



**By: Paul Frenken**

Many of us watched the CEO of TikTok, Shou Zi Chew, give testimony to congress a few months ago. The line of questioning only highlighted how much Congress really does not understand technology, at best it made them look naive and at worst, morons. Their main line of questions focused on privacy issues and if the Chinese Government had access to American data. Chew throughout the line of questioning continued to emphasize that data is not hosted in China. He however, never really answered the question if the Chinese government could gain access to the data.

He conveniently left out the fact that under Chinese law TikTok is obligated to allow government access to company data. Currently there are 3 Chinese laws, National Intelligence Law of 2017, Data Security Law of 2020, and the Cryptology Law of 2020 that require a company doing business in China to allow for the Peoples Republic of China, PRC government to have access to any data it deems necessary. These laws require all Chinese or foreign companies doing businesses in or with a Chinese firm or its citizens to support and facilitate China's government access to the collection, transmission, and storage of data.[1] Virtually giving unfettered access to company records and files, to include business contracts, intellectual property, confidential strategies, and employee and customer personal data. So, it really does not matter where the data is hosted, if a company is owned by a Chinese citizen, does business in China or with a Chinese company the PRC can demand access. [2]

The laws focus on data hosted in China, however they also cover equipment or software made by Chinese firms used in data centers around the world. Another reason why western governments have been focusing on removing Huawei equipment from any western data centers due to security issues and built in vulnerabilities. In addition to hardware vulnerabilities the law also incentivizes Chinese software firms to build in backdoors to such mobile device applications as TikTok, fitness wearables, and other devices that can provide data to the Chinese government.

### **What is it? Why is it a threat?**

TikTok is one of these mobile applications that is created and owned by a Chinese company, ByteDance. It is a video sharing app that allows users to create and share short form videos on any topic. Upward of 97% of TikTok users utilize it on their mobile device. At first look this is just another playful app that allows people to share their world with friends and family. It is easy to download and setup on your phone. It allows one to easy use to create content with their device and share it with others. Some creators of content have built up large numbers of followers and have been coined "Influencers" as their content can be watched by millions at any given time. Influencers have made millions through endorsements of products and services by just talking about them with their followers. In a word this application is "Popular", not only in the United States, but with almost 1 billion people around the world.

TikTok's facade is that it is a playful fun application for people to have fun with. However, there is anecdotal evidence that it has a more sinister use. FBI director Christopher Wray told lawmakers in September of 2022 he was extremely concerned that PRC could weaponize the media app TikTok. [3] When a person downloads and opens TikTok on their device it could open it up to hidden code much like a Trojan Horse. Similar to the famous Trojan Horse of the Stuxnet worm. Developed in 2005, this highly specialized worm floated around the world for almost 5 years before it was discovered in 2010. It went to work in early 2011 when an Iranian engineer had it on his computer and plugged into a network that connected to centrifuges in one of the Iranian Uranium enrichment plants. The virus infected the centrifuges and caused them to spin out of control damaging the internal components of the hardware. The damage to the hardware set back the Iranian enrichment process by 3 to 5 years. A TikTok Trojan Horse could act the same way but with even more impact by damaging American society.

When you download and install TikTok it asks for access to the following items on your phone the camera, microphone, WIFI connection, and your contact list. These items are expected for a video collection and sharing app. However, there are other items that seem to be suspicious for a video recording application such as access to GPS, network, IP addresses, clipboard, photos, calendar, browser cookies and the ability to read, write, and delete contents in your phone's memory. Once installed it can install and remove apps and shortcuts,

record your keystrokes, read home screen settings, and reorders running apps. The most concerning requests is that it wants access to other apps on your phone in addition to your biometric data such as your faceprint, voiceprint, or your fingerprint if you use these as a security authentication on your phone. These are items that we know it accesses or utilizes. What about what we don't know. Could the PRC have hidden code buried in the application that sends more information to a state-sponsored agency? Could there be a Trojan Horse concealed within TikTok?

China is notorious for stealing sophisticated military weaponry and intellectual property and now with TikTok it can gain access to over 100 million Americans' personal information. With TikTok on your phone it is now collecting personal information about your usage or even waiting for a more sinister motive.



Think about all that you do on your phone. Many of us shop on our phones through Amazon, Home Depot, Walmart, or purchase groceries from our local supermarket. We have an app for our insurance, health track our blood pressure, sugar, or weight. Purchase airline tickets, Uber/Lyft, Bank, Venmo, or trade stock, or have a digital wallet. We access IoT devices such as our ring, web cameras, or the countless other IoT devices in our homes and businesses. Our phone is the key to our personal, financial, and health information and interaction to the world around us.

Think about if you lost your phone, the mental anguish you would go through, the fear of some bad actor getting into our lives and messing up what we have worked so hard to organize.

We simply do not know what is in TikTok's code base as it proprietary. Unlike China, most of the western world does not require companies to give their governments unfettered access to code base or collected data. No one knows if there is a Trojan Horse built into its code. However, many in the intelligence and security communities believe that it is not if, but how many are hidden within its code. According to the Counterterrorism Group, TikTok is very likely collecting account data such as usernames, passwords, and credit card information on several of your applications on your mobile device and could transfer funds or hold data for ransom to obtain financial profits.[4] This information could be used later to hold you hostage.

#### **What Would Happen If?**

What would happen to your personal life if someone got a hold of your phone and was able to log into your bank account and transfer money to an offshore account. Use your digital wallet for cash advances or purchase of services or merchandise. Log into your Amazon account and order hundreds or thousands of dollars' worth of merchandise. Buy airline or cruise tickets using your stored credit card information. Gain access to your retirement or broker's account and sell your portfolio then transfer the funds out of the account. Cancel your insurance, capture your biometric data, create and send inappropriate email to your contact list, damage to your reputation and credit, the list goes on. Visualize the chaos that would occur if all the apps on your phone did the opposite of what you wanted. Think about the work it would require, the dozens of phone calls, emails, and possible lawyer expenses to get some of your life back in order. It could take months or even years of constant effort to try to fix your life. In some cases, it will never be the same.

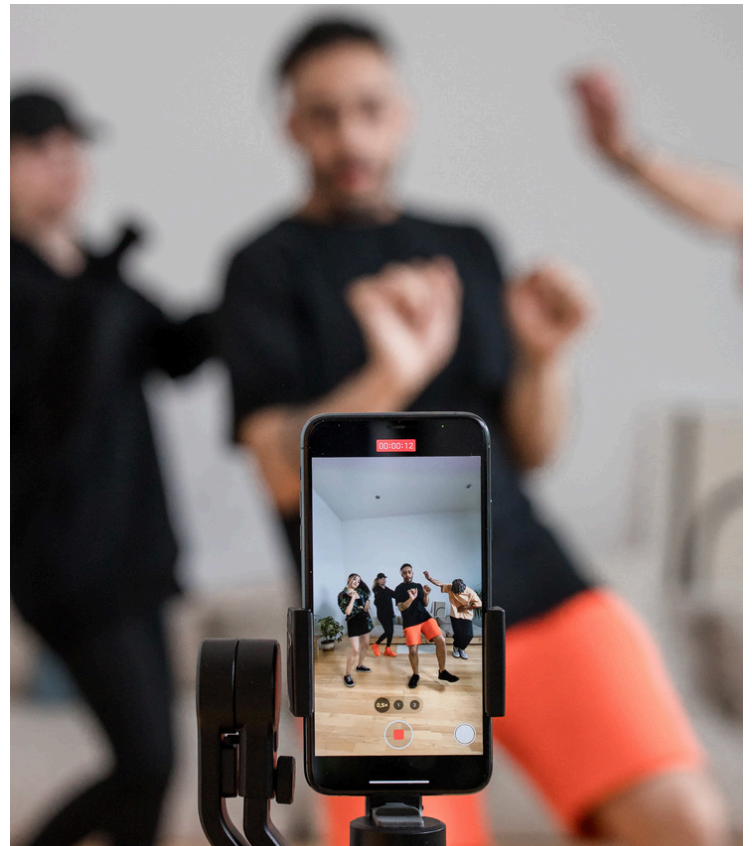
Imagine the other side of the coin, all the work a business will need to do to try to get your accounts cleaned up, if they can, return the money, restock or write off merchandise that was missed ordered and shipped, cancel and reissue credit cards, close and reopen new bank, brokerage, insurance accounts, etc. Collectively the firms that you do business with could spend several hundred-man hours correcting your accounts. Mind you in some cases they are not legal bound to correct these issues, this work is a direct expense and negatively impacts their bottom line. They do this work out of positive customer service. They could choose not to clear up the issues if it becomes too costly.

#### **Preemptive Strike**

Now let's step up this to how it could be a national security issue. Imagine the Chinese want to make a preemptive strike against the United States. As they coordinate an invasion of Taiwan, they activate the Trojan Horse in TikTok that runs through your phone's apps and does the mass bank account clearing, credit card purchasing, appointment canceling, email sending, totally reeking havoc with your personal life. Now multiply it by 100 million users. 100 million users experiencing issues with their life essentials would inflict havoc across our society tying up our financial, retail, and health care infrastructure. This act would pull our attention from the regional conflict in the west Pacific to our homeland. Institutions we take for granted would be in chaos, it would take months or even years to fix the billions of issues and billions of dollars that would be experienced by American society. We would not be able to focus on the matter at hand an ally being invaded with such chaos going on in our society.

Now think about the soldier or sailor stationed overseas in direct conflict with the Chinese. With communication being relatively easy with the home front they may have direct and instant contact with their loved ones at home experiencing this pandemonium. How do you expect them to focus on the task at hand when they are distressing about what their family is dealing with back home trying to fix their lives.

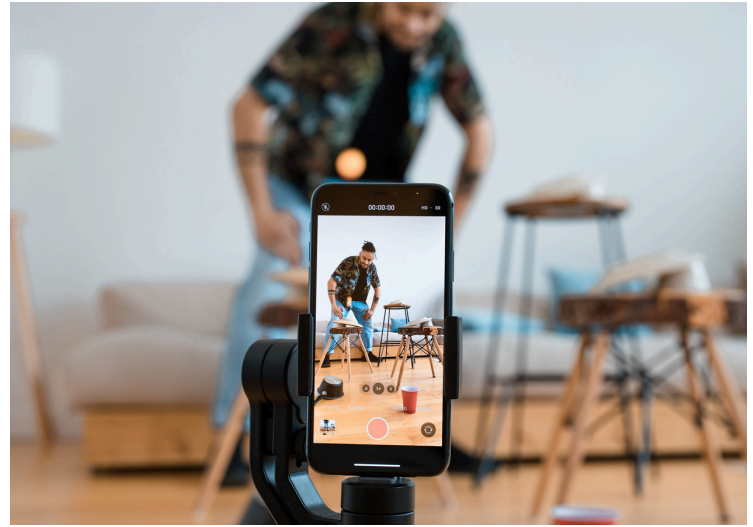
It was recently confirmed in an October 22, 2023 60 Minute story, The Five Eyes, that China is the defining threat to our current era and is using every resource available to gather and/or steal technology and intellectual property.[5]



Given its history and national goals it is hard to believe that PRC would not be using this platform to spy, influence, manipulate, or launch an attack on the western world as they attempt to usurp the United States as the world's preeminent superpower. There is anecdotal evidence that TikTok has hidden code within its codebase.

For this reason, the US government and several state governments have banned TikTok from being on government devices. In April of 2023 Montana lawmakers passed a bill, SB 419[1], making it illegal for app stores to give users the option to download the app and making it illegal for the company to operate within the state. Additionally, several public universities across the country have prohibited the app and other Chinese products from being accessed on campuses. As a push back, TikTok has started a public relations campaign in the past few months airing commercials on television promoting the positives of the TikTok app by users. With the hope of defending their usefulness and down playing the application's threat to the general public.

The PRC is a motivated puppet master and has stated in public that its goal is to replace the United States as the sole superpower. There is plenty of evidence that TikTok is a tool they would use to bring the average American to their knees. TikTok is spyware that we need to treat as such and ban it from our society by removing it from our phones and out of our lives. I understand that this stance will impact some people negatively, however leaving it alone will cripple the nation and damage our society beyond repair when the PRC activates the sinister parts of the app.



### About the Author



Paul Frenken is an Enterprise Architect consultant focusing on bringing value by implementing emerging technology and best practices for his clients. He brings more than 25 years of experience in IT infrastructure, development, change management, customer and consulting services.


### References

- [1] Wiley, "U.S. Businesses Must Navigate Significant Risk of Chinese Government Access to Their Data:" <https://www.wiley.law/newsletter-Mar-2021-PIF-US-Businesses-Must-Navigate-Significant-Risk-of-Chinese-Government-Access-to-Their-Data>, Nazak Nikakhtar, March 2021
- [2] The Hill, "For Chinese firms, theft or your data is now a legal requirement." <https://thehill.com/opinion/cybersecurity/532583-for-chinese-firms-theft-of-your-data-is-now-a-legal-requirement/>, B. Thayer, January 7, 2021
- [3] Forbes, "Is TikTok Really A National Security Threat?" <https://www.forbes.com/sites/petersuciu/2022/11/18/is-tiktok-really-a-national-security-threat/?sh=79078a2d4ade>, Peter Suci, November 18, 2022
- [4] The Counterterrorism Group, "TIKTOK'S Data theft and A Trojan Threat to Latin America" <https://www.counterterrorismgroup.com/post/tiktok-s-data-theft-and-a-trojan-threat-to-latin-america>, M. Tovar, R. Flood, August 2022
- [5] CBS News 60 Minutes, "More from the "Five Eyes" intelligence chiefs' warning to 60 Minutes - CBS News" <https://www.cbsnews.com/news/more-from-five-eyes-intelligence-chiefs-warning-to-60-minutes/>, B. McCandless Farmer, October 22, 2023
- [6] Montana Legislative Services, "leg.mt.gov/bills/2023/billhtml/SB0419.htm", April 18, 2023



## General Membership Benefits

Here are just a few of the many reasons why ISSA is the association of choice for cyber security specialists around the world:

-  **Local Chapters**
-  **Professional Networking**
-  **Learning and Development**
-  **Career Advancement**
-  **Leadership Opportunities**
-  **Recognition**
-  **The ISSA Journal**
-  **Exclusive Savings**
-  **Earn CPE/CPU Credits**
-  **Access to a Global Network**