“Testimony before the U.S.-China Economic and Security Review Commission”

Current and Emerging Technologies in U.S.-China Economic and National Security Competition.

February 1, 2024
Ivan Tsarynny
CEO, Feroot Security.

Thank you very much, Co-Chairs Wessel and Helberg, for inviting me to the hearing today.

I am the CEO and Co-founder of Feroot Security, a company that helps organizations eliminate threats posed by software that secretly tracks people online.

My testimony will focus on China’s IT software products and the risks they pose to American users’ data and privacy.

Feroot’s research has given us an unprecedented look into the techniques our adversaries use to steal sensitive information. Therefore, I'm going to cover these three important areas:

Number one - what our research has revealed on web tracking pixels collecting sensitive information of U.S. persons and making it accessible to entities under China’s jurisdiction including the Communist Party, Chinese Intelligence, PLA and other Chinese authorities.

Number two - how software connected hardware has the potential to conduct—and has been conducting—equally damaging surveillance.

Number three - policy recommendations along these lines that the Commission might make to Congress.

Why Data Collection by Tracking Pixels is a National Security Risk?

The first portion of my testimony will focus on the collection of U.S. user data on websites.

Feroot analyzed more than 3,500 websites of major companies, healthcare providers and governments to establish the baseline of collection of user data by tracking pixels. A tracking pixel is a piece of code used by websites to track digital ad campaigns, and usually remain on websites after ad campaigns end.

We found that ByteDance's TikTok collects a huge amount of U.S.-based user data, even data belonging to people who have never signed up or used the TikTok app.

In fact, we worked with the *Wall Street Journal* to inform government agencies that their sites were indeed activating TikTok web tracking pixels without their knowledge, contrary to the executive orders that prohibited the use of TikTok and other technologies products from China.

By March of 2023, TikTok web tracking pixels were collecting user data on 7.5% of U.S. business and government websites.

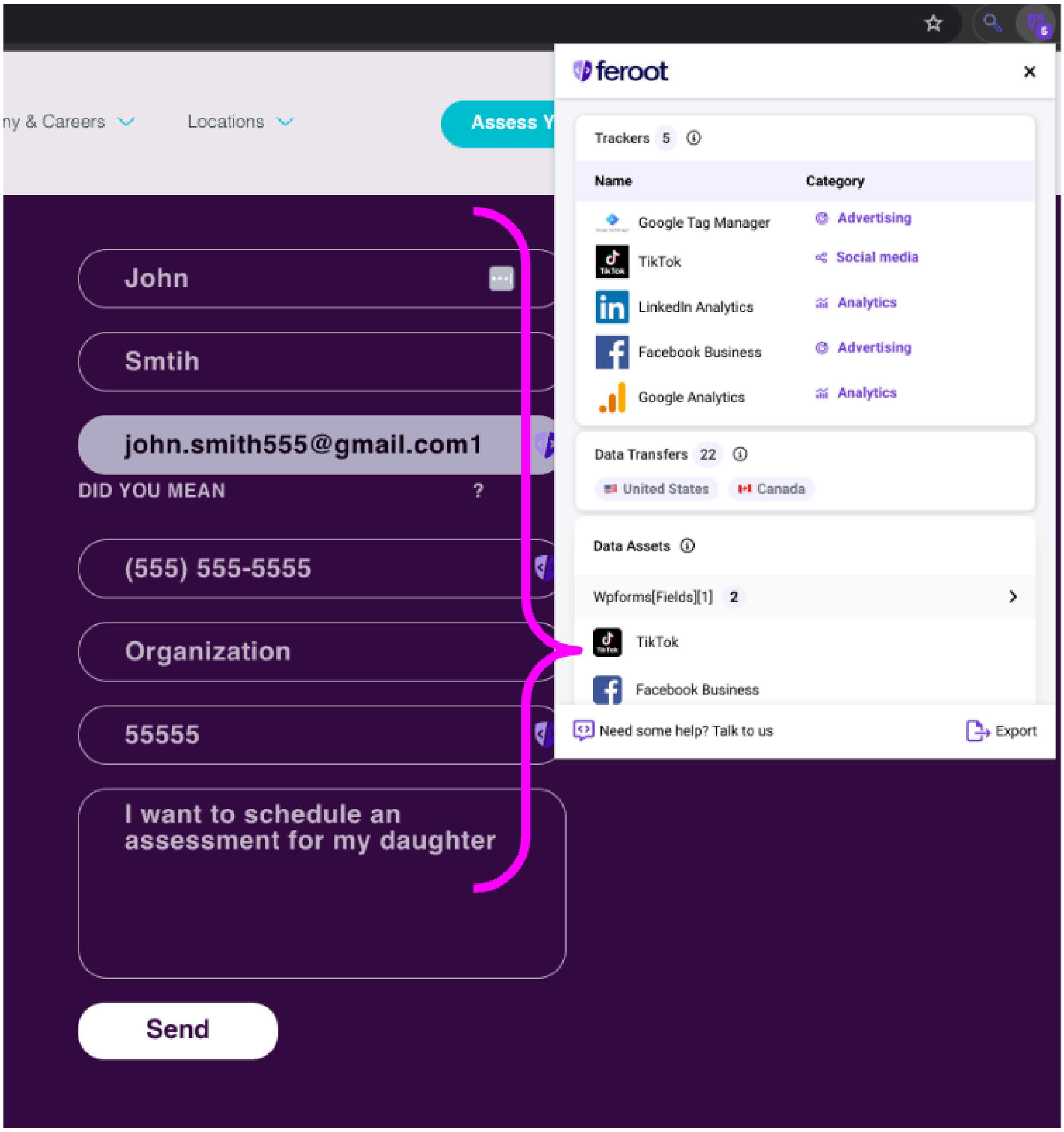
What's even more startling is that by December of 2023, we found that the presence of TikTok tracking pixels increased by 75% on financial services and banking websites—rising from 5% to 8.5%; and increased by 178% on healthcare service provider websites—rising from 2% to 5% of healthcare websites.

While tracking pixels collect data for legitimate purposes such as to advertise, enhance user experience, personalize content, or improve services, the collected data can also be used for illegitimate or nefarious purposes including spying, interference in elections, and illegal surveillance.

For instance, TikTok tracking pixels are silently loaded on webpages where users enter their login and password, schedule an appointment, renew a license or buy an airline ticket. TikTok sees everything users enter into online forms—and unlike tracking pixels from other similar companies such as Meta, we found instances when TikTok tracking pixel also collects information that is *shown to* users on web pages.

Given this, the data collection can capture very personal information: search keywords, search results, purchases, transactions, and any other information you exchanged or were shown online—which can reveal medical test results, pregnancy status, or pre-existing health conditions.

The below real life example demonstrates this:



John

Smtih

john.smith555@gmail.com1

DID YOU MEAN ?

(555) 555-5555

Organization

55555

I want to schedule an assessment for my daughter

Send

Trackers 5

Name	Category
Google Tag Manager	Advertising
TikTok	Social media
LinkedIn Analytics	Analytics
Facebook Business	Advertising
Google Analytics	Analytics

Data Transfers 22

United States Canada

Data Assets

Wpforms[Fields][1] 2

TikTok

Facebook Business

Need some help? Talk to us

Export

In short, TikTok tracking pixels can know what websites you visit, what banks you log into, where you shop, travel and who your doctor is. *And all that data can be collected on people who have never used TikTok*.

Overall, collection of data isn't new to social media companies or data brokers. But, because TikTok is governed by China's Cybersecurity Law, which requires all Chinese companies to share data with China's authorities which are under Communist Party control, data collected by TikTok, and other companies from China, can be shared with the actors in China. Based on publicly available information it appears to have been shared already.

For example: in 2023, TikTok admitted to using the application's data to spy on journalists. Specifically, employees of TikTok's Chinese parent company ByteDance, accessed users' personal data including location data to track the reporters' physical movements.

This act of surveilling journalists appears to have been authorized by the highest level at ByteDance. Chris Lepitak, the chief internal auditor, led the team responsible for the spying. Lepitak's boss—based in China—reported directly to ByteDance's CEO Rubo Liang.

Additionally, on January 30, 2024, the WSJ reported that TikTok workers are sometimes instructed to share data with ByteDance workers without going through official channels, according to current and former employees and internal documents.

That data sometimes includes private information such as a user's email, birth date and IP address. Additionally, ByteDance workers in China update TikTok's algorithm so frequently that TikTok's U.S. employees struggle to check every change, and fear they won't catch problems if there are any.

Why surveillance by software connected hardware is also a national security risk

I will now turn to the second point I would like to make, which is how software connected hardware has the potential to do equally damaging surveillance.

Another channel for China's surveillance are *backdoors* in "smart" devices and appliances. Backdoors act as hidden passages that can be used to covertly gain access and allow someone to turn on cameras and microphones, and silently modify software without the consumers' knowledge or permission.

For instance, TCL Smart TVs were found to have a wide-open backdoor that enabled its Chinese operators to silently modify software on TVs, take screenshots and upload them to mainland China.

On January 25, 2024, Radio Freedom published findings that various CCTV cameras manufactured by Hikvision and Dahua still uploaded video to their servers even after users disable that service. Last but not least, these cameras were found to have been used by Russia to coordinate its January 2, 2024 bombing of Ukraine that killed 39 civilians.

Today many TVs, refrigerators, music speakers, cameras, tablets, even light-switches are considered "smart" because they are always on, connected to the internet, and are controlled by software that is manipulated by Chinese companies, which means they are particularly vulnerable to silent surveillance.

TikTok, ByteDance, or TCL are not the only threats. There are hundreds of companies and products from China with similar technology that can collect data on U.S. users.

What can we do about it?

The third part of my testimony provides the conclusion and suggestions for the Commission.

The Chinese Communist Party (CCP) has created powerful channels to collect data of U.S.-based users. They're doing this by embedding their software into the building blocks of smart, web and online products, which enables the CCP to perform mass surveillance of both online and offline lives.

China's tech giants including ByteDance, Tencent, Huawei, Alibaba, TCL Technology, and others, through their marketing and sale of highly popular tech products in the U.S., are gaining access to data of hundreds of millions of Americans. These are extremely popular applications like TikTok, CapCut, Lark, News Republic, Riot Games, WeChat, Tencent cloud, PUBG Mobile and countless online and smart products that collect data in the U.S.

The reason data collected by companies under China's jurisdiction can be used for surveillance is because, as you know, they are required to grant CCP's agencies access to the data they collect.

Our research overwhelmingly discovered that U.S.-based users' data are exposed to the CCP on websites that we all use on a daily basis.

If nothing is done about data collection by China in the United States, there will be a point where nearly all U.S. citizens could be surveilled by China's government.

While there have been a number of new data protection and privacy regulations introduced (noted below), they don't adequately protect data against surveillance by China, while creating a nightmare in terms of complexity and growing costs for honest businesses that follow the law.

Some examples include the European GDPR, multiple U.S. Federal and State Regulations: the Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act's 2023 Safeguard Rules, California Consumer Privacy Act, Colorado Privacy Act, Washington My Health My Data Act and similar laws in Connecticut, Delaware, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia.

I have five recommendations to conclude with:

Number One - establish clear rules for everyone.

Number Two - Make these rules compatible with other major regulations, such as the European GDPR.

Number Three - Prohibit granting access to and transfer of U.S.-based users' to entities under the jurisdiction of the government of China.

Number Four - Furthermore, companies should be required to secure their technology supply chain to protect the data of U.S.-based users at every stage, from the point of data creation and collection to the point of data destruction.

Number Five - Accountability: Companies, along with their executives, that collect data from U.S. users should be held accountable, in a manner similar to how companies and their executives are personally accountable for compliance with the Sarbanes-Oxley Act.

Thank you.