

**Transcript of Opening Address delivered by Mrs Josephine Teo,
Minister for Communications and Information,
at ST Asia Future Summit (1 Nov 2022)**

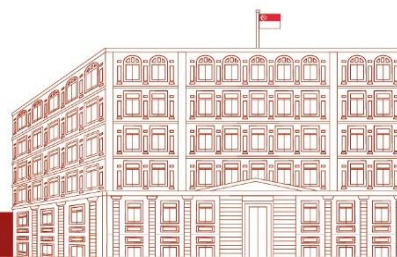
Mr Wong Wei Kong, Editor-in-Chief of the English, Malay, and Tamil Media Group of SPH Media

Mr Jaime Ho, Editor of The Straits Times

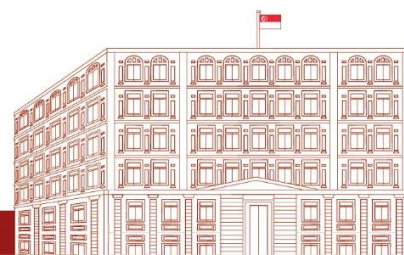
Mr Sunny Quek, Head of Global Consumer Financial Services at OCBC Bank

Colleagues and friends

1. Thank you for inviting me to join you for today's discussion. As its name suggests, this Summit focuses on Asia's future and among the many trends that we observed in our part of the world, one bears watching – that is, how quickly it is digitalising. If you consider in ASEAN alone with a population of about 660 million, about 350 million are already digital users. And 60 million of them were added just during the course of the pandemic. That is how fast the landscape is changing and how many people are coming on board.
2. So in the time that we have, I'd like to focus on the topic of trust in a digital age and more specifically, how digital trends have placed increasing strain on the trust ecosystems that support our societies, and what steps we might take to address this.
3. The last decade has seen a global decline in trust across nearly all institutions, including governments, the media, and corporations. The 2021 Edelman Trust Survey showed that pandemic-related fears and misinformation have accelerated this process. Globally, trust in all sources of information has dropped to record lows, with the largest loss accruing to governments.
4. The consequences of this are nothing short of dire. Most recently, we have seen the rise of anti-vaxxer movements. But even before the pandemic, pervasive cynicism towards government and media institutions have profoundly changed the world we live in. It fuelled the rise of populist movements worldwide, fed the growth of conspiracy theories such as QAnon, and precipitated era-defining events such as Brexit.
5. What has caused this loss of trust? It would be simplistic to pin all the blame on technology, but there is no denying that digital trends have exacerbated pre-existing issues, deepened or even created new fault lines in society.
6. Social media has made it possible for millions of people to live almost exclusively within their own echo chambers. In these silos, fringe views are not just insulated from criticism but can reinforce each other and become an alternate truth that people can believe in. Online anonymity and the power of virality have allowed falsehoods to spread faster than regulators can address them. At the same time, online scams are a growing problem; we also see emerging technologies such as deepfakes and AI-generated content being employed to deceive those who are taken in by their hyper-realism.

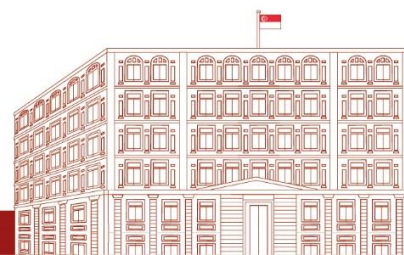


7. Unfortunately, internet culture does not always bring out the better angels in us. When interacting with those we disagree with on social media, we are often tempted to resort to performative name-calling and virtue-signalling that prevent good-faith discussions; and create a cancel culture that deepens social divides.
8. Left unchecked, the erosion of trust across societies will have dangerous consequences. If we as societies cannot agree on a bare minimum of common, shared facts, policymaking will be impossible. This infrastructure of trust is vital to public discourse and proper debates on issues that matter. It does not mean that we cannot disagree, nor we will not challenge each other's views. But it is a different situation altogether if arguments are advanced purely to stir up negative emotions, and distort or even disregard facts. Genuine discussions will fade away, to the detriment of society.
9. Against such a backdrop, how can we establish and protect an infrastructure of trust in our societies? There are no ready playbooks to copy. But there are pockets of good examples that are worth emulating.
10. The first is to try our very best to maintain effective government communications. In a fragmented and highly contested information space, this is much easier said than done.
11. As a bedrock factor, we should be honest in our communications with the public. Information must be released and updated quickly, before fake news has time to take root and embed a misleading narrative.
12. We have to reach out to people where they are, on platforms they are most comfortable with using, and not where we have been used to communicating.
13. We will also have to cater our communications strategies to different groups of people, who have varying levels of digital literacy and will prefer to consume information in diverse formats and languages. To illustrate this, one attempt by the Singapore government over the course of the COVID-19 pandemic was to push out regular updates on official government websites and social media such as the Gov.sg WhatsApp channel. At the same time, we also broadcast information through traditional channels such as print media, radio, free-to-air TV, and display panels in HDB estates.
14. The more difficult challenge comes when dealing with unpopular policies or decisions. It is often tempting to avoid presenting "hard truths" or to talk about difficult trade-offs that a government must make on behalf of society. And yet, failure to communicate on tough issues, in an honest way, must eventually lead to failure in governance. Honesty will often come at a price, but shying away is not the answer, because the costs borne by future generations will likely be higher as a result.
15. The emphasis on honest communications over the course of the pandemic managed to help us stave off the worst of the social effects. According to a Pew survey that was done earlier this year, Singapore – alongside Sweden and Japan – was among the minority of countries where people felt more united in the aftermath of COVID. In most other countries, it was the opposite – people felt more divided. Our pandemic communications and indeed our measures were not



perfect. But more so than in many countries, people in Singapore understood what was at stake and did their part to support our actions.

16. A second important plank of building the infrastructure of trust lies in laws and regulations, to protect citizens from harmful or misleading content.
17. The notion and necessity of regulation is not new. What has changed is the speed with which technology is evolving, and how this challenges the traditional concept of highly prescriptive, top-down regulation.
18. In this digital age, regulation will have to be agile and accretive. Agile – in order to respond quickly to new domains, such as challenges posed by the emergence of Web 3.0 and the metaverse; and Accretive – so we can tailor our regulations to address specific problems, without resorting to sudden, destabilising shifts in policy.
19. We will also have to transition from a prescriptive approach to focusing on the outcomes we hope to achieve. One example is our proposed Code of Practice for Online Safety, which we are introducing under our Broadcasting Act and debating in Parliament later this month. Instead of specifying how social media services should go about protecting users, we set out the outcomes they should achieve in relation to community standards, child protection, and user reporting. Depending on the features of their products, social media services can develop their own tools to achieve these outcomes, rather than overhauling their systems to meet very specific requirements.
20. The third lever is to encourage trust by design. We are all familiar with the start-up adage that is to “move fast, break things”. But now that we have seen exactly how things might break, whether in the form of harmful content, data breaches, or cybercrime, there’s good reason for a pivot from this approach.
21. These problems I mentioned dent trust and confidence in digital services that we increasingly see as indispensable parts of our lives. It has hence become critical for data and system owners to integrate safety and security as key priorities at the design stage of their services, so that users are protected from the outset. If we fail to do so, the level of distrust and lack of confidence will eventually cause people to hold back from engaging digitally and decide that they do not want the risks that come with it. A good example is how our banks in Singapore have introduced a “kill switch” for customers to freeze their bank accounts if they suspect their accounts have been compromised, as well as a deliberate delay in activation of certain changes to stymie fraudulent changes of personal details.
22. I also challenge all of us to consider how to incorporate *society* by design for our services. Building a trusted digital space is about more than legal rules and community standards – it is also about giving people the time and the tools to grow their confidence.
23. This will mean looking out for those who are vulnerable or less digitally-savvy. For example, we designed CDC vouchers so that people could access them via QR codes on their smartphones. But we also retained the option of using printed vouchers, so that those who didn’t have a smartphone were not stranded. Their numbers dwindle as they are nudged by their peers and digital ambassadors to go digital, but this process cannot be overly rushed. This ethos of



inclusivity is not something government can compel after the fact. Instead, it will have to be baked into the design of services that corporates deliver and make available to their customers.

24. It is also important to note that we can harness the power of digital to build trust. We recently launched our National Digital Trust Centre to lead our R&D efforts for trust technologies such as Privacy Enhancing Technologies and trustworthy AI. We have developed AI Verify, an AI governance testing toolkit that allows organisations to be transparent about their AI systems and build trust with their stakeholders. GovTech has developed OpenCerts and TradeTrust. These are platforms that leverage blockchain technology to allow for decentralised verification of documents and certificates.
25. The point is to not see digital as the enemy only, but to leverage its power to strengthen our infrastructure of trust. To put in place the building blocks I talked about, the government has to play a central role, as it is ultimately responsible for the safety of its citizens, whether offline or online. There are no short cuts or easy workarounds, and we will have to put in the hard work to maintain our trust ecosystems even as the technology evolves.
26. Yet any single government on its own cannot hope to address the complex, global issues thrown up in the digital domain. It is necessary and beneficial for governments to partner with companies and civil society to develop solutions.
27. We carry out extensive consultations with tech companies, citizens, and researchers when developing our regulations. We also started the Digital for Life movement last year. This initiative brings together Singaporeans from all walks of life to embrace lifelong learning and encourage all of us to co-create solutions to digital challenges.
28. Apart from collaboration across sectors, collaboration between governments is also critical. We must work together to share experiences and best practices, as the digital domain and its challenges cut across state boundaries. In fact, for digital, and especially cybercrime, no state or geographical boundaries are respected at all. Collaboration will therefore allow us to build consensus on what is needed for a trusted online space, and collectively set rules of the road for an increasingly contested domain.
29. To conclude, digital technologies, left on their own, can threaten to erode the infrastructure of trust which undergirds our societies, deepening divides and hobbling government.
30. But if we adopt a collaborative mindset and a nimble approach to policymaking, we can go beyond mitigating this threat to using digital to reinforce trust in government, in our institutions, and in each other. This is the hope we must have and the future we must try to build.
31. Thank you once again for inviting me, and I wish you very fruitful discussions ahead.

