NEPCAP
POLICY BRIEF

uclan
University of Central Lancashire
Asia Pacific Studies

Volume 2020, N.1

Chinese social media applications: Privacy and data security implications

Filip Jirouš

Chinese social media and other types of applications have long dominated the Chinese internet ecosystem and also the Chinese diaspora. Now, applications and digital tools owned by entities registered in China have started to expand beyond these traditional spaces. The implications and potential risks brought by using such products, with regards to the Party-state influence over tech companies and a track record of data abuse, could be significant. Governments and private entities should increase their awareness of potential data exploitation by third parties, primarily those with links to authoritarian regimes with a history of information control and manipulation.

Privacy and data security are becoming important issues in modern societies as the world becomes more dependent on the virtual space. From government hacks to ransomware attacking hospitals and other parts of critical infrastructure until recently believed to be immune to such 'invisible' threats, cybersecurity in general should now be reviewed both at a personal and an institutional level.

Many digital and tech giants have, in the recent years, been involved in data breach and data abuse scandals. The most famous one would probably be Cambridge Analytica, but even 'smaller' players, such as the Czech anti-virus software developer Avast, have been caught exploiting user data. But nowhere is this practice as widespread as in China, where individual data protection regulation (or its enforcement) and consumer awareness are rather small-scale. It is well documented that Chinese companies are storing their user data on unsecured servers. Such servers have been accessed easily by Western hacktivists on several occasions (Udemans 2019).

Most disturbing is the scope of the Chinese government's access to data stored by supposedly private companies such as Tencent. There have already been many cases of local authorities swiftly responding to private conversations on Chinese social media apps and persecuting the authors of what has been classified as 'illegal' content. The most famous example in recent months is possibly the repression of Dr Li Wenliang and his seven colleagues when they discussed the discovery of coronavirus on the Chinese communication app WeChat (Zidan 2020). Other abuse involves the Islamic text-reading app Zapya developed by a Beijing-based start-up in 2016. Its user data was later used to target Uyghur and other Muslims in Xinjiang who had been using the app to read and share religious texts with friends and family. Research among the Chinese diaspora in Western societies also shows that using WeChat and other Chinese social media apps by overseas Chinese can lead to personal freedoms being limited and democratic processes being threatened (Cook 2020).

The PRC government's intention to exploit user data for various purposes can be seen in the recent spike in industrial espionage cases involving Chinese citizens, some with government or military links. The Equifax hack, involving massive leaks of citizen data, is more evidence, being allegedly conducted by four Chinese military officers. Government hacks traced to the Chinese Party-state have been on the rise even in non-traditional spaces such as the CEE (Justice 2020; National Cyber 2020).

PRC-related data security risks are not limited to companies with Chinese ownership. A recent incident involving the video conferencing tool Zoom showed that even companies with no Chinese ownership can put their users' data privacy at risk by outsourcing research and development and data traffic to China Murphy (2020).This case should give us even more pause for thought, considering users were not informed about this until Canada-based digital research organization Citizen Lab released its report mapping Zoom's data traffic.

Some countries have already become aware of the risks posed by PRC-linked software and hardware. Among the Western countries sensitive to Chinese tech, Australia and the USA are most prominent. Their treatment of the Chinese short video platform TikTok and Chinese social media clearly shows concern about the security implications of such apps' usage, especially among military members and defense officials. In stark contrast, Europe neglects these issues, as documented by European soldiers posting videos (including what seems to be on-duty) on TikTok and possibly using even other apps linked to authoritarian regimes intent on exploiting the gathered data (Facebook 2020).

Governments, international bodies and citizens should be more protective of their data security in general, but even more so when their data can be vulnerable to exploitation by authoritarian regimes. Lack of cybersecurity and data security can have serious implications for defense, company competitiveness, personal freedom and the democratic processes of free societies.

Considering the data presented above and its possible implications, I suggest the following measures:

1. European security forces should consult with their democratic allies in the US, Australia, and elsewhere with regards to social media (and other) applications and tools that are linked to authoritarian regimes. They should apply the necessary measures to restrict unsecure usage of such apps, when there is a potential for the gathered data to be exploited to compromise security and operational capacity.
2. Governments should protect the data security and privacy of its institutions and citizens by verifying companies' data policies and making sure local data is stored in a jurisdiction which has adequate privacy and data security regulations. This is especially relevant when that data can be accessed by companies and other entities linked to authoritarian regimes.
3. Governments and private entities should invest more into research and education about data privacy and the potential risks of personal or institutional data exploitation.
4. Similarly, cybersecurity should be upgraded both on personal and institutional levels in a world that is rapidly progressing towards major dependency on the virtual space. It is to be expected that this process will be significantly accelerated as a result of the current coronavirus pandemic.

Social media, and digital applications in general, linked to authoritarian regimes, pose an increasing risk for a modern society which is heavily reliant on virtual spaces for economic, social, political, cultural and other exchanges. The increasing amount of data available online and the growing range of tools available for analyzing the data for different purposes should be considered an important issue over the next few years. Both governments and private entities should take the matter seriously and apply appropriate measures to mitigate the risk of data and privacy breaches. Weak cyber security exposes potential targets. The risk quickly spreads, however, to any entity that interacts with the target.

References:

Chris Udemans (2019) *Another unsecured server in China found containing trove of personal information. Available at https://technode.com/2019/07/10/china-trove-personal-data-open/ (Accessed 7 April 2020).*

Ahmed Zidan (2020) *Q&A: Citizen Lab documents Chinese censorship of coronavirus keywords. Available at https://cpj.org/blog/2020/03/citizen-lab-chinese-censorship-coronavirus.php (Accessed 7 April 2020).*

Sarah Cook (2020) *Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017.* Available at *https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone* (Accessed 7 April 2020).

Department of Justice (2020) *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax*. Available at *https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking* (Accessed 7 April 2020).

The National Cyber and Information Security Agency (2020) *Report on the state of cyber security in the Czech Republic in 2018.* Available at *https://www.nukib.cz/download/publications_en/report-czech-cyber-security-2018-en.pdf* (Accessed 7 April 2020).

[1] Hannah Murphy (2020) *Zoom admits user data 'mistakenly' routed through China.* Available at *https://www.ft.com/content/2fc518e0-26cd-4d5f-8419-fe71f5c55c98* (Accessed 7 April 2020).

Sample of military videos on TikTok Eesti (Facebook page): https://www.facebook.com/tiktokeesti/videos/553025355251321/ ; https://www.facebook.com/tiktokeesti/videos/190952875340859/ (Accessed 16 June 2020).

Filip Jirouš. A sinologist from Prague's Charles University. For the last three years he has been working at Sinopsis.cz, a China-focused think-tank based in the Czech Republic publishing both in Czech and English to inform local and global audiences on Chinese-related issues and consulting politicians on policy towards China. Filip specializes on Chinese United Front Work in Europe, China's Digital Leninism and covers the surveillance state in Xinjiang.