SOURCEREE

NATIONAL SECURITY NEWSLETTER

APRIL 2023

- The TikTok Saga
- Two New Bills on TikTok and Beyond: The DATA Act and RESTRICT Act
- Bank Failures May Raise CFIUS Issues
- Will 2023 Be an Inflection Point in National Security Regulation?

April 2023 Newsletter

National Security Investment Reviews

Issue 1: The TikTok Saga

Source: https://www.cnbc.com/2023/03/23/tiktok-ceo-set-to-face-a-grilling-in-house-hearing.html and https://www.techdirt.com/2023/03/24/how-forcing-tiktok-to-completely-separate-its-us-operations-could-actually-undermine-national-security/

Considerations:

TikTok CEO set for grilling in House hearing. But U.S. lawmakers also face questions –

- Although TikTok is in the hot seat, the hearing will also raise existential questions for the U.S. government regarding how it regulates technology. Lawmakers recognize that the concerns over broad data collection and the ability to influence what information consumers see extend far beyond TikTok alone. U.S. tech platforms including Meta's Facebook and Instagram, Google's YouTube, Twitter and Snap's Snapchat have raised similar fears for lawmakers and users.
- Conversations with lawmakers, congressional aides and outside experts ahead of the hearing reveal the difficult line the government needs to walk to protect U.S. national security while avoiding excessive action against a single app and violating First Amendment rights.
- Even if the U.S. successfully bans TikTok or forces it to spin off from ByteDance, there's no way to know for sure that any data collected earlier is out of reach of the Chinese government. "If that divestment would occur, how do you segregate the code bases between ByteDance and TikTok?" asked John Lash, who advises clients on risk mitigation agreements with the Committee on Foreign Investment in the U.S., or CFIUS, but hasn't worked for TikTok or ByteDance. "And how is the U.S. government going to get comfortable that the asset, TikTok, which is hypothetically sold, is free of any type of backdoor that was either maliciously inserted or just weaknesses in code, errors that occur regularly in how code is structured?"
- But given that federal digital privacy protections don't currently exist, Lash said the U.S. should consider what it would mean if Project Texas were to go away. "In lieu of comprehensive federal data privacy regulation in the United States, which is needed, does Project Texas give the best available option right now to protect national security?" asked Lash, whose firm is one of only a few that have the expertise to advise the company on an agreement should a deal go through. "And does it continue if ByteDance is forced to divest their interests?"

How Forcing TikTok To Completely Separate Its US Operations Could Actually Undermine National Security (Yoel Roth – tech policy fellow at UC Berkeley and former Head of Trust & Safety at Twitter)

- Even as I believe at least some of the single-minded focus on TikTok is a moral panic driven by xenophobia, not hard evidence, I share many of the national security concerns raised about the app.
- But, whatever your anxieties about TikTok (and I have many!), banning it, and the haphazard Project Texas reaction to a possible ban, won't necessarily help national security, and could make things worse. In an effort to stave off Chinese surveillance and influence on American politics, Project Texas might just open the door for a bunch of other countries to be more effective in doing so instead.

Issue 2: Two New Bills on TikTok and Beyond: The DATA Act and RESTRICT Act

Source: https://www.lawfareblog.com/two-new-bills-tiktok-and-beyond-data-act-and-restrict-act

Considerations:

- On Feb. 24, Rep. Michael McCaul (R-Texas) introduced the **Deterring America's Technological Adversaries (DATA) Act**, which would provide the president with more authorities to block transactions associated with the import or export of Americans' "sensitive data" where there are national security risks. The bill quoted previous, public comments from FBI Director Christopher Wray, Director of National Intelligence Avril Haines, and CIA Director Bill Burns that they believe TikTok presents national security risks to the United States.
    - The DATA Act takes another swing at the president's ability to invoke the International Emergency Economic Powers Act (IEEPA) to ban TikTok in the United States. This is the authority that former President Trump invoked in August 2020 when he signed two executive orders that attempted to ban, respectively, TikTok and WeChat in the U.S., citing national security risks. (The TikTok order was later overturned in the courts, and President Biden withdrew the TikTok and WeChat orders in June 2021.) One of the core challenges with this IEEPA approach to banning TikTok has been the "Berman amendments," or IEEPA's 50 U.S.C. § 1702(b)(3) provision: It excludes from the president's IEEPA authorities the ability to prohibit transactions related to "any information or informational materials," irrespective of the "format or medium of transmission."
    - For defining "sensitive personal data," the DATA Act points to 15 CFR § 7.2, the Treasury Department's final rulemaking on the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018. FIRRMA expanded the authorities of the Committee on Foreign Investment in the United States (CFIUS)—which screens foreign investments in the U.S. for security risks—and increased CFIUS's focus on data and technology risks. The DATA Act therefore uses the Treasury Department's recent regulations on how to define sensitive data. Those "sensitive data" FIRRMA regulations cover, for instance, many forms of genetic data as well as "personally identifiable information" focused on finances, health, and location.
    - Some parts of the bill draw on existing work concerning the national security risks of certain tech companies, products, and services—like FIRRMA regulations on sensitive data—but it still has elements, like the proposed IEEPA amendment, that raise significant policy questions.
- Just a few weeks later, on March 7, Sen. Mark Warner (D-Va.) and Sen. John Thune (R-S.D.), along with 10 other senators, introduced the **Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act**. It would authorize the secretary of commerce to review and prohibit certain transactions between persons in the U.S. and foreign adversaries, focused on information and communications technologies (ICTs) that pose risks to U.S. national security—put simply, investigating tech products and services that could pose national security risks. The bill did not name TikTok specifically, but it was clearly one of the companies in mind when the bill was written: Thune's press comments on the bill mentioned TikTok seven times, and the other co-sponsors

mentioned TikTok in press comments as well. The bill could lead to restrictions on TikTok and non-U.S. technology companies, products, and services.

- The RESTRICT Act would establish a framework for the secretary of commerce to review covered, foreign-linked ICTs for national security risks and then develop options that could range from no action to restrictions on a tech company, product, or service. It has some broad elements—and much remains to be seen about how the legislation is received—but its risk framework, spectrum of responses, and provisions for the U.S. government to declassify evidence of security risks make it a much stronger bill on non-U.S. tech companies, products, and services than most (if not all) of what Congress has seen in recent years.
- Importantly, the RESTRICT Act defines a "covered entity" as a foreign adversary; "an entity subject to the jurisdiction of, or organized under the laws of, a foreign adversary"; or "an entity owned, directed, or controlled by a person" that falls under the prior two categories. The bill defines a "foreign adversary" as "any foreign government or regime"—per the secretary of commerce and based on the risks discussed later in the bill (and below)—that has "engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of United States persons." It explicitly designates China, Cuba, Iran, North Korea, Russia, and Venezuela as countries on the list, with the potential for them to be removed pursuant to the later-discussed risk criteria.
- A covered ICT "holding entity" is defined as any entity that (a) owns, controls, or manages ICT products or services and that (b) at any point in the year prior to review has at least 1 million annual, U.S.-based active users or had more than 1 million units sold to U.S. persons. The 1-million-people figure seems to be a theme in these kinds of laws and policies; it appears in several bills on foreign data risks as well as in FIRRMA in 2018. Of course, it begs the question of whether 1 million Americans is the right threshold to denote an enhanced national security risk—and who came up with the 1-million-people figure in the first place.
- The bill identifies five main categories of risks—covered transactions that:
  - Pose an undue or unacceptable risk of:
    - Sabotage or subversion of ICT products and services in the U.S.
    - Catastrophic effects on the security or resilience of U.S. critical infrastructure or the U.S. digital economy.
    - Interfering in or altering the result or reported result of a U.S. federal election (as determined by a specified group of executive branch agencies).
    - Coercive or criminal activities by a foreign adversary designed to undermine democratic processes and institutions or steer policy and regulatory decisions in favor of a foreign adversary's objectives (as determined by the specified group).
  - Otherwise pose an undue or unacceptable to U.S. national security or U.S. person's safety.
- In some ways, delineating covered transactions is far more precise than some previous policy proposals that blurred together distinct risks, such as the risk of a foreign government using a technology product or service to gather data on Americans with clearances, and the risk of that government influencing a foreign platform's content moderation practices.

Issue 3: Bank Failures May Raise CFIUS Issues

Source: https://www.kslaw.com/news-and-insights/bank-failures-may-raise-cfius-issues

Considerations:
Companies need to be aware of filing requirements before taking foreign money: On March 14, 2023, after a week of three bank failures that marked the largest such crisis since 2008, policymakers continued seeking private buyers and working to stem any contagion by backstopping deposits. While the FDIC is currently ensuring the availability of deposits beyond the $250,000 insurance limit for banks in receivership, companies could nevertheless encounter difficulties, particularly if more banks collapse or if there are other restrictions on liquidity. Companies that turn to foreign investors or lenders for needed funding for ongoing operations or debt must determine beforehand whether they trigger a mandatory filing with the Committee on Foreign Investment in the United States ("CFIUS").

The customer bases of the recently failed banks were heavily populated by U.S. venture-backed startups and companies operating in the technology, life sciences, and cryptocurrency sectors. Customers operating in these areas are more likely to be U.S. TID businesses under CFIUS regulations. Thus, there also is a higher likelihood that a mandatory filing would be required if they took foreign investments or made equity-like loans or financing arrangements with foreign persons.

CFIUS Implications in Bank Receivership

Foreign Investment in Banks. Depending on the types and volume of services performed and U.S. citizen data held, financial institutions may be considered U.S. TID businesses. Thus, if a foreign-owned entity acquired 25% or greater of that institution, as well as access, board, or decision-making rights, the parties could be required to file with CFIUS. Such a mandatory CFIUS filing would have to be made at least 30 days before closing the transaction.

Foreign Investment in Bank Customers. Bank customers may be required to submit a CFIUS filing before accepting foreign money if the companies are U.S. TID businesses. Thus, if such a company is seeking to raise foreign capital to cover its operations or debts until it can recover funds from the FDIC receivership or new owner, it may need to file with CFIUS before closing that transaction. Alternatively, the parties would need to agree that the foreign investor will forego the important rights that establish CFIUS jurisdiction.

Foreign Loans to Bank Customers. CFIUS regulations generally carve out traditional lending transactions, even where the foreign person has a secured interest over securities or other assets of the U.S. business. However, if a loan or a similar financing arrangement enables a foreign person to acquire an interest in profits of the U.S. business, the right to appoint board members, or other comparable financial, access, or governance rights characteristic of an equity investment, the transaction is reviewable by CFIUS. Moreover, if the recipient is a U.S. TID business, the transaction could trigger a mandatory filing. CFIUS may also have jurisdiction over lending transactions in circumstances of imminent or actual default or other conditions with the significant possibility that a foreign lender may, as a result of the default or other condition, acquire the requisite control or other important rights.

Like lending transactions, convertible debt instruments generally are not covered transactions, unless a foreign holder has control over certain elements (e.g., when the instrument is converted) or obtains equity-like rights upon conversion. When determining whether such an instrument may be a covered transaction, CFIUS considers:

- the imminence of conversion or satisfaction of contingent conditions;
- whether the acquiror controls the conversion or satisfaction of contingent conditions; and
- whether the amount of interest and the rights acquired upon conversion or satisfaction of contingent conditions can be reasonably determined at the time of acquisition.

Otherwise, a contingent equity interest is not subject to CFIUS jurisdiction until conversion.

Issue 4: Will 2023 Be an Inflection Point in National Security Regulation?

Source: https://www.cov.com/en/news-and-insights/insights/2023/02/will-2023-be-an-inflection-point-in-national-security-regulation

On the heels of Russia's invasion of Ukraine, pandemic-induced supply chain disruptions, and U.S.-China tensions over Taiwan, 2022 accelerated a sweeping effort within the U.S. government to make national security considerations—especially with respect to China—a key feature of new and existing regulatory processes. This trend toward broader national security regulation, designed to help maintain U.S. strategic advantage, has support from both Republicans and Democrats, including from the Biden Administration. National Security Advisor Jake Sullivan's remarks in September 2022 capture the tone shift in Washington: "…[W]e have to revisit the longstanding premise of maintaining 'relative' advantages over competitors in certain key technologies…That is not the strategic environment we are in today…[w]e must maintain as large of a lead as possible."

This environment produced important legislative and regulatory developments in 2022, including the CHIPS and Science Act, first-ever Enforcement and Penalty Guidelines promulgated by the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee"), President Biden's Executive Order on CFIUS, new restrictions under U.S. export control authorities targeting China, and proposals for a new regime to review outbound investments by U.S. businesses. The common thread among these developments is the U.S. government's continuing appetite to use both existing and new regulatory authorities to address identified national security risks, especially where perceived risks relate to China.

Outlook for CFIUS & Outbound Investment Screening—Potential Stress in the System

CFIUS will face increased stress as an institution owing to a combination of factors, including an increased caseload, a policy push on enforcement (discussed below), and the drain of additional policy initiatives, including outbound investment (discussed below). The prospect of Congressional investigations of the Biden Administration almost certainly will further exacerbate the pressures on the Committee. While we anticipate that CFIUS will continue to process in a timely manner transactions that do not raise complex national security considerations, the stress in the system may make resolving complex cases even more challenging and, in turn, places an even greater premium on thorough—and early—planning by transaction parties.

Since enactment of the Foreign Investment Risk Review Modernization Act ("FIRRMA") in 2018, we have seen a steady increase in overall activity from CFIUS, backed by dramatic increases in staff and expanded funding. As we observed in the Committee's Annual Report to Congress released in August 2022 (Covington alert), CFIUS's heavy caseload continues to grow, with a record-setting 164 declarations and 272 notices reviewed in 2021. Based on Covington's internal estimates, CFIUS caseload last year appears to have surpassed even 2021's record, with at least 280 notices filed in 2022. This is particularly striking given the concomitant decline in U.S. merger and acquisition ("M&A") activity of as much as 43 percent during the same period, and a reported 56 percent contraction in global M&A in the fourth quarter.

Further Policy-Related Initiatives, Especially on Outbound Legislation. We also continue to see momentum, both in the White House and Congress, toward a new outbound investment review process (colloquially, a "reverse-CFIUS") to screen certain foreign-bound investment by U.S. persons. The Consolidated Appropriations Act, 2023 ("Omnibus Bill"), signed into law by President Biden on December 29, 2022, requires the Departments of Commerce and Treasury to prepare a report setting out the details of a new outbound investment review regime. While the text of the Omnibus Bill itself does not expressly reference outbound investment, explanatory statements released by the conference committee contain provisions directing each of the Departments of Commerce and Treasury to "consider its role in the establishment of a program to address the national security threats emanating from outbound investments … in certain sectors that are critical for U.S. national security." Both Commerce and Treasury must submit a report within 60 days after the enactment of the bill (i.e., by February 27, 2023), and Treasury is required specifically to identify resources "required over the next three years" to establish and implement an outbound investment screening program. While the bill provides no additional insight into the scope of a new potential outbound regime, the inclusion of a short-fuse report requirement in the Omnibus Bill signals enduring (and energetic) support for some form of outbound investment screening in the near future.

Scrutiny from Congress and the China Select Committee. Meanwhile, we expect increasing domestic scrutiny, including in the form of Congressional investigations, to further exacerbate pressures on the Committee. The feedback loop between Congressional pressure and recent media focus, for instance, on Chinese real estate investments in North Dakota and elsewhere, has created a constrictive environment for CFIUS that exposes the Committee's processes to political stress and, in turn, could trigger a chilling effect.

Expanding Scope of National Security: Impact on Other Regulatory Regimes

Amid regulatory developments in the EU, what makes the environment in 2023 especially notable is the appetite within the U.S. government—across both major political parties, both houses of Congress, and the Executive Branch—to stretch national security regulation beyond the more traditional national security domains, into adjacent regulatory landscapes touching on data, communications, and antitrust.

ICTS. For the past few years the U.S. government has increasingly become concerned with the ability of foreign adversaries to expropriate U.S. technologies, intellectual property, or sensitive government or commercial information, including through the implementation or exploitation of Information and Communications Technology and Services ("ICTS") vulnerabilities. Reflecting this concern, President Trump signed Executive Order 13873 (the "ICTS EO") in 2019, which granted the Department of Commerce ("Commerce") authority to implement a regime to review and prohibit certain transactions for purposes of securing the United States's ICTS supply chain. Notably, "transactions" is broad in definition, and can mean an acquisition, importation, transfer, installation, dealing in, or use of ICTS, including ongoing activities such as updates or repairs. Reflecting the bi-partisan consensus around this issue, Commerce under President Biden issued an Interim Final Rule in 2021 implementing the ICTS EO (the "ICTS Rule").

Potential Related New EO on Protecting Sensitive Personal Data. Separate but related to the U.S. government's concerns around the exploitation of ICTS vulnerabilities is the focus on protecting U.S. sensitive data from foreign collection and exploitation, including data associated with users of software applications. While President Biden suspended the Executive Orders signed by President Trump that sought to address this issue through targeting two specific applications—

WeChat and TikTok—he also signed Executive Order 14034 (the "Connected Software EO") in June 2021 that broadly focused on protecting sensitive data of U.S. persons through the scrutiny of transactions with foreign adversaries that involve connected software applications. In December 2021, Commerce issued an Advanced Notice of Proposed Rulemaking indicating it would amend the ICTS Rule to also capture transactions involving connected software applications, and in turn Commerce planned to leverage the authority under the ICTS Rule to also review and potentially prohibit transactions involving connected software applications. Likely due to the same resource constraints that appear to have limited investigations and enforcement under the ICTS Rule generally, however, Commerce to date has taken no further action to formally amend the ICTS Rule.

Tying Antitrust Considerations to National Security. At the end of 2022, a version of the Foreign Merger Subsidy Disclosure Act became law as part of the 2023 Omnibus Bill. The legislation requires parties filing merger notifications under the Clayton Act to now disclose subsidies from certain "foreign entities of concern" including China, where "subsidies" can take the form of "direct subsidies, grants, loans, loan guarantees, tax concessions, preferential government procurement policies, or government ownership or control." The provision specifically highlights the role of Chinese foreign subsidies with explicit references to Made in China 2025 and its anti-competitive consequences.

Increased National Security Scrutiny in Telecommunications Services. The Federal Communications Commission ("FCC") has also focused on expanding national security scrutiny within its processes. Most recently, FCC Chair Jessica Rosenworcel announced that she expects to circulate a proposal that will authorize the FCC, in coordination with Team Telecom, to periodically evaluate the foreign ownership of FCC licensees in light of national security considerations. Currently, foreign ownership review occurs only when FCC licenses are first sought, or when transfers of control or assignments occur. The perceived shortcomings of this approach arose in connection with the FCC's review of the China state-owned enterprise 214 licensees, which were specifically referenced in Rosenworcel's speech. Because most of those licensees did not have a transaction or license application before the FCC, the FCC had to undergo additional processes to initiate and conduct those reviews and, ultimately, commence license revocation proceedings.

While the scope of the new FCC proposal remains unclear, this development is notable because it could affect an existing licensee's ability to bring on foreign investors that do not otherwise trigger a transfer of control. It also could subject licensees to evolving thinking by national security agencies about which owners/investors trigger national security concerns, as the agencies will be able to act on that evolving thinking more quickly. When applied only to investments by Russian or Chinese investors, the impact of this change may be modest because most FCC licensees are aware that investors from those countries can trigger considerable scrutiny. That said, it is possible that over time the gaze of the FCC, and of the supporting national security agencies, may broaden to investors from more benign jurisdictions.

Another notable development has been the FCC's use of its authority over electronic equipment to achieve national security goals. In November 2022, the FCC effectively banned certain Chinese telecom and video surveillance devices from the U.S. market—demonstrating the power of its authority over virtually all electronics equipment, which until this decision had been exercised only to address technical, scientific, and engineering concerns. With Congressional backing, the FCC now has established itself as a potent vehicle for excluding products from the U.S. market on national security concerns.