Ministry of Communications
and Information
An Engaged and Connected Singapore

Speech by Minister for Communications and Information Mrs Josephine at the Dentons Rodyk Dialogue 2022 on Monday, 31 October 2022

Mr Gerald Singham, Global Vice-Chair and ASEAN CEO, Dentons Rodyk

Professor Timothy Clark, Provost, Singapore Management University

Ladies and gentlemen

Introduction

1 Good morning and thank you for inviting me to today's Dialogue.

2 Technology, and the digital landscape move quickly. Every year, computer chips get smaller, faster, and more power efficient. Many of the transactions we used to perform physically have gone online. Who remembers the aerogramme? For most young people, it's Telegram. When was the last time you went to the bank or even used the ATM? Have you thrown out all your CDs yet, since almost everything is available on Spotify?

3 These developments have brought goods, services, and information to our fingertips. Businesses have become more productive; governments can also deliver services more efficiently; significant numbers of people have found new livelihoods.

4 But it has not been all hunky-dory. There are risks, and we can all fall victim whether as individuals or as part of larger organisations. Every digital connection can be attacked. Globally, it is estimated that almost US$950 billion was lost to cybercrime in 2020. Some of these attacks have been crippling. For example, in Costa Rica, two ransomware attacks disrupted over 30,000 medical appointments, took down their tax systems, and resulted in a national state of emergency. Cybersecurity is therefore critical. Our data is also at risk. Both individuals and companies are aware that when data confidentiality is breached, the damage – be it to personal well-being and reputation, or business competitiveness – may be irreparable. Online platforms have helped countless content creators build global audiences. But not all content is good. Child pornography, for example, is a problem some of my counterparts face. Fake news and hate speech can go viral when they are amplified on social media. In 2019, a gunman live-streamed his attack at a mosque in New Zealand. Videos of the shooting were later circulated millions of times on social media, affecting even more users.

5 In fact, these risks have been talked about for some time. The word "Internet" entered Parliamentary lexicon in the early 1990s. By 1998, then-Senior Minister Lee Kuan Yew had warned that "the Internet is as much a purveyor of truth as it is of outright lies." He said this at the Asian Media Conference in Los Angeles.

6 But he also said, "Governments that try to fight the new technology will lose". In other words, we can't just walk away, shutter up the island and pretend the technologies do not exist. Instead, we must try and understand how the technologies work – even the

emerging ones that are difficult to grasp – put in guardrails to keep people safe, and help them reap the benefits of the technologies.

7 Mr Lee ended his speech with this advice, "…for a society to hold together, it needs institutions and high points which citizens look up to. The media has the responsibility to preserve some of these high points, or at least not to diminish them unnecessarily."

8 This was well before the era of social media. But there can be no mistaking the key thrust of Mr Lee's message – which is that any form of communication that captures so much attention of ordinary folks, shapes how they see the world and how they interact with one another, surely has a responsibility for what's being carried, and the impact they create.

9 Owners of online communications services profit from their users. They may not be the creators of all the content their users encounter, but most of them have accepted they cannot externalise the potential harms and do nothing to help. Even if they are driven by self-interest, they see the need to moderate the risks. How else will their users have the confidence to keep engaging digitally? Why should users trust services that pay no heed to their safety and well-being, that tear apart the communities they belong to?

10 In today's context where online harms are prevalent, building a safer digital world will be an uphill task. But giving up is not an option. As hard as it is, we must keep trying. The question is how?

11 Allow me today to share Singapore's approach. I must caveat that this did not come about as some grand design that was settled years ago. It came about as we were confounded with new problems and sought fresh solutions. Unlike when we were developing physical Singapore, there are no tried and tested approaches to reference, no playbooks to adapt, no off-the-shelf formulae to adopt. Thus, we have to invent new methods, and accept that they do not provide perfect answers in the first instance and we must keep trying to get better answers to the questions that remain. There are three key features to the approach. Let's refer to them as the 3 'As'.

12 First, the approach is to be **accretive**. Think of building blocks. You stack one on top of the other in order to reach higher. You don't try to get there in a single step.

13 We also have to **agglomerate**. It's a fancy way of saying to bring together, pull in partners and groups that can add something to our solution. The reason we have to do this is because digital is like an octopus-on-steroids, growing new tentacles all the time. We don't stand much of a chance unless we reach out and hear what people and businesses have to say, to enrich our understanding of the problems and possible ways of dealing with them. We have to be intensely curious and accept that many a times, the answer is to pull in even more stakeholders.

14 Third, and perhaps most importantly, be **agile**. We will not, and cannot, assume that what we have built is good enough. As kids or parents, we might have tried using wooden blocks to build towers. You build the base, then the next player removes a block, and the original tower becomes shaky again. Digital is somewhat like that. You think the tower is

strong, and then an emerging technology exploited by bad actors removes the stability, and you have to quickly insert new blocks to re-stabilise it. That's just the way it is.

Our accretive approach to regulation

15 Let me first elaborate on our **accretive** approach to regulation.

16 We are not the only ones in the world trying to keep our citizens safe from harms online. Australia and Germany have introduced new laws to do so. The UK and EU are currently developing theirs. Approaches to regulation may differ but as governments step up to meet this challenge, one thing is clear – it is unrealistic to cover everything at one go.

17 So, what are we doing in Singapore? We prefer a calibrated approach, taking time to understand the problem and then design targeted measures. At each juncture, we consult widely, often publicly and sometimes privately. The result has been a number of new laws.

a. For example, to deal with the prevalence of fake news online, which threatened social cohesion and trust between citizens and in government, we introduced the Protection from Online Falsehoods and Manipulation Act (or POFMA) to counter misinformation. It proved to be tremendously useful during the COVID-19 pandemic.

b. We saw how hostile information campaigns carried out online can fracture societies, we passed the Foreign Interference (Countermeasures) Act (or FICA).

c. Another law, the Protection from Harassment Act (or POHA) brings relief to victims who face harassment, both offline and online.

18 Our proposed Online Safety Bill will be debated in Parliament next week. We should see it as another building block towards a safer and more inclusive digital future. It will require Designated Online Communications Services with significant reach or impact to comply with Codes of Practice, including to implement measures to protect Singapore users against harms. IMDA would also be empowered to issue directions for all forms of Online Communications Services, to restrict access to egregious content that reach Singapore users. The only exceptions are if the communications are private.

19 We believe a targeted approach of having fit-for-purpose laws work better for us. If we attempt to cover all issues with just one single law, this will likely come at the cost of tools being too blunt. They may not be fit for purpose or effective as a result.

20 The Bill is therefore carefully scoped to include only the key risks Singaporeans are concerned with regarding online content. It does not attempt to cover everything. We fully expect that it will evolve as the risks in the online domain shift. Should the codes of practice need to be updated upon implementation, we will do so.

21 We will also take a phased approach to implementing the proposed measures. Our focus is now on Social Media Services given their significant reach and risks. As a next step, we will determine how best to tackle harmful content on other types of Online Communication Services.

We agglomerate ideas to remain relevant

22 But one could argue – does being accretive suggest a piecemeal approach, bereft of any understanding of the big picture? It's a valid concern. Like the tale of a few blind men each touching a different part of the elephant, if we are not careful, we have regulations that have no synergy, or worse still, are at odds with each other.

23 This brings me to the next point – how we **agglomerate** ideas. We reach out and attend dialogues like this; meet new people, exchange ideas and bring in more stakeholders to help us develop more holistic understanding as well as solutions to our challenges.

24 Two weeks ago, Singapore hosted the Singapore International Cyber Week. A broad spectrum of ideas was exchanged – from opportunities and threats in cyberspace, implementation of cyber norms, tackling ransomware, among others. There was clear recognition by participants that a collaborative, multi-stakeholder approach to counter threats in cyberspace is the way forward. No single entity has all the answers. Such is the nature of the digital domain. It knows no borders.

25 A multi-stakeholder approach is, in fact, not new to Singapore. It has been our *modus operandi*:

a. In the area of making data sharing secure: we collaborated with key stakeholders in the industry to conceive of and launch the Singapore Trade Data Exchange in June this year. Also known as SGTradex, it is designed to provide trusted, verifiable data from source. We are now working with key partners to drive adoption and expand its use cases.

b. I have also announced previously that we will be reviewing our Cybersecurity Act to strengthen our national cybersecurity posture. In doing so, we will consult a wide range of stakeholders to ensure that what we propose is sensible, forward-looking, and balanced. We look forward to working with the legal fraternity as part of this process.

26 In the formulation of the Online Safety Bill, we engaged a broad range of stakeholders, including members of the public, community, and industry groups. We received over 600 responses, which informed our approach to the Bill.

27 A survey by MCI in June 2022 found that about 8 in 10 Singapore residents were concerned with online harms, and almost 9 in 10 had encountered harmful online content in the past six months[1]. Sexual and violent content as well as cyberbullying were the top

[1] MCI study conducted online between 15 to 22 June 2022, with 1,053 Singapore residents aged 15 and above.

areas that respondents felt that young users needed the most protection from. These concerns were reaffirmed during the consultation process, where parents expressed concern over viral social media content featuring dangerous pranks and challenges that could be copied by their children. Guided by such concerns, measures were drawn up for designated services to have in place appropriate systems to address such harms[2].

28 Key stakeholders in industry were also engaged. Companies explained their unique business and operating models. It was reasonable for them to request that our proposed measures take these into account, and we will.

<u>Agility means keeping up with technologies as they emerge</u>

29 Even the most casual of observers know that technology does not stand still. We must therefore remain **agile**. Otherwise, the solutions we develop may become irrelevant when implemented.

30 This means continuing to keep an eye on emerging technologies, such as the Metaverse and Web 3.0. They will ignite new possibilities that are exciting. But they will also bring new challenges.

31 Due to the higher level of user immersion in the Metaverse, anti-social behaviour can have real-life impact, more than even the doxxing or cancel-culture experienced today. For example, anecdotally, users have reported being harassed on VR platforms – the sense of embodiment and immersion accorded by VR amplifies the psychological impact of such experiences.

32 Web 3.0 is understood to be the third evolution of the web, using blockchain as its core technology to decentralise the execution and verification of transactions. Yet the privacy accorded by blockchain, which shields users from scrutiny, is a double-edged sword. The general lack of Know-Your-Customer rules in this space has increased users' vulnerability to money laundering, fraud, and scams.

<u>Agility also means empowering users to seize opportunities and manage risks</u>

33 But **agility** is not restricted to just the writing of laws and regulations.

34 Agility also means moving quickly to equip people with new skills and tools to respond effectively to online harms. This is critical as it is impossible for the regulator to be everywhere, at every single moment, to protect everyone. We will not be as effective unless we also increase confidence and ability at every level of society. Through our public education programmes, we are doing everything we can to help people with skills and information to navigate digital technologies safely.

35 Some of you might have heard about the Digital for Life (DfL) movement which was launched in 2021. It brings together partners from the people, private and public (3P)

[2] In areas such as sex, violence, suicide and self-harm, cyberbullying, the endangerment of public health, as well as content facilitating vice and organised crime.

sectors to jointly develop solutions and galvanise the community to embrace digital learning as a lifelong pursuit.

36 Since the launch of the movement, our partners have kickstarted projects across multiple causes:

a. For example, Google has partnered IMDA and the Media Literacy Council to train 50,000 primary school students and their parents on online safety over the next 12 months.

b. Meta has partnered TOUCH Community Services to provide low-income families with essential digital life skills, such as how to use basic platforms as well as giving them cyber wellness tips.

37 As a movement, DfL does not only help people play defence. It goes upstream to promote digital inclusion. For example, telcos, social service agencies and community partners came together to collaborate on the Data for All initiative, which aims to provide digital access and connectivity to up to 30,000 persons in need.

Conclusion

38 Let me conclude.

39 Safety and inclusion in Digital Singapore are worthy goals. They reflect our long-standing values as a society where people don't live in fear of being attacked or violated, and those who need help get more support.

40 But these aims won't materialise by chance. Neither will they be achieved overnight. We will need steadfast commitment and thoughtful interventions including laws and regulations. But more importantly, it is the effort of everyone in society helping each other to gain confidence and stay safe online.

41 I thank Dentons Rodyk for your interest, and for organising this dialogue. I wish you all a fruitful day ahead. Thank you.

+++