as investigations and responding to emergencies. We are updating this list by adding business improvement and legitimate interests and updating the research exception for the benefit of consumers and organisations in the digital economy.

16. The Bill is also clarifying the deemed consent provision to cover multiple layers of subcontracting when needed to fulfil a contract and to facilitate organisations notifying customers and giving a reasonable period to opt out, before they use data for new purposes. And I would like to reinforce this point and a point that Ms Jessica Tan had also picked up, that ultimately, consumers can opt out at any time and they have the freedom to do so.

17. I want to assure Mr Desmond Choo that all private sector organisations can rely on these new provisions, regardless of the industry they are in. It is meant to apply uniformly.

18. And on the whole, the amendments regularise current practices, provide organisations with clarity and confidence to use data, while protecting consumers' interests. As Mr Yip Hon Weng has noted, this will also enhance Singapore's status as an innovation and commercial hub.

19. Some Members have asked about the safeguards for the new provisions. Stricter process safeguards are prescribed for the general legitimate interests exception and deemed consent by notification, while specific exceptions, such as business improvement and research, are tightly scoped. The safeguards have been designed based on the following principles.

20. Before relying on the legitimate interests exception, organisations have to conduct a risk assessment and be satisfied that the overall benefit outweighs any residual adverse effect to an individual. And before relying on deemed consent by notification, organisations must conduct a risk assessment to be sure that there is not likely to be any adverse effect on an individual. Individuals may withdraw their consent even after the opt-out period. The PDPC may also require organisations to produce these assessments for its review. Some Members have asked how these provisions might be operationalised. The PDPC has provided guidance on how to conduct risk assessments. It will also issue detailed guidance on the legitimate interests exception and how to identify adverse effect, which generally refers to any physical harm, harassment, serious alarm or distress to an individual.

21. Exceptions for specific purposes, such as business improvement and research purposes, are tightly scoped. For example, the business improvement exception supports internal use of data within an organisation or a group of companies, with clearly defined limits. And when it comes to sending direct marketing messages, organisations still need to obtain express consent. Mr Sharael Taha enquired about the safeguards for deemed consent by contractual necessity. Essentially, organisations can rely on this provision to share personal data only to the extent necessary to perform their contracts with the individual. So, that is the test.

22. Mr Desmond Choo asked about the “evaluative purposes". This is actually an existing exception in the PDPA which has now been reclassified under the “legitimate interests exception”.

23. There has been another set of queries about how we can ensure or have confidence that organisations can be trusted to use personal data in good faith. I think this is an important point. I would start by saying firstly, we must recognise, more importantly, organisations must recognise that it is in their self-interest to safeguard personal data as that would foster consumer trust, strengthen their business reputation, and ultimately, their competitiveness and bottom line.

24. To support that and to ensure organisations take their obligations to protect data seriously, we are introducing both incentives and penalties – carrots and sticks, if you will. The PDPC will issue new advisory guidelines with examples and illustrations, so that organisations have ample notice of the expected standard of conduct.

25. As data breaches cannot always be prevented, the PDPC’s enforcement framework reinforces the importance of dealing expeditiously with data breaches to reduce harm, through measures like breach reporting and statutory undertakings.

26. Last year, PDPC investigated 185 cases, issued 58 decisions and ordered 39 organisations to pay a total of $1.7 million in financial penalties and that includes the highest financial penalty sums the PDPC imposed in 2019, which were $750,000 and $250,000 on IHiS and SingHealth respectively.

27. The Bill enhances PDPC's investigation powers and raises the financial penalty cap, to improve the effectiveness of PDPC's enforcement.

28. We are also creating market incentives, which can motivate organisations to practise high standards of data protection.

29. I agree fully with Mr Sharael Taha on the value of certification systems and that is why PDPC launched the Data Protection Trust Mark or DPTM in 2019, to make it easier for consumers to recognise organisations with accountable practices and create the demand for good practices along the entire supply and delivery chain. Organisations with the trust mark require their suppliers and contractors to also adhere to the same standards. It has a very beneficial ripple effect. There are signs, based on PDPC's Perception and Awareness Study, that this is having a positive impact on the industry.

30. For secure exchanges of personal data with overseas entities, transferring organisations must put in place contractual arrangements or binding corporate rules, to ensure that receiving organisations provide a level of protection comparable to PDPA. Apart from contractual transfer mechanisms, the PDPC joined the APEC Cross Border Privacy Rules, or CBPR, and Privacy Rules for Processors systems. These are multilateral certifications which require participating businesses to implement data protection policies consistent with the APEC Privacy Framework.

31. Consumers also have a crucial role in safeguarding themselves. I think this is a point that I made earlier, and Mr Sharael Taha and Mr Melvin Yong have reinforced that.

32. That is why on the part of PDPC, it has reached out to almost 70,000 individuals, including youths, through school talks, exhibitions, community roadshows and events. I am also heartened that these efforts have yielded promising results with consumer awareness of the PDPA and PDPC increasing.

33. Mr Desmond Choo has proposed that a right of erasure be explicitly recognised. I believe Mr Louis Chua was also referring to this. Currently, section 16 of the PDPA provides for individuals to withdraw their consent at any time and the organisation would have to cease the collection, use or disclosure of the personal data unless

otherwise required or authorised under any legislation. In addition, the PDPC can also direct an organisation to destroy personal data collected in contravention of the Act. So, we have the provisions. Whilst they are not identical to the right of erasure, I think they give a substantively similar effect.

34. On unsolicited messages, Mr Melvin Yong asked about our efforts to address spams and scams. In 2019, the PDPC received 2,255 complaints on unsolicited calls and text messages, and has taken action against 427 organisations. These actions range from issuing advisory notices and warnings, to prosecution in Court. The proposed amendments to the PDPA and Spam Control Act establish clear guardrails for sending unsolicited commercial messages, to safeguard consumer interests while permitting legitimate direct marketing.

35. Ms Tin Pei Ling and others have asked about the change in enforcement regime for DNC complaints – why we moved towards a civil administrative regime. The answer is that the assessment we had is that this would allow for a more efficacious enforcement. DNC infringements typically stem from commercial motives. Hence, directions and financial penalties are more effective in addressing poor practices by depriving offenders of the financial or commercial gains that they seek. So, it is not a step down. I think it is a more effective way of dealing with this problem.

36. To Ms Joan Pereira's and Mr Sharael Taha's queries, our response to spam that originates overseas will continue to be multi-pronged, comprising a mix of public education, industry self-regulation and international collaboration.

37. Scams, on the other hand – the letter makes all the difference; scams versus spams – scams are serious crimes and they are dealt with by the Police. They are enforced under laws like the Moneylenders Act for unlicensed moneylending; and Penal Code, for example, for cheating offences.

38. For transnational scams, the Police collaborates closely with foreign law enforcement agencies to investigate and, where possible, cripple these syndicates. MCI is part of the Inter-Ministry Committee on Scams formed by MHA to combat scam messages and calls. As many of these scams originate overseas, we have to rely more heavily on technological solutions, as Mr Yip Hon Weng and Mr Melvin Yong have noted. For example, IMDA has required all telcos to implement the "+" prefix for all incoming overseas calls since April this year to help consumers better identify and reject spoof calls. Telcos are also blocking international incoming calls that resemble our Government agency or emergency numbers. So, these are efforts to help consumers discern and avoid being duped.

39. I would urge consumers to carefully look at the numbers when they receive calls from overseas because I think this is one way. We cannot prevent these calls from coming in but we can put up red flags, and this "+" sign and some of these other measures are for that purpose. We will continue to support the Police in their efforts to tackle scams and other illegal activities.

Businesses

40. There have been questions on compliance costs and higher financial penalties.

41. I think many have asked about what support we are going to give to organisations and clarity for compliance with the new provisions. First, these amendments mark the culmination of a multi-year journey. So, we would like to ask organisations to see this as part of their own investment and effort in building customer trust and commercial reputation. Instead of conducting selective audits for the few as suggested by Ms Joan Pereira, the PDPC will continue to support organisations by providing guidance, training and access to expertise, and recognising accountable organisations, to inculcate good data protection practices as broadly as possible. Essentially, we think a comprehensive upstream approach may be more beneficial.

42. On guidance, PDPC provides accountability tools and resources, such as guides on implementing data protection management programmes, conducting risk assessments and adopting a data protection-by-design approach when developing IT systems.

43. On training, PDPC has been building up data protection capabilities through the Data Protection Competency Framework and Training Roadmap. Since its launch in July last year, more than 6,200 people have been trained. Data Protection Officers or DPOs, trained under this framework will be able to implement robust data protection practices as well as support innovation.

44. On access to expertise, we know and recognise that SMEs may need more help to comply with their data protection obligations. So, we have developed the Data Protection Starter Kit for them and Data Protection-as-a-Service as an affordable alternative for SMEs to outsource some DPO functions. PDPC also makes simple data protection solutions available on its website for free.

45. We launched the DPTM last year to recognise organisations with good data protection standards. And to-date, 37 organisations have already been recognised.

46. There are some concerns about the reasonableness of the increased financial penalty cap. Mr Desmond Choo proposed aligning the financial penalty cap with other Asian jurisdictions. The objective here is to ensure that we achieve the requisite deterrent effect on organisations. And that is why the financial penalties have been calibrated in the way that I have described. The proposed maximum financial penalty is comparable with other domestic legislation such as the Telecommunications Act and Competition Act and signals that data protection is of that level of importance in the digital economy.

47. Some have asked – I think Mr Patrick Tay was one of them – whether in light of the current circumstances we can exercise some flexibility in how these penalties and other elements are phased in. As I mentioned earlier, we intend for the revised financial penalty cap to take effect no earlier than one year after the Act comes into force, and the Minister has the discretion under the Act to review the effective date. So, we will be informed by the overall circumstances because we are conscious of not wanting to unduly burden our companies. The revised penalty cap will apply to breaches that occur after the effective date.

48. On compliance costs for the Data Portability Obligation, we want to make sure that the approach is balanced and achieves the intended results. So, to address the concerns over the scope of data that can or has to be portable, we have basically intend to help organisations with this new obligation, and introduce the data portability obligation in phases and will issue Regulations and advisory guidelines to provide clarity. This is new for Singapore. So, we want to make sure we do this in a measured way, clear about where we want to go – our destination – but prepared to be flexible in the path.

49. On Mr Sharael Taha's query on the safeguards for individuals, the regulations will prescribe consumer protection measures like cooling-off periods when porting certain types of data, in case consumers change their minds. To provide additional clarity on scope of implementation, we have also catered for the following:

(a) the scope has been narrowed to only cover individuals with whom the porting organisation has an existing and direct relationship;

(b) data portability will be scoped to user activity and user provided data in electronic form and will apply only to prescribed categories of data; and

(c) organisations are also not required to port data when the burden of porting, including the cost, is unreasonable.

50. Let me turn to mandatory data breach notification. In the Bill, "significant harm" refers to the impact of a data breach on affected individuals and is used in the context of a data breach notification. I think Mr Leon Perera, Mr Louis Ng and also Mr Shawn Huang had asked about this and I want to tell them that we plan to prescribe in the Regulations, a numerical threshold. This is something that has been developed through consultation and it is a numerical threshold of 500 individuals for what constitutes a data breach of a significant scale. This threshold is based on past enforcement cases and other jurisdictions' practices as well.

51. The Regulations will also include categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to individuals, such as identity theft or fraud. One example of such data is full name and confidential financial information.

52. We will give more guidance through the Regulations but I want to stress – because I think the question was asked how we derived at these numbers. I do not think that there is any rocket science or magic behind it. This is an exercise in judgement, working with the industry and learning from our experience and past practices to arrive at what we think is a reasonable threshold. And I think what will then have to happen is, we see it in practice and learn from experience, and adapt as we go along.

53. I want to assure Mr Louis Ng that PDPC will take a reasonable approach in exercising its powers proportionately and judiciously. PDPC's decisions are also subject to appeal to the Data Protection Appeal Panel and further appeals can be pursued in the Courts. So, there is recourse but in the first instance, PDPC will exercise due care and proportionality.

54. Ms Pereira suggested that organisations notify the PDPC of all data breaches and she also advocated setting a fixed timeframe for notifications to individuals. Setting such a threshold for notification is important, but we have to take into account the compliance costs on organisations and also focus the effort on potentially systemic issues. We have not set a fixed timeframe for an organisation's notification to affected individuals of a data breach because data breach circumstances can be very varied. Our positions have been developed in consultation with the public and benchmarked against jurisdictions like Australia, Canada, the EU and California. I will not rule out anything, but I think in the first instance we want to move forward and see how this works in practice.

55. There was a question of whether PDPC will exercise its expanded powers appropriately. The new section 48J details a list of factors that the PDPC will consider before imposing financial penalties. To Mr Melvin Yong's query, this will include whether the organisation had previously failed to comply with the PDPA which can be considered as an aggravating factor.

56. Mr Patrick Tay has raised a very important question on individuals' mishandling of personal data: how the new offences would apply for mishandling personal data?

57. We intend for this to apply only to egregious cases. Employees and service providers who are duly authorised should not have to be concerned. Additionally, we recognise that roles such as teaching and research may require re-identification of anonymised data and hence we have provided for applicable defences for them in the Act.

58. We do not intend for these offences to apply in situations where the conduct is solely in the nature of a private dispute. For example, a relationship manager transfers his clients' personal data to his new company with their consent, or a sales agent contacts his clients after commencing new employment. In such cases where the individual reasonably believes that he has the legal right to use or disclose personal data, he has a defence to the new offences. Such private disputes should continue to be resolved through civil suits or other forms of dispute resolution.

59. To ensure that these actions are not caught, we have provided for defences under clauses 22 and 38.

60. Ms Jessica Tan can be assured also that we will further set out in Advisory Guidelines the examples on how the new offences would apply so that organisations and workers have clarity and can continue to use data confidently.

61. Mr Patrick Tay asked about the removal of the exclusion for agents of Government. This makes clear that the PDPA applies to all private sector organisations. Currently, the exclusion of agents of Government has created a situation where the Government can only hold them to account via contracts or laws such as the Official Secrets Act. This gap can undermine security as such agents of Government may handle large and sensitive volumes of personal data.

62. The removal of the exclusion for agents of Government would provide much-needed clarity and certainty that private sector organisations are subject to the same obligations under the PDPA regime, regardless of the sector their customers are in.

Comparison between the Public and the Private Sector Data Regimes

63. My colleague, Senior Minister of State Janil Puthucheary, has explained in detail our approach towards the data regimes in the public and private sectors, so I do not propose to repeat those, but Ms Tin Pei Ling has asked about whether the two regimes would be aligned.

64. We will continue to ensure alignment of data protection principles where the policy intent is the same. The amendments further strengthen this by aligning the penalties and scope of offences for individuals' egregious mishandling of personal data across the public and private sectors. In the same vein, the PDPC and the Smart Nation and Digital Government Office or SNDGO are working together to ensure the public sector data protection policies continue to be aligned with the relevant changes to the PDPA.

Conclusion

65. Deputy Speaker, Sir, I believe I have substantively dealt with the issues that have been raised by Members.

66. If I may conclude, since the PDPA was enacted eight years ago, we have made significant strides in the extent we use data to make decisions and deliver services. Businesses are employing more sophisticated measures to safeguard personal data. Consumers are also more aware of the importance of data protection.

67. We need to adapt to the new landscape where digitalisation has shaped our world, bringing new opportunities but also new risks. This Bill is an important step in this direction. It aims to promote strong data governance to enable greater use of data for the benefit of our society and our economy.

68. What we want is equal emphasis on protection and innovation, so that consumers benefit from data-driven services and solutions, with trust that their data is used responsibly. And businesses use data confidently with proper accountability. And Singapore continues to be an important node in global data flows. Mr Deputy Speaker, Sir, I beg to move.