Source: *The Straits Times,* pB3
Date: 3 April 2023

TikTok chief executive Chew Shou Zi testifying at a US Congressional hearing in Washington on March 23. The hearing serves as a reminder that virtually no one's data is safe – regardless of the nationality of the firm in question, says the writer. PHOTO: REUTERS

US action on TikTok will change social media and the Internet as we know it

The TikTok case represents a watershed on two distinct levels – as a symbol of US-China decoupling and with implications for the global datasphere

Alex Capri

As the dust settles from TikTok's Congressional hearing in Washington, United States lawmakers are set to move forward with a ban on the app in America.

This was a predictable outcome. It became apparent early in the five-hour public grilling of TikTok's chief executive officer, Mr Chew Shou Zi, who withstood a barrage of questions and accusations from both Republicans and Democrats.

At stake was whether TikTok could be fully divested of its Chinese investors and its majority owner ByteDance, and sold to an American buyer. The Congressional hearings focused on Beijing's national cyber security laws, which require Chinese companies to turn over data and information to the Chinese state apparatus.

Singapore was watching the hearing closely, not only because Mr Chew is a native son, but also because TikTok's fate in the US could set a benchmark for how the US might approach other Chinese companies, even those with subsidiaries or regional headquarters in other countries.

Chinese tech giants such as Alibaba Cloud and Tencent, for example, have set up regional data centres in Singapore, and some would argue that this might allow them to be insulated from the long reach of Beijing's laws. Or, maybe not, considering that Mr Chew's argument that US data would be stored in US data centres and managed by Oracle was summarily dismissed.

A CONTESTED BAN, AN UNLIKELY SALE

For 150 million American TikTok users, including well-paid content creators, educators, business owners – even US politicians who use TikTok to reach voters – a ban is seen as patently unfair and, probably, unconstitutional.

Just as the original ban on TikTok by the Trump administration, in 2020, was blocked by a federal judge, legal experts are predicting a long-protracted series of TikTok court battles.

But all of this is a moot point.

No sale of TikTok can take place without the approval of the Chinese government. TikTok's highly sophisticated algorithm and its proprietary AI, which determine which videos are served up to viewers, fall under China's laws on tech exports, which give Chinese regulators a final say on a sale of the company. And Beijing appears to have no desire to share this technology.

US-CHINA PLATFORM DECOUPLING

The TikTok case represents a historic watershed on two distinct levels. On the first level, it is another symbol of US-China decoupling. But on a second, overarching level, the TikTok case has placed a wider spotlight on the datasphere and the global digital commons.

It has highlighted a trifecta of existential issues facing states and firms, namely: rampant data insecurity, the need for better cyber defences, and, on an even grander scale, the issue of accountability for all social media platforms.

In the social media space, TikTok highlights the animus between China and the US and all the reasons why the two systems are incompatible.

With Chinese authorities having taken steps to firewall its people digitally from US influences, US reciprocal action should not come as a surprise.

Indeed, US lawmakers won't be able to disassociate present-day TikTok from Beijing's decades-old ban on American platforms, including Facebook, Google, YouTube, Instagram and WhatsApp. Beijing had selectively decoupled from the US long before a paradigm shift in Washington compelled lawmakers to adopt similar practices.

CHALLENGES IN THE GLOBAL DATASPHERE

On Capitol Hill, deep-seated fear of data theft has been decades in the making. It is the result of a long string of cyber intrusions.

In 2010, a series of WikiLeaks uploads revealed that American officials, as early as 2006, had been grappling, unsuccessfully, with rampant data theft from the US defence establishment as well as from a wide swathe throughout the corporate and academic sectors.

Forensic analysis covering a window of just a few years, from 2006 to 2010, revealed 30,000 confirmed hacking incidents and significant intrusions where hackers made off with a treasure trove of intellectual property, designs and blueprints for advanced weapons systems and leading-edge commercial and military research.

Individual data was regularly targeted, including hundreds of thousands of user accounts, user IDs and passwords at key institutions. In one instance, personnel records of more than 30,000 US Air Force officers were stolen.

The TikTok Congressional hearing demonstrated a woeful lack of understanding on the part of policymakers regarding the technology underpinning an app like TikTok. The knowledge chasm between regulators and innovators must be bridged. This will require the curation and onboarding of a wide range of good ideas and practices, regardless of whence they may come.

In 2013, Edward Snowden, a National Security Agency contractor, leaked classified documents revealing the extent of US science and tech activities involving electronic surveillance, hacking and digital tradecraft.

The conclusion: The datasphere has long been a virtual war zone.

Since the 2010 WikiLeaks and the Snowden incident, cyber intrusions have increased in scale and sophistication. No wonder, then, that the private data of 150 million American TikTok users has been the subject of so much heated debate.

THE DATA SECURITY QUESTION

On a much higher existential level, the TikTok hearing serves as a reminder that virtually no one's data is safe – regardless of the nationality of the firm in question.

The most vaunted cyber defences continue to be breached by a wide range of actors. Facebook, Instagram, YouTube and TikTok have suffered multiple breaches, which resulted in the theft of data of hundreds of millions of users.

Even WhatsApp, the encrypted messaging app, was breached by spyware created by the Israel-based NSO group, which resulted in the surveillance of journalists and human rights activists and other targets of authoritarian regimes.

The question is how to build a truly secure data environment, one that not only locks out a would-be intruder but also restricts access to only authorised people.

A good starting point is TikTok's own plan, Project Texas. Yes. The company has spent some US$1.5 billion (S$2 billion), legitimately trying to figure out how to effectively use third parties – in this case, US firm Qualcomm – to act as independent safekeepers of data.

The idea is similar to how a sound financial institution might safeguard a company's money, but without the systemic market risks. Such an endeavour would require the application of state-of-the-art data segregation, anonymisation and encryption.

TikTok's Project Texas also lays out groundwork for a more collaborative and active role of regulators, allowing them to vet company employees and enabling them to place representatives on the board of directors – which sounds eerily similar to the practices of China's regulators.

But the TikTok Congressional hearing demonstrated a woeful lack of understanding on the part of policymakers regarding the technology underpinning an app like TikTok. The knowledge chasm between regulators and innovators must be bridged. This will require the curation and onboarding of a wide range of good ideas and practices, regardless of whence they may come.

What is certain is a new regulatory environment will have to bring business and government much closer together. There will be increased tensions, but this new kind of symbiotic relationship can more effectively ensure greater data security, and ironically give wider latitude to trade and commerce.

ACCOUNTABILITY FROM SOCIAL MEDIA PLATFORMS

Finally, beyond issues of universal data insecurity and how to get government and business to reach the next level of effective data governance, TikTok has steered the conversation to the most pressing existential issue: accountability.

The big social media platforms continue to have an oversized impact on society. Public discourse on streaming video apps such as TikTok and YouTube, inevitably turns to issues of mental health, particularly as it pertains to younger people. It is near impossible to broach this topic without questioning social media's fundamental business model and the function of its algorithms.

The algorithms that power social media platforms are geared towards the direct advertising model. These algorithms continue to have a propensity to amplify extreme positions and to polarise users. Disinformation, hate speech, violence, outlandish conspiracy theories all make for more precise targeted advertising. Fixing this will require relooking at social media's fundamental revenue stream model.

All of this could come out of the March 2023 TikTok hearings in Washington, regardless of whether TikTok is banned or sold. The trouble is that banning one Chinese TikTok platform is an easier slogan to sell compared with the hard work needed to pass legislation to overhaul the social media giants.

As TikTok and other companies look to fortify the digital moat around their data, this will accelerate the fragmentation of cyberspace.

And why stop at the walling off of a database? What if a national 5G network can't be trusted? Here, large multinationals will work to seal off their communications network, as well, turning to companies like Starlink Internet to provide them with their own private satellite communications networks.

• Alex Capri is a Research Fellow at the Singapore-based Hinrich Foundation and a Senior Lecturer at the NUS Business School. He is the author of Techno-Nationalism: How It's Reshaping Trade, Geopolitics And Society (Wiley) due out later in 2023.