RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 102 – 19 October 2022

The Indian Government Ban on Chinese Apps and the Singapore Connection

By Asha Hemrajani

SYNOPSIS

The ban by the Indian Government of the widely downloaded multiplayer game Free Fire, has shone a spotlight on their banning of apps developed by Chinese companies and the subsequent fallout on Singaporean app developers.

COMMENTARY

At the behest of the Indian Home Affairs Ministry, MeitY (Ministry of Electronics and Information Technology) started banning mobile apps perceived or known to be originating from Chinese companies in June 2020. These apps include globally popular ones such as *SHAREit*, *TikTok*, *Weibo*, *WeChat* and *Free Fire*. The apps were banned invoking emergency powers under Section 69 of the Indian Information Technology Act, which enables the Indian central government to block access to any domain or app that is deemed to be a threat to national security. The first batch of apps to be banned has grown from 54 to over 200 today.

One of these apps is *Free Fire*, one of the most widely downloaded multiplayer games in the world, grossing over US$4 billion worldwide. However, *Free Fire* was not developed by a Chinese company, but by Garena, a subsidiary of Sea Limited, a tech conglomerate headquartered in Singapore. Sea was founded by a former Chinese citizen who is now a Singaporean. Sea is also partially owned by the Chinese internet and social media giant Tencent, which the Indian Government perceives to be linked to the Chinese Communist Party.

Another app which was banned is *SHAREit*, a file sharing app which was first developed by the Chinese IT giant Lenovo, before being spun off and run under a Singapore based technology company several years ago. Despite the spin-off, the app is widely described in the Indian press as a Chinese app.

What were the reasons for the ban?

The most commonly reported reason for this ban are the military tensions between India and China along the Sino-Indian border in 2020. However, even three years **prior** to the ban, the Indian Ministry of Defence had already issued an order requiring military personnel to remove Chinese apps from their devices due to security concerns that these apps may transfer data belonging to their users, from India or elsewhere, to corporate or government entities in China. This data could include identities, locations, messages, facial recognition data, and other personal information.

For instance, *TikTok*, the popular video hosting and social media service owned by Chinese company ByteDance, clearly states in their Terms of Service that they may "share your information with other members, subsidiaries, or affiliates of our corporate group", many of which are based in China. China's National Intelligence Law, enacted in June 2017, stipulates that Chinese businesses could be required to hand over information to the Chinese government. The Law includes Article 7 which requires organizations and citizens to "support, assist and cooperate with the state intelligence work", and Article 10 which makes the National Intelligence Law applicable to Chinese businesses operating outside of China.

Yet another security concern revolves around the several serious software vulnerabilities found in the *SHAREit* app as reported by global IT security giant Trend Micro. These vulnerabilities if exploited, could have led to "remote code execution" allowing the execution of malicious code or leakage of sensitive data from the devices in which the app was installed.

What has the ban achieved?

Given the massive size of the Indian market as well as the popularity of Chinese apps amongst the young mobile-savvy netizens in India, the ban has in some cases hit the bottom line of the app developers. After the ban, Sea shut down its operations and laid off employees in India. Sea which had, at one point, been described as the world's best performing stock by a well-known stock analyst in Singapore, has seen its stock price plunge. The banning of the game *Free Fire* in India is said to have contributed partially to an overall massive 75% drop in the Sea share price. Sea also announced a withdrawal of another of its subsidiaries (e-commerce entity Shopee) from India mere months after launching.

The ban has, on the other hand, spurred on innovation in app growth and development amongst domestic developers in India, with a flurry of new homegrown apps springing up to take the place of banned Chinese apps. Some popular replacements include *Jio Switch* as an alternative to *SHAREit* and *Josh* as an alternative to *TikTok*.

However, there has not been a complete replacement of Chinese apps such as messaging apps like *WeChat*, that require significant market share penetration and scale in order to succeed. Young Indian consumers have successfully gotten around the government ban and are continuing to use certain Chinese apps via virtual private networks (VPNs).

What does the ban mean for Singapore?

Although India's ban was targeted at Chinese apps, the Singapore companies that developed *SHAREit* and *Free Fire* are also affected because of perceived links to Chinese entities. This illustrates that Singaporean companies that have significant investment from or connection to Chinese entities may be targeted by other nations due to rising suspicions of Chinese companies.

To reduce these risks, app developers and their owners will need more transparency and stricter corporate governance. The press has described Sea's founder as secretive, and also reported that "fund managers have urged Sea to be more transparent about its strategy and numbers".

App developers will also need to manage data sovereignty. Although Sea declared in March 2022 that it does not transfer or store data of Indian users in China, governments may not be satisfied with statements alone and may require, for instance, strict compliance programmes incorporating robust controls that provide clear demonstrable proof that data is not being transferred out of the country.

Asha Hemrajani is a Senior Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg