SOURCEREE
NATIONAL SECURITY NEWSLETTER

# JANUARY 2023

# January 2023 Newsletter

National Security Investment Reviews

## Issue 1: As China Tech Crackdown Continues, Don't Overlook The Danger Of Lenovo

**Source**: https://www.forbes.com/sites/roslynlayton/2022/12/28/as-china-tech-crackdown-continues-dont-overlook-the-danger-of-lenovo/?sh=190f9af65d72&cs-from=2b55e3a3-b349-4cc2-a030-80823c671047

**Considerations**:

There is one Chinese entity which has largely escaped policymakers' notice, despite its presence in many American IT systems and its connection to one of the Chinese organizations which just landed on the Entity List. That company is Lenovo.

Many are familiar with the name Lenovo from the ubiquity of the company's laptops – especially popular with many American businesses. Lenovo is the brainchild of the Chinese Academy of Sciences (CAS) – the Chinese-government's crown jewel institution of scientific research. Since its founding at CAS in 1984, Lenovo has grown to be the world's market leader in personal computer sales, and today controls roughly 15% of the PC market in the United States. The company's purchase of IBM's laptop business in 2005 gave it brand recognition and global revenue. Its purchase of Google and Motorola assets in 2015 further accelerated its rise. These acquisitions are unthinkable today as the reformed Committee on Foreign Investment in the US (CFIUS) now screens such deals for personal data risk.

Indeed some 900 US municipalities and states use Lenovo products today, potentially endangering the sensitive personal and enterprise data of millions of Americans and enterprises. While some US states have enacted rules on such equipment, Lenovo slips through the porous loopholes of federal security regulation. Lenovo's popularity belies its danger as a data mining dream machine for the Chinese government. General James "Spider" Marks (Ret.) writes,

"Lenovo has unmitigated access to millions of Americans' personal information. This should raise red flags, given the company's history of security and privacy abuses. Lenovo's Watch X sent user locations to a server in China without their knowledge; its Superfish adware installed in hundreds of thousands of computers allowed third-parties to spy on browser traffic, resulting in a settlement with the Federal Trade Commission; security researchers found that its Adups mobile data mining software o could collect personal data without consent. There are other examples that should give potential buyers pause, not just for the chance that sensitive information falls into the hands of third parties, but that the Chinese government obtains and exploits it."

The U.S. military has long known Lenovo's danger. In 2008, the U.S. Marine Corps in Iraq got rid of these machine after they were discovered transmitting data to China. In 2015, the U.S. Air Force, fearing China could access data on U.S. ballistic missile technology, immediately replaced $378 million worth of IBM servers purchased by Lenovo. And a 2019 DOD IG report found that Lenovo products – characterized as "known security risks" – were all over the Pentagon. Sadly, as of 2020 the U.S. government, including DOD, continued to purchase mass quantities of Lenovo laptops.

# Issue 2: The New Proposed TikTok Ban: What to Know

**Source**: https://globalcyberstrategies.substack.com/p/the-new-proposed-tiktok-ban-what

**Considerations**:
Banning TikTok would be a significant action, with broader implications for evolving US positions on the risks associated with foreign technology companies, products, and services. Here are the bill's key takeaways for businesses, investors, policymakers, and the public.

**The Bill's Contents**

- **The One-Liner:** The bill establishes a list of security criteria and definitions around foreign social media companies that pose a risk to national security — and then calls on the president to ban TikTok and ByteDance under those criteria.

**Key Takeaways**

- **The One-Liner:** Businesses and investors should prepare for greater, continued impacts from US technology security policy, while policymakers should clearly delineate risks as the public faces the prospect of a reattempted TikTok ban.
- **The Paragraph — for Policymakers:** The proposed responses to security concerns about TikTok vary widely, ranging from partial bans that would target usage by specific demographics (e.g., the users of US government-issued devices) to complete bans whose backers perceive no reasonable way to mitigate the risks. As these proposals evolve, on TikTok and beyond, policymakers must remember the importance of clearly delineating between distinct security risks, clearly linking specific risks to proposed responses, and clearly and publicly articulating their cost-benefit analysis. US security reviews of foreign technology issues, from investments to data entanglements, are going wide, which makes credibility with companies, the public, and even other governments all the more critical.
- **The Paragraph — for Businesses:** If this bill passed and the president invoked IEEPA to ban TikTok, without successful legal challenge, it would prohibit US companies from engaging in transactions with TikTok and ByteDance. This would force a range of advertisers, analytics companies, and other businesses with relationships with TikTok or ByteDance in some form to terminate them. Regardless of its immediate prospect for passage, the bill's introduction should also compel US companies to assess whether or not they interact with TikTok or ByteDance as part of their data or software supply chains. Businesses should also understand the security criteria and definitions in the bill — because they serve as a point of reference for other bills and policies, and if the bill passed, this TikTok and ByteDance ban could theoretically be expanded in the future to other foreign social media companies.

## Issue 3: U.S. Security Reviews of Foreign Tech Are Going Wide. The Details Matter.

**Source**: https://www.barrons.com/articles/security-reviews-of-foreign-tech-huawei-zte-china-cuba-51670449952

**Considerations**:
U.S. government security reviews of foreign technology and investment, especially from China, appear more frequent and more encompassing, touching on everything from biotechnology to data. But paradoxically—for security reviews that draw on classified information and usually entail a high degree of secrecy—transparency and clarity is key to the functioning of this evolving regulatory regime. The more the U.S. conducts these reviews, the more important for the public, companies, and even other governments to understand alleged security risks and why (at least at a high level) the U.S. acts in some cases and not others. American policy makers should also want to refute any claims of political bias, which rightfully circled the Trump administration's botched Huawei campaign and TikTok ban, and that means clearly spelling out alleged security risks.

Despite many real national security risks (after all, every country spies, and Beijing has no limits on its ability to coerce Chinese firms), Trump officials conflated specific technical risks with economic concerns about Huawei's market dominance. Meshed with Trump's chest-thumping on China, it was hard to shake the air of politically driven decision-making. Trump's attempted ban on TikTok was a worse iteration of this problem: The 2020 executive order did not clearly define the problem, blurred together different security risks, like Beijing seizing data versus issuing censorship orders, and did not describe a cost-benefit analysis. People also had plenty of reason to believe the "security" decision was just politics: Trump told reporters a month before the order that banning TikTok would be payback for Beijing's handling of the coronavirus outbreak.

Explicitly spelling out the reasoning behind security review decisions helps encourage precision and accountability. It allows companies, the public, and even governments to analyze foreign investment, technology, and other reviews that are getting more frequent and broader in scope. It also, as relevant, enables people to criticize the stated justifications or even request further explanation. For instance, in Team Telecom's case, some internet infrastructure experts have pointed out that it's already possible to misroute internet traffic through Cuba and that blocking a submarine cable does not change a malicious actor's ability to do so. (The FCC made a similar claim in October 2021 when it expelled China Telecom, even though the company can also hijack internet traffic without any U.S. presence.) Publishing no justifications would make scrutiny more difficult.

This especially matters for U.S. allies and partners. The botched Huawei campaign and overturned TikTok ban, among others, put center stage the costs of bad digital security arguments, or at least poorly articulated ones: Canada, the U.K., and other countries did not trust them. Providing more transparency around investment, technology, and other security reviews—such as listing high-level review criteria or the reasons for a specific decision—lets other governments track U.S. arguments and make their own assessments. This could be done publicly (such as foreign officials reading the Team Telecom press release) or behind closed-doors, through classified information-sharing. But even if an ally or partner ultimately disagrees with the U.S., that is preferable to black-box decision-making hindering cooperation altogether.