CENTRE FOR AIR POWER STUDIES

In Focus

New Delhi

CAPS InFocus: 41/2022

12 July 2022

Shanghai Police Database for Sale: Breaches, Bruises, and China's Data Dilemma

Divyanshu Jindal

Research Associate, Centre for Air Power Studies

Keywords: Cyber, Cybersecurity, Breach, China, Surveillance.

Image Source: BBC

Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS]

On June 30, 2022, a user named 'ChinaDan' on the online hacking forum 'Breach Forums' offered around 24 terabytes (TB) of data from the Shanghai National Police (SNP) database.[1] This revelation has taken the world by storm. The offer was priced at 10 bitcoins (around USD 200,000) and included a sample of 750,000 data entries from the database.[2] The Wall Street Journal and CNN-linked reporters have confirmed the authenticity of the data by cross-checking the information with some of the victims that were listed in the sample.[3] The claim that the 24 TB file exists has also been authenticated.

A data breach of this magnitude, in terms of the number of victims, is not a first. In December 2016, it was revealed that in August 2013, around 3 billion Yahoo accounts-related data was exposed.[4] In November 2019, an Alibaba-related breach impacted 1.1 billion pieces of user data, while a Facebook-related incident in the same year exposed information related to more than 530 million Facebook users.[5] The year 2020 witnessed a Sina Weibo (China's largest social media platform) related breach which gave the hackers details on 538 million Weibo users.[6] And in June 2021, LinkedIn users' data was posted on a dark web forum, which impacted 90 per cent of its users – around 700 million.[7]

The investigations related to the Yahoo breach revealed that while the attackers were able to access account information such as security questions and answers, other sensitive datasets like plaintext passwords, credit card details, and bank details were not stolen. In the Alibaba breach, the attacker collected customer data like usernames and phone numbers from the Alibaba shopping website. Similarly, the LinkedIn, Facebook, and Sina Weibo data contained information including email addresses, social media details, phone numbers, and geolocation records.

While the above breaches provide significant abilities to curate social engineering attacks on the victims, it can be argued that these breaches would not be enough to coerce the victims through blackmailing or intimidation. However, the SNP breach is much more significant.

It has been estimated that this breach has not only exposed details like names, addresses, and mobile phone numbers, but also sensitive information like national identification numbers, police records like case details, as well as medical records. The breach has also allegedly exposed the data detailing user activity on most popular Chinese online and social media platforms, including the information related to minors.[8]

China's severe domestic surveillance and censorship mechanisms are widely known. Its unique 'social credit system' seeks to develop a national credit rating and blacklist through a unified record system to track the 'trustworthiness' of Chinese businesses, individuals, and government institutions. For this, Beijing collects vast troves of data on its citizens through both government and private mechanisms. Taking advantage of its technical expertise, China has also exported round-the-clock surveillance and mass data collection technologies to other countries in recent years.

The SNP database breach is also not the first instance when mass surveillance data has been exposed. In February 2019, a Chinese company operating facial recognition systems was breached, exposing the personal details of 2.5 million Chinese citizens, including the location data of the last 24 hours.[9]

Interestingly, a recent report by VPN service company Surfshark highlighted that the number of people affected by personal data breaches fell by 95 per cent in the last year.[10] While personal data like passwords, email addresses, and credit card details of nearly 500 million people were breached in the first quarter (Q1) of 2021, the Q1 2022 figures stood at just 18.2 million. The Surfshark analysis said that Russia was the only country in 2022 that witnessed a rise in users affected by data breaches, with 3.55 million victims in Q1 of 2022. The SNP breach has turned these figures upside down.

In 2021, two new laws dealing with privacy and data security in China came into force that appended its 2017 Cybersecurity Law. The new 'Data Security Law' and the 'Personal Information Protection Law' aim to regulate data localization, data export, and data protection requirements.[11]

According to a readout from the Chinese official Xinhua News Agency, President Xi Jinping had stressed the necessity to "safeguard China's data security, protect personal information and business secrets, and promote the efficient circulation and use of data so as to empower the real economy", in a high-level government body meeting less than two weeks before the breach came to light.[12]

With data now regarded as the new 'oil' and its importance well recognized for both the governance and sustenance of any country, the SNP breach has arrived as a bruise to Beijing's psyche and its ability to safeguard sensitive data.

There is speculation that the breach might have been caused due to a compromised cloud service provider. In China, the three biggest cloud services are Huawei Technologies, Tencent Holdings, and the Alibaba Group.[13] These are also among the biggest cloud service providers across the world. In case the blame for the breach comes to their end, they will face bruising as well.

Data breaches also impact the psyche of the population by endowing the data holders with the ability to manipulate how people behave and feel.[14] Since the current incident came to light, Chinese social media has been abuzz with restless citizens worried about their medical, police, and social media records lying exposed in the public domain. To silence these discussions and the rising panic, Beijing has censored words like ‘Shanghai data leak’ from its cyberspace.[15]

Incidents of data breaches have the capability to severely impact the functioning and reputation of both the government and private sector. With a high extent of vagueness between the two in China, the breach will have an exponential impact.

The SNP breach has once again brought to prominence the debates around Chinese censorship, surveillance, and mass collection of data. As Xi Jinping looks forward to a unprecedent third term, data breaches are bruises that create a data dilemma for Beijing. Other nations interested in establishing an ecosystem for mass surveillance and data collection similar to China should consider the ramifications of such ambitions as well. The control endowed by data can turn into chaos as well.

NOTES:

[1] "Alleged Chinese police database hack leaks data of 1 billion", *The Indian Express,* July 6, 2022, https://indianexpress.com/article/world/alleged-chinese-police-database-hack-leaks-data-of-1-billion-8011433/. Accessed on July 6, 2022.

[2] Ibid.

[3] Catalin Cimpanu, "China faces its first truly mega-leak", *Risky Business News,* July 6, 2022, https://riskybiznews.substack.com/p/risky-biz-news-china-faces-its-first. Accessed on July 6, 2022
.

[4] Michael Hill and Dan Swinhoe, "The 15 biggest data breaches of the 21st century", *CSO ASEAN*, July 16, 2021, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html. Accessed on July 6, 2022.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] "Alleged Chinese police database hack leaks data of 1 billion", n. 1.

[9] Kate O'Flaherty, "China Facial Recognition Database Leak Sparks Fears Over Mass Data Collection", February 18, 2019, https://www.forbes.com/sites/kateoflahertyuk/2019/02/18/china-facial-recognition-database-leak-sparks-fears-over-mass-data-collection/?sh=59061f96fb40. Accessed on July 6, 2022.

[10] Claudia Glover, "Personal data breaches are falling – except in Russia", *Tech Monitor,* April 15, 2022, https://techmonitor.ai/technology/cybersecurity/personal-data-breaches-are-falling-except-in-russia/. Accessed on July 6, 2022.

[11] "China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies", *Skadden*, November 3, 2021, https://www.skadden.com/Insights/Publications/2021/11/Chinas-New-Data-Security-and-Personal-Information-Protection-Laws. Accessed on July 6, 2022.

[12] Sarah Zheng, "Shanghai Data Breach Exposes Dangers of China's Trove", July 5, 2022, https://www.bloomberg.com/news/articles/2022-07-05/hacker-s-record-theft-claim-exposes-dangers-of-china-data-trove. Accessed on July 6, 2022.

[13] Ibid.

[14] Yuval Wollman, "Why CISOs should pay more attention to geopolitics", *UST,* March 1, 2022, https://www.ust.com/boundless/why-cisos-should-pay-more-attention-to-geopolitics.html. Accessed on July 6, 2022.

[15] "Alleged Chinese police database hack leaks data of 1 billion", n. 13.