SHIELD

by SOURCEREE

What's Inside

CFIUS Newsletter

September 2020

SOURCEREE

Authors: Adam Murphy & John Lash

TikTok:

This situation is highly dynamic and changing by the day; the purpose of this brief on the situation is primarily surrounding the deal structure and national security concerns inherent in the proposed plans. This is not a comprehensive or conclusive analysis as the dynamic nature of the problem set is evolving.

The unintended consequence – China argues what is good for the US and TikTok should be used as a model for American or other companies who want to operate in China:

- Many Chinese officials have applauded the restriction of TikTok's stake by the United States, calling for using this model of company control to be promoted globally. China notes that overseas operations of American companies such as Google and Facebook should undergo similar restrictions and control measures for the purpose of 'security concerns' in the countries which they operate.

The proposed ownership structure of a newly formed TikTok Global would have software company Oracle (12.5%) and retailer Walmart (7.5%) jointly owning 20% with ByteDance owning 80%.

- Americans will make up four out of five board seats of TikTok Global.
- ByteDance's CEO and founder Zhang Yiming will be the fifth board seat[1].

Dueling geopolitical rivals, the United States and China, both have the regulatory power and authority to block the deal.

- "If related enterprises are transferring technology abroad during trade, investment or technical cooperation that fall under the regulations, they are advised to immediately consult provincial-level commerce department offices and handle that in accordance with the law,"[2] noted Gao Feng, spokesman for the Ministry of Commerce.

ByteDance maintains control over TikTok's algorithm / intellectual property.

- *Critique*: While Oracle will host the data, ByteDance remains in full control of the source code and any operational changes to the code.
- *Critique*: There is a provision for Oracle to inspect the source code. However, since TikTok and Douyin (the Chinese version of TikTok) share the same code base, this means the U.S. will know the operations of the Chinese version. This could be seen as a benefit to the U.S.

Oracle would become TikTok's cloud provider; notably TikTok currently stores U.S. user data on Google Cloud

- *Critique*: Previously, TikTok did not store its U.S. user data in China, on Chinese servers, or on Chinese networks. Ultimately this deal moves the data from one U.S. company to another.
- *Critique*: Oracle has close ties to President Trump. Larry Ellison, Oracle's Chairman and Founder, is an ardent supporter who has fundraised for the President. In addition, Oracle CEO Safra Catz served on President Trump's 2016 transition team.

[1] https://www.cnbc.com/2020/09/21/tiktok-deal-splits-control-between-us-and-chinese-owners.html

[2] https://sinvole.com/pulse?id=4514&Article=china-affirms-right-to-approve-tech-deals-as-tiktok-sale-looms

Walmart obtains a new base of over 100 million U.S. users

- *Critique*: Walmart brings little value to the table from a technology standpoint; the retailer stands to gain significant access to users in the e-commerce space where Walmart is attempting to compete with Amazon (owned by Jeff Bezos, who also owns the Washington Post – an often critical mainstream media organization of President Trump). This could provide data to Walmart that can be mined to give the retailer a targeted marketing edge over other eCommerce retailers.

Factors and Threat Vectors:

- TikTok's data collection "potentially allow[s] China to track the locations of federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."[3] - Executive Order on TikTok.

- TikTok has drawn the attention of the Trump administration, as well as other parts of the government, due to concerns that TikTok attains information on Americans that could be given to the Chinese government. As a result, U.S. government institutions have implemented measures to discourage government employees from using TikTok. The Senate together with the House of Representatives voted to prohibit the use of the application on government-issued phones. The U.S. Army and Navy issued guidance banning service members from downloading the app to government-issued phones. Two Senators have also requested the Department of Justice investigate TikTok and the associated video conferencing app Zoom for potential security risks.

- Concerns of TikTok partially stem from the perceived inability of Chinese companies to reject requests from China's ruling Communist Party to access user data. China critics often cite a 2017 law that requires Chinese companies and citizens to comply with all matters of national security. TikTok says all American user data is stored in the U.S., with a backup in Singapore. TikTok also says none of its data is subject to Chinese law. If location of the user data is essentially not changing, is the perceived threat being properly mitigated?

What about… gaming?

- Another critical consideration is whether TikTok is inherently more threatening to Americans than any other Chinese-owned app that collects data. If TikTok is a threat to national security, then analysis of other popular video games owned by Tencent (such as the suite of Riot Games – League of Legends, or Epic Games which owns Fortnite) and applications/games owned by Alibaba would also fall into a security risk category. These could be the next target of CFIUS.

[3] https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/

CFIUS Now Uses Export Controls rather than NAICS codes for Declarations

The U.S. Department of the Treasury published a Final Rule on September 15, 2020, revising provisions in the regulations of the CFIUS. The new Rule implements section 721 of the Defense Production Act of 1950, as amended by the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA). The Rule becomes effective October 15, 2020, and once in place, will do away with the critical technology mandatory declaration based on North American Industry Classification System (NAICS) codes.

The new Rule modifies the mandatory declaration provision for certain foreign investment transactions involving a U.S. business that produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies. Specifically, mandating declarations in connection with covered transactions where U.S. regulatory authorizations would be required to export, reexport, transfer (in country), or retransfer a U.S. business's critical technology to certain transaction parties or others in the ownership chain.

The key innovation here is the rule's requirement that parties analyze whether a license will be required under a hypothetical export, reexport, transfer (in-country) or retransfer of controlled technology to the foreign investor. The parties do not have to attempt an export for the rule to apply.

Important to note this presently only impacts mandatory declarations. At the end of 2018, Treasury implemented a Pilot Program establishing mandatory declarations in defined circumstances. The focus was on non-controlling investments and transactions that could result in foreign control of a U.S. business involved in critical technologies. The Pilot Program identified 27 specific industries by referencing NAICS codes.

- This rule update provides additional clarity to industry with respect to whether a mandatory declaration is required by leveraging established U.S. export control regimes.
- Declaration submission instructions can be found here: https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/declaration-submission-instructions-part-800

A mandatory declaration is intended to represent a more concise and faster review by CFIUS and must be assessed by CFIUS within 30 days. At the end of the 30 days, CFIUS can opt to:

1. Clear the transaction.
2. Request that the parties file a formal notice, restarting the clock of the initial 45-day review once the application is accepted as complete. (Failure to submit this new mandatory filing could be penalized up to the value of the transaction.)
3. Inform the parties that CFIUS is unable to conclude action, but not request or self-initiate a notice (an outcome now commonly referred to as the "shrug").

For the 2019 period, only 35 of the 94 declarations were cleared by CFIUS. This is a signal to deal-makers that there is greater than 60% probability that a declaration will require a full notice. Ultimately extending the timeline of the deal and increasing the uncertainty. For additional information, see Forbes article by John Lash **The Invisible Risks of CFIUS: Timing and Uncertainty**

Cyber Sovereignty – Internet to Splinternet?

The U.S. Department of State describes the Clean Network Program as a comprehensive approach to guarding our citizens' privacy and our companies' most sensitive information from aggressive intrusions by malign actors, such as the Chinese Communist Party (CCP).

Clean Network Lines of Effort: https://www.state.gov/the-clean-network/

On August 5, 2020, Secretary Pompeo announced the expansion of the Clean Network program:

Clean Carrier: To ensure that People's Republic of China (PRC) carriers are not connected with U.S. telecommunications networks. Such companies pose a danger to U.S. national security and should not provide international telecommunications services to and from the United States.

Clean Store: To remove untrusted applications from U.S. mobile app stores. PRC apps threaten our privacy, proliferate viruses, censor content, and spread propaganda and disinformation. Americans' most sensitive personal and business information must be protected on their mobile phones from exploitation and theft for the CCP's benefit.

Clean Apps: To prevent untrusted PRC smartphone manufacturers from pre-installing—or otherwise making available for download—trusted apps on their apps store. Huawei, an arm of the PRC surveillance state, is trading on the innovations and reputations of leading U.S. and foreign companies. These companies should remove their apps from Huawei's app store to ensure they are not partnering with an abuser of human rights.

Clean Cloud: To prevent U.S. citizens' most sensitive personal information and our businesses' most valuable intellectual property, including COVID-19 vaccine research, from being stored and processed on cloud-based systems accessible to our foreign adversaries through companies such as Alibaba, Baidu, China Mobile, China Telecom, and Tencent.

Clean Cable: To ensure the undersea cables connecting our country to the global internet are not subverted for intelligence gathering by the PRC at hyper scale. They will also work with foreign partners to ensure that undersea cables around the world aren't similarly subject to compromise.

Clean Path: On April 29, 2020, Secretary Pompeo announced that the U.S. Department of State will begin requiring a Clean Path for all 5G network traffic entering and exiting U.S. diplomatic facilities. The 5G Clean Path is an end-to-end communication path that does not use any transmission, control, computing, or storage equipment from untrusted IT vendors, such as Huawei and ZTE, which are required to comply with directives of the Chinese Communist Party. The 5G Clean Path embodies the highest standards of security against untrusted, high-risk vendors' ability to disrupt, manipulate or deny services to private citizens, financial institutions, or critical infrastructure.

Critique: This type of policy must consider the technical capabilities and consequences to U.S. citizens. For additional information, see Forbes article by John Lash **CFIUS and a Tale of Two Internets.**

In September 2020, China's Foreign Minister Wang Yi unveiled a new program as well, the Global Initiative on Data Security. The initiative parallels the Clean Network Program, outlining data privacy concerns for Chinese citizens and businesses and urges governments to respect other countries' cyber sovereignty, whereby countries exercise full control in their corners of the internet.

It remains presently unclear how both policies will be implemented in the long run, but some have compared Trump's Clean Network Program to China's "great firewall", while others argue it is more posture than policy. Could it be more than that?

Tech leaders have long cautioned against governments dictating internet data flows based off political considerations rather than technical ones — an idea commonly referred to as the "splinternet". However, the global divide toward a more fragmented internet may be closer than most businesses realize, specifically, how the CFIUS interprets cyber sovereignty could impact investment activity as well as research and development.

The Clean Network Program enables the U.S. government to dictate how its citizens and businesses will access the world wide web. The Program is an expansion of the White House's 5G Clean Path initiative, which previously banned Huawei and ZTE from America's 5G infrastructure. America's allies like Japan, Australia, New Zealand and Taiwan also banned Huawei's equipment in their mobile networks. The UK banned the company from contributing critical parts to its 5G network. Huawei signed agreements to offer 5G services and trials in many markets in Asia and Europe, a risk many tech leaders consider a step toward a more segmented internet along localized infrastructure.

While the future of 5G is still developing, there must be a recognition that the competition is reliant on the underlying technologies – from R&D to maintenance and onto ultimate deployment. Within these broad categories both governments and operators should prioritize the security standards around these concepts that are ingrained on the pillars of security, stability, capacity, and speed. In context, 5G is considered one of the many ways the internet can be 'splintered', with other areas including software, infrastructure, and network architecture.

Critiques of the "Clean Network" plan:

- Lack of technical detail.
- No reference to legislative tools required.
- Would require internet sovereignty capabilities to not only mandate the localization of data (which is possible), but also the control and resources to directly oversee and censor the domestic internet at an extensive level.
- Could present significant disruption to the global tech industry, particularly American companies.
- Public backlash against the vectors of censorship of applications that are hugely popular in the United States such as: TikTok, WeChat, Call of Duty, Clash of Clans, and other various mobile games and titles.

SHIELD VISION

Software platform for on-demand supply chain risk assessments and financial intelligence

SHIELD SQUAD

Analytical Support

SHIELD INTEL

Business intelligence reports on critical suppliers

Protected by

SHIELD

by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.

SOURCEREE