CHINESE APPLICATIONS AND DATA SECURITY IN THE 21st CENTURY

*Ishita Dutta**

INTRODUCTION

Chinese innovations and technological development have been rapidly increasing, the growing power of China has also exploited mobile phone applications as a tool for spying and surveillance across the world. As data has become one of the most important elements of national security across the world, data security is a crucial part of security studies and Chinese companies have been investigated for spying on countries and for collecting data through their applications across the world. This paper is important to measure the security threat imposed by Chinese applications to understand the future of security studies.

The growing power of China, technological advancement, and projects like Belt and Road Initiatives (BRI) also imposes a threat to the world. The laws under Chinese leader Xi Jinping also support the data collection and spying through Chinese applications. The paper also identifies the importance of data sovereignty and the failure of Chinese tech giants to guarantee data security around the world. China's rise as a superpower can be estimated by the wide web of data collected.

The digital element of the BRI threatens the data security of the countries[1]. Chinese tech giants like Tik Tok and Huawei are banned in countries for stealing data. The role of Chinese applications and data security in security studies can be regarded as a threat to sovereignty and digital authoritarianism by the Chinese. At least six of the ten most popular Chinese apps, including Helo and Shareit as well as browsers such as UC Browser, ask users to provide access to camera and microphones on their smartphones even when such access is not required, the study found[2]. This paper drawing understanding of Chinese applications as a threat to the security of countries, the use of applications by Chinese governments as a tool for surveillance and spying on countries, surveillance within China and technology advancement for governance, understanding the reason behind banned applications, and laws in China supporting spying abroad.

* ***The Author is a student at the Jindal School of International Affairs and Research Intern at the Centre for Security Studies, JSIA.***

[1] LY, B. (2020). Challenge and perspective for Digital Silk Road. Cogent Business & Management, 7(1). doi: 10.1080/23311975.2020.1804180

[2] Sangani, P., & Khan, D. (2020). Chinese apps seek excessive information from users: Survey – The Economic Times. Retrieved 13 October 2020, from https://m.economictimes.com/tech/internet/chinese-apps-seeking-way-more-information-than-needed-survey/amp_articleshow/67633562.cms

CHINA AND SURVEILLANCE APPS

Globalization and the rising power of China have exposed the data of millions of users to tech giants in China. The applications like WeChat and TikTok have been banned in parts of the world and investigated in some. Many other Chinese applications are under review for stealing data and spying on countries outside China. Other applications like Alibaba, PUBG Mobile, CamScanner, and as many as 118 Chinese applications have been banned in India alone[3]. The Indian authorities claimed to have credible information to ban the applications as they impose a security threat to the nation. WeChat has been banned by countries across the world for security reasons, but the data collected by WeChat or other Chinese applications impose a more serious threat of data marketing and is a threat to the data sovereignty of a country[4].

TikTok that operates outside China is still seen as a counterintelligence application by China in the United States and the United States has launched a national security investigation on TikTok. Although TikTok has denied all claims of data misuse and has denied any ties with Chinese law imposed on TikTok's data, it has still been banned in India after the faceoff with China in the Eastern Ladakh[5]. Four major threats imposed by TikTok that has led to the policymakers in the United States decide to ban the application are: first, TikTok can collect data from government employees in the United States that pose a threat to the national security, second, the application can also collect data of citizens of the United States that could be used as a tool to collect data, shape minds and alter election results, thirdly, TikTok application can also be used to spread misinformation and creating a public discourse that is uncensored and does not involve government authorities and finally, the application has altered information on Hong Kong in the favour of the Chinese government, that can cause speculation about China's involvement in TikTok's data collection.

Chinese applications and tech companies are not looked at as an independent entity in China due to a lack of institutionalization checks which makes data security a major issue for Chinese companies abroad. Many applications have also distanced themselves from Chinese companies to stay in business. The Chinese government plays a very important role in data collection by tech companies as the state and companies in China have a collaborative front. Data is a strategic asset to China, and it threatens the security of many countries across the world. Many countries fail to trust Chinese companies in data security as there is a lack of transparency and accountability in China by the government. The sanction imposed against Chinese applications

[3] chinese apps banned: Here's the full list of 118 Chinese mobile applications banned by the government. (2020). Retrieved 7 October 2020, from https://www.google.com/amp/s/m.economictimes.com/tech/internet/heres-the-full-list-of-118-chinese-mobile-applications-banned-by-the-government/amp_articleshow/77892540.cms

[4] Xiao, E. (2020). China's WeChat Monitors Foreign Users to Refine Censorship at Home. Retrieved 6 October 2020, from https://www.wsj.com/amp/articles/chinas-wechat-monitors-foreign-users-to-refine-censorship-at-home-11588852802

[5] Meakem, Táíwò, Cibralic, Mackinnon, Jones, & Agrawal et al. (2020). Why Is India Banning China's TikTok?. Retrieved 10 October 2020, from https://foreignpolicy.com/2020/07/02/india-banning-chinese-mobile-apps-tiktok-tech-market/

and tech giants will play an important role in shaping international, political, and economic relationships.

DATA COLLECTION

A study conducted by the Economic times found out that on average, these apps transfer data to around seven outside agencies, with 69% of the data being transferred to the US. TikTok sends data to China Telecom; Vigo Video to Tencent; BeautyPlus to Meitu; and QQ and UC Browser to its parent owned by Alibaba[6]. The collected data is not confirmed to be used for the Chinese government but there has been information for the data to be stored in Singapore. The data collected by the applications include face selfies, preferences, personal information, audio recording, etc. that can be easily sold to e-commerce giants in China for advertisement. The data is not secured in China, in the year 2018, a number of data thefts in China took place. The biggest leak in five years was discovered in August when 130 million customers of Huazhu Hotels Group realized their data was being sold online for 1 bitcoin[7]. This was followed by a data leak of 30 million users of the dating app Momo – the kind of app that takes a lot of data about the user, and this was revealed in 2019. Hackers stole the personal information of nearly 5 million people from several Chinese online ticket reservation platforms. The data collected by these applications can track user's locations, preferences to create an advertisement, and personal information. Apart from this, Chinese applications can also be installed in government employee's phones, the data on these phones may contain sensitive information about the country's security. Some applications seek excessive information about the user that is not required but some take personal sensitive information about the user related to their identity, phone number, etc. All this database can be accessed by the Chinese authorities that impose a greater threat to the country's sovereignty.

LAWS IN CHINA AND SURVEILLANCE APPS

The National Intelligence Law came into effect on 27th July 2017 that has caused a lot of controversies and fear in countries. Especially, Article 7 under China's National Intelligence Law that allegedly poses a threat to data security. The reason for fear is also the overpowering role of the Chinese Communist Party (CCP) in companies and tech giants of China. Article 7 under the National Intelligence Law of the People's Republic states "any organization or citizen shall support, assist and cooperate with the states intelligence work in accordance with the law, and keep the secrets of the national intelligence work known to the public. The state protects

[6] Sangani, P., & Khan, D. (2020). Chinese apps seek excessive information from users: Survey - The Economic Times. Retrieved 13 October 2020, from https://m.economictimes.com/tech/internet/chinese-apps-seeking-way-more-information-than-needed-survey/amp_articleshow/67633562.cms

[7] TechNode. 2020. *Leaked Data From Chinese Hotel Chain May Affect 130 Million Customers · Technode*. [online] Available at: <https://technode.com/2018/08/28/huazhu-hotels-data-leak/> [Accessed 13 October 2020].

individuals and organizations that support, assist, and cooperate with national intelligence work[8]."

The National Intelligence Law of China not just oblige people of China to support the government in a matter of national security but also imposes a threat to the data of countries abroad. Cybersecurity experts analyze the National Intelligence Law as a threat to data security and many countries have set up an investigation against Chinese applications, tech companies, and other Chinese companies due to Article 2, Article 7, Article 11, and Article 14 under National Intelligence Law.

The National Intelligence Law is crucial to understand the legal support, national security importance, and relationship between state and organizations/ companies in China. Though Chinese companies and officials have come forward to give clarifications under the National Intelligence Law, data security and its increasing importance are resulting in countries taking preventive measures against Chinese companies. The government in China does not limit its power to citizen's or company's privacy which makes it difficult for countries abroad to trust Chinese tech giants with their data[9].

BANNED APPS ACROSS THE WORLD

Chinese cyberspace is one of the most surveilled in the world and the censored content through Chinese applications makes data security a priority for countries. China's surveillance and censorship have been researched with applications like WeChat.[10] Many countries across the world are struggling to secure data and applications can access mobile data that makes data security a more complex task with the involvement of foreign entities on phone applications, therefore data sovereignty becomes a necessity for security and national interests.

India banned 118 Chinese applications in 2020 over the national interest that included famous applications like PUBG MOBILE, WeChat, UC Browser, Shareit, and many more over the engagement in activities which are prejudicial to the sovereignty and integrity of India, defense of India, the security of the state and public order.[11] Chinese applications are expanding outside Chinese cyberspace and collect data from millions and billions of foreign users. Chinese

[8] (2020). Retrieved 10 October 2020, from https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf

[9] Understanding the National Intelligence Law of China: Why India banned Tik Tok?. (2020). Retrieved 10 October 2020, from https://diplomatist.com/2020/09/05/understanding-the-national-intelligence-law-of-china-why-india-banned-tik-tok/

[10] Xiao, E. (2020). China's WeChat Monitors Foreign Users to Refine Censorship at Home. Retrieved 6 October 2020, from https://www.wsj.com/amp/articles/chinas-wechat-monitors-foreign-users-to-refine-censorship-at-home-11588852802

[11] chinese apps banned: Here's the full list of 118 Chinese mobile applications banned by the government. (2020). Retrieved 7 October 2020, from https://www.google.com/amp/s/m.economictimes.com/tech/internet/heres-the-full-list-of-118-chinese-mobile-applications-banned-by-the-government/amp_articleshow/77892540.cms

applications like WeChat and TikTok have been accused by many users over the restriction of information sharing in various parts of the world. This is one of the major reasons for countries to ban Chinese applications and secure their data.

Chinese tech companies expanding globally, expose nations to a wider threat of censorship over information globally. The national security of China is more important than the privacy of its citizens, the same pattern can be used to extract data from Chinese organizations for national security. China has taken steps to remove non-sanctioned online content with the help of Tencent, Alibaba, and Holdings Ltd. to increase surveillance on citizens which have also censored content abroad for national interests and therefore have been investigated and even banned in some parts of the world.

The Chinese applications sensor data against cyber terrorism risk but the regulation of censorship has been centric to China's interest which makes these applications even more questionable. Chinese tech giants have also produced affordable phones that intelligence has warned as a device for spying and many countries have restricted government employees from buying Chinese phones or installing Chinese applications.

SURVEILLANCE WITHIN CHINA

Chinese applications and growing technical innovations have also played a crucial role in surveillance within China. Applications on mobile phones are used by the state as a tool for surveillance and to control citizens. A particular mobile application IJOP (Integrated Joint Operations Platform) is an application that helps police trace people and analyzes data to know, control, and servile people of China[12]. China has face recognition software, phone scans and online activity monitoring for all people and the technological advancement in China is creating more advance technical governance through surveillance. Chinese applications like WeChat follow algorithms and prevent users from sharing messages including keywords. The invention of censorship applications should be looked at as a threat, as Chinese companies expand globally, the same applications can be used to collect data and censor information in favor of China. China has also banned websites that criticized the Chinese Communist Party (CCP) along with 200 million cameras for surveillance[13].

SURVEILLANCE THROUGH TOURISTS

Another role of Chinese applications is to collect data from the tourist's phone that come to China. Chinese border police are secretly installing surveillance applications on the phones of tourists and visitors especially in the Xinjiang region to track movement and even get personal

[12]Doffman, Z. (2020). Xinjiang: How China Uses A Spying Smartphone App To Automate Citizen Oppression. Retrieved 6 October 2020, from https://www.forbes.com/sites/zakdoffman/2019/05/02/xinjiang-how-china-uses-a-spying-smartphone-app-to-automate-citizen-oppression/amp/

[13] China's surveillance app | ShareAmerica. (2020). Retrieved 7 October 2020, from https://share.america.gov/chinas-surveillance-app/#:~:text=In%20China%2C%20apps%20also%20are,(Integrated%20Joint%20Operations%20Platform).

data of tourists.[14] The applications designed by Chinese authorities scan data to find problematic content, these applications can also cause damage to the security and privacy of people downloading the applications. Around 100 million people visit Xinjiang every year, secretly installed applications can collect data and invade the privacy of millions of tourists across the world. The human rights authorities have identified the harmfulness of these applications, but the growing power of China and technical advancements impose a similar threat of data security through Chinese applications and threatens data security.

TECHNOLOGY AS A WEAPON

Technology and data are playing the role of weapons in the 21st century. The new dimension of security studies is data and privacy because of the growing technological advancement. Technology has endangered the freedom and privacy of billions of users; this makes it even more important for countries to investigate applications and companies for data security and privacy of its citizens. The Chinese applications and tech companies are looked like a threat to national security due to cybersecurity findings on data collection and other factors. The debate on data security re-emerged with 5G and Huawei, many countries including the United States, Japan, New Zealand, and many others have imposed restrictions on Huawei over security threats under data safety. Another threat to data security is the mobile phone itself, the smartphones sold in India are majorly made in China and the information harvested by these smartphones impose a great threat to India's sovereignty and security.

The surveillance and data collection are used as tools for spying on many country officials and are used to understand nations and their national interests and within China, the technological advancements are securing China's even more. The Chinese applications are taking more and more cyberspace and the increasing accusation of spying and data collecting is creating insecurity. The digital aspect of Belt and Road is important to understand the growing interest of China in cyberspace. The human rights watch (HRW) also exposed information of Chinese applications and invasion of privacy within China.

CONCLUSION

The paper covers the dimensions of Chinese mobile applications as a threat to national security for many countries. It reasons the ban on Chinese applications and draws an understanding of the consequences of international relations. The role of data security is increasing drastically in the 21st century due to growing technological advancement and the growing role of data in shaping the world. The increasing influence of the Chinese Communist Party (CCP) along digital transmission and cyberspace has resulted in investigations and even ban of Chinese applications across the world. Technology has endangered the freedom and privacy of billions of users; this makes it even more important for countries to investigate applications and companies for data security and privacy of its citizens. Countries need to take measures for

[14] Chinese border guards put secret surveillance app on tourists' phones | China | The Guardian. (2020). Retrieved 9 October 2020, from https://amp.theguardian.com/world/2019/jul/02/chinese-border-guards-surveillance-app-tourists-phones

data security and build safer cyberspace, there is a need for the more active involvement of national intelligence to explore and secure the data security studies.