David Feith
Adjunct Senior Fellow, Center for a New American Security
Former Deputy Assistant Secretary of State for East Asian and Pacific Affairs

Testimony before the U.S. Senate Committee on Finance
Subcommittee on International Trade, Customs, and Global Competitiveness
"Opportunities and Challenges for Trade Policy in the Digital Economy"

November 30, 2022

Chairman Carper, Ranking Member Cornyn, and members of the Subcommittee: It is a privilege to appear before you today. Thank you for your invitation.

This hearing addresses digital trade, and I will focus my testimony on the national-security problems in this area posed by China – specifically, concerns about China's open access to American data.

I want to stress three points:

> First: The importance of recognizing the China challenge. China is an outsize player in global digital trade flows. It is implementing aggressive strategies of data control, data exploitation, and data mercantilism. U.S. policy is not yet answering those strategies.
>
> Second: The United States not only should work *overseas* to expand our digital trade arrangements, we also have urgent work *at home*. Our domestic task is to curb the massive unregulated flows of sensitive data to China. Our trading partners in Europe, Asia and beyond face the same challenge, even if some fail to recognize it.
>
> Third: Immediate action can be taken in at least three areas: (a) to ban TikTok and the TikToks yet to come, (b) to begin controlling exports of Americans' biodata, and (c) to implement the so-called "ICTS" process endorsed by both the previous and current administrations but not yet in use to limit U.S. data flows to China.

The China Problem in Digital Trade

In our unfortunately polarized politics, it is an important sign of health that there is strong bipartisan support for countering China's national security threats. There is also bipartisan support for boosting U.S. digital trade links overseas.

The digital economy accounts for some 10% of U.S. GDP; digital trade contributes more to U.S. GDP than financial or merchandise flows; and digital trade is growing faster than traditional trade in goods and services. There is particularly strong support for increasing such trade with the Indo-Pacific, where the United States has vital interests and strong allies and partners eager to work with us to prevent China from achieving regional hegemony.

But to set new global rules for the data age, and to compete with China, it is not enough to expand digital trade with friends. We also need to limit our digital trade with China. And we need to take action not just overseas but at home. Our challenge is how to begin placing national-security controls on data flows to and from China. We are late in addressing this challenge. If we don't do so soon, the national-security costs may be so high that they will far outweigh the benefits of any improvement in trade rules with our foreign friends. Our failures in domestic regulation may severely limit our ability to shape rules abroad.

A necessary first step is understanding China's approach to digital trade, which has long been far more strategic, mercantilist, and non-reciprocal than U.S. policy has recognized. It is a key element of China's national-security strategy.

For nearly a decade, Chinese leader Xi Jinping has declared that data in the 21st century is like oil in the 20th century: the critical input for fueling economic strength and national power. In 2013, he told his state-run Chinese Academy of Sciences:

> *The vast ocean of data, just like oil resources during industrialization, contains immense productive power and opportunities. Whoever controls big data technologies will control the resources for development and have the upper hand.*

The analogy between data and oil later became something of a cliché in certain circles. But U.S. policy never recognized its logic. China's did.

The Chinese Communist Party developed a comprehensive strategy to control, accumulate, and exploit data. Data such as personal health records, personal genetic sequences, and personal online browsing habits. Data such as corporate trade secrets, corporate supply chain records, and corporate financial accounts. Data such as the photos, voice recordings, and mapping imagery pulsing through phones, drones, and smart cars all around the world.

Beijing recognizes that the competition for global influence in the 21st century will require protecting and harnessing such data to achieve commercial, technological, military and intelligence advantages. And that's what it is doing.

Beijing has built a latticework of laws and regulations to make the Chinese Communist Party the world's most powerful data broker. A set of laws implemented in 2017 gave the Communist Party unchecked access to private data on Chinese networks, whether those networks are in China or associated with Chinese firms such as Huawei overseas. Last year, Beijing enacted additional laws that go even further, demanding not just access to private data but effective control over it.

This has a huge impact on foreign firms operating in China. Not only must their Chinese data stay in China and be accessible by the Chinese state, but Beijing now demands control over whether those firms can send the data to their own headquarters; or to a corporate lab in, say,

California; or to a foreign government that has made a lawful regulatory or law-enforcement request. Under Beijing's new laws, it may be criminal to comply with foreign sanctions against China that involve data. So if the U.S. government, for example, wants to shut off banking or cloud services to a Chinese entity linked to human rights atrocities, a U.S. or other company can comply with U.S. law, or it can comply with Chinese law, but not both.

Boxed in by Beijing, Tesla, Apple and others have opted to build dedicated Chinese data centers – sometimes in partnership with Chinese state entities, lest they lose access to the large Chinese consumer market and valuable manufacturing supply chain.

Beijing's bullying data rules inside China complement its longstanding efforts to buy, steal, and otherwise acquire data from outside of China. Beijing hacks foreign corporate databases. It runs "talent recruitment" programs at foreign universities and firms. It buys foreign companies. And it funds its own data-driven companies to conduct research, forge partnerships, win customers, and vacuum up data in open foreign markets like Silicon Valley, Boston, and Austin.

Beijing's data strategies also prize global propaganda, censorship and influence, all to advance Xi's stated goal of winning the digital "public opinion struggle." Xi wants the Chinese Communist Party to have what he calls "discourse power," meaning the ability to set and shape global narratives. Hence his aggressive regulation of the algorithms and other data technologies that power Chinese apps such as TikTok that are increasingly dominating the U.S. social media market. TikTok enables Beijing not only to harvest mass American data but to transmit favored messages, export censorship preferences, and potentially manipulate and mobilize Americans on a grand scale completely without precedent for a foreign power.

Beijing's approach is nakedly non-reciprocal. It relies on access to data from foreign countries while denying foreigners access to data from China. In China, Beijing controls the data of foreign companies. Outside of China, Chinese companies operate comfortably, creating and accessing valuable new data sets primed for easy transfer back to China in all manner of data-intensive fields – biotech, pharmaceuticals, medical devices, drones, autonomous cars and trucks, social media, digital payments, e-commerce, and more. These data flows to China contain massive quantities of information about American citizens, American companies, American government, and American critical infrastructure.

This is the stuff of digital trade. Yet there are effectively no rules governing any of it. There is nothing effective under the World Trade Organization or any U.S.-China bilateral trade accord, and not under U.S. domestic law either. The United States has no comprehensive federal approach to data governance. Because of the nature of the internet – namely, that it was able to expand globally in a permissive environment, without any of the state controls inherent with traditional goods transported by truck or ship – digital trade (including U.S.-China digital trade) has remained fundamentally unregulated.

In this environment, for upwards of a generation, Beijing has been effective in designing a strategy of global data mercantilism: hoarding and controlling data for me, relinquishing and

exposing data for thee. If the United States and our allies do not organize an effective response, Beijing will succeed in commanding the heights of future global power. Any new digital-trade arrangements we make with our partners would still operate in the shadow of a global digital-trade order that is open to fatal exploitation by Beijing.

The Domestic Regulatory Imperative

The Biden Administration has spoken about the importance of data in our competition with China. "Our strategic competitors see big data as a strategic asset, and we have to see it the same way," said National Security Adviser Jake Sullivan in 2021. But no visible strategy has emerged.

The U.S. government has traditionally had no mechanism for limiting cross-border data flows, even on national-security grounds. Traditional national-security restrictions on commerce are designed to address other issues, and they have historically been narrowly scoped, consistent with important American traditions of limited government. The Committee on Foreign Investment in the United States (CFIUS) screens inbound investment. Export controls restrict outbound flows of U.S. goods and technology (and of some data, in limited cases). Procurement restrictions limit what federal government departments and agencies can buy.

But vast areas of economic life are largely or completely untouched by those tools – including the cross-border exchange of data by private companies, individuals, academic institutions, and state and local governments. When a U.S. hospital system wants to partner with a Chinese pharmaceutical or genomics company, or an American teenager wants to download a Chinese social-media app onto her phone, or your state government wants to procure Chinese drones to monitor the power grid or assist in law enforcement, the federal government has traditionally had no way to regulate such activity to protect national security.

Washington began to address this problem only recently, through the creation – at least on paper – of a new regulatory regime for reviewing cross-border data flows. Known as "ICTS" (for Information and Communications Technology and Services), this regime was established in the previous administration's waning days and maintained by the Biden team through a June 2021 executive order on "Protecting Americans' Sensitive Data From Foreign Adversaries." Under the ICTS process, a Commerce-led interagency panel can investigate, modify, block, or unwind data-related commercial transactions believed to present "undue or unacceptable risks" to U.S. national security.

This ICTS panel has authority across six sweeping sectors: critical infrastructure; network infrastructure, including satellites, wireless networks, and cable access points; data hosting, including services with the personal information of more than one million Americans; surveillance and monitoring technology, including drones; communications software, including mobile and gaming apps; and emerging technologies, including artificial intelligence and autonomous systems. These sectors touch nearly the entire modern economy.

But the ICTS process has not yet been put to use – not against Chinese access to U.S. data centers or biotech labs, not against Chinese drones with eyes on U.S. critical infrastructure, and not against other channels through which large volumes of sensitive U.S. data can flow to China.

Apart from ICTS, the Congress could of course consider legislative approaches. Various bills have been proposed to limit the ability of Chinese apps to operate and collect data in the United States, but without success.

Another idea is to create a new export-control category to restrict the sale of bulk personal data to certain foreign countries. This is the essence of the "Protecting Americans' Data from Foreign Surveillance Act" introduced in June by Chairman Wyden of this Committee, with four Republican and Democratic co-sponsors. But the fate of that bill is uncertain, and the issue of Beijing's data mercantilism was largely unexamined in the congressional work that resulted this summer in the CHIPS and Science Act.

Elsewhere on Congress's agenda, there is the risk that efforts intended to rein in domestic Big Tech platforms could end up imposing stricter standards on American firms than on Chinese ones. This would be perverse in terms of commercial competition and U.S. national security.

The International Path to 'Data Free Flow with Trust'

Also perverse is our longstanding failure to work with our allies (especially in Europe) to address China's digital-trade abuses as part of our international trade diplomacy.

Across effectively the entire era of digital trade, we have been at cross-purposes with Europe over data-privacy rules, while far greater data-related harms from Beijing have mounted. Chinese companies processing European data are in principle subject to localization and privacy-protection requirements under the European Union's General Data Protection Regulation (GDPR). But the EU has to date shown no great concern with mass data collection and exploitation by Chinese companies functioning as extensions of the Chinese state – especially compared with the EU's longstanding rage against U.S. Big Tech.

To be sure, there is a new test case involving TikTok. The Irish government recently investigated the Chinese platform's data practices and sent findings to the EU Data Protection Commission. Brussels has yet to report back.

In the Indo-Pacific, the dynamic is more fluid. The 11-nation Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) includes high digital standards consistent with those of the U.S.-Japan Digital Trade Agreement (2019) and USMCA (2020), both of which were crafted with Beijing's abuses in mind.

Beijing prefers lower digital-trade standards, like those in the Regional Comprehensive Economic Partnership (RCEP) agreement, to protect its mercantilist and authoritarian interests.

That is why it is now pushing to join both the high-standard CPTPP and the non-binding but potentially high-standard Digital Economic Partnership Agreement involving Singapore, New Zealand and Chile – to try to shape (that is, restrain) their standards from the inside. Beijing realizes that digital-trade flows are still overwhelmingly unregulated, and it wants to influence whatever might emerge to fill this international regulatory gap.

Important as it is, keeping Beijing from entering CPTPP against the rules is not enough. Fashioning a high-standard Indo-Pacific digital-trade agreement would be good. So would beginning to impose reasonable national-security restrictions on U.S.-China data flows, followed by consultations to encourage partners to do the same.

The concept that combines these two elements – digital-trade expansion with friends, digital-trade limitation with rivals – is what late Japanese Prime Minister Shinzo Abe called "Data Free Flow with Trust" (DFFT). We should maximize data trade with those we can trust and limit data trade with those we cannot. In other words, more data flow among democratic allies and other like-minded countries, and less data flow with China.

DFFT is a simple notion that will be hard to implement given China's size, strength, and deep integration into our digital economy and that of our allies. It is necessary, however. We are overdue in recognizing data as a strategic resource. Our responsibility now is to design a global digital-trade order that reflects democratic values and not Beijing's.

Three Immediate Opportunities for Action

U.S. legislators and policymakers can prioritize immediate action in at least three areas:

1. **TikTok – and the TikToks to Come:** As the Biden administration reviews TikTok via the Committee on Foreign Investment in the United States (CFIUS), Republicans Marco Rubio and Mike Gallagher have called for legislation to ban the app. Their approach could provide statutory authority to overcome the statutory barriers (namely the Berman Amendment to the International Emergency Economic Powers Act) that caused the previous administration's attempted TikTok ban in 2020 to fail in court. Democratic Senator Mark Warner (also on this Committee) recently endorsed a TikTok ban in principle, calling the platform "an enormous threat."

   TikTok's fate is an acute test of Washington's seriousness about data privacy, counterintelligence, election integrity, and democratic sovereignty. No hostile foreign power has an entitlement to control a leading U.S. media platform. And keeping hostile foreign powers from wielding such influence is a safeguard of free speech.

   But TikTok's fate is also a test for other data threats looming on the horizon. TikTok parent Bytedance has a virtual-reality subsidiary, Pico, that wants to compete in the U.S. metaverse market soon against Meta and Apple. Fellow Chinese tech giant Tencent operates WeChat and other platforms in the United States. As long as such Chinese-

owned and -controlled platforms enjoy unfettered access to U.S. consumers, Beijing will exploit that access for asymmetric strategic advantage.

2. **Biodata:** For all the controversy over TikTok and the obvious complexities in regulating a wildly popular platform, it is widely agreed that Americans should protect their health and genomic data, on grounds of personal privacy and national security. And yet U.S. law and policy have not yet risen to this challenge.

   The protection of biodata deserves to be at the top of Washington's tech-competition agenda. We have seen much commendable action in recent years on semiconductors, including initial moves by the previous administration, the CHIPS Act this summer, and the pending Schumer-Cornyn proposal to extend "Section 889" federal government and contractor procurement restrictions to Chinese-manufactured chips. President Biden recently announced measures to promote domestic biotech and biomanufacturing, but there are no corresponding protections on biodata flows.

   Meanwhile Chinese pharma and genomics companies such as WuXi Apptec and BGI are expanding operations in the United States and partnering with U.S. hospitals and universities. These companies answer to Beijing's Party-state and military, part of Xi Jinping's growing military-industrial complex for precision medicine. As the University of Virginia's Aynne Kokas has written in an invaluable new book, China's access to U.S. health data, especially DNA, threatens harms "with multigenerational consequences."

3. **"ICTS" Implementation:** The new "ICTS" process may be the single best tool Washington has for addressing the multi-faceted China data problem. It is vital, then, that ICTS get off the ground with appropriate staffing, funding, and authority. The administration may have most or all of what it needs to activate the ICTS, but some congressional action may be helpful, too.

   Consider the wide range of problems that ICTS could address, if appropriately used:

   - Data centers: The June 2021 executive order clearly threatened Chinese firms' continued access to U.S. "large data repositories," and Commerce reportedly subpoenaed several Chinese communications firms in early 2021. Yet no enforcement action has followed.

   - Drones: U.S. officials have issued years of warnings about Chinese drone giant DJI, which DOD recently added to a list of firms tied to China's military. Yet DJI still dominates the U.S. commercial drone market. Another Chinese drone maker, Autel, is growing its U.S. sales while keeping a relatively low profile. Drones are within ICTS's mandate but they have not been the subject of any known enforcement action – or even investigation.

- Autonomous vehicles and digital mapping: Many leading U.S. autonomous transport companies rely on financing and engineering from China, while facing no restrictions on the export of sensitive data about U.S. roads and critical infrastructure. ICTS appears to have authority to stop this, but hasn't done so.

ICTS was designed to solve all of these cases. As with TikTok and biodata, addressing them would demonstrate prudent data regulation at home that could be a model for digital-trade policy promotion overseas.

China threats and digital trade are overlapping fields of bipartisan concern. The stakes are high. Immediate action is possible and would be valuable. The administration would benefit from congressional action, and the American people would appreciate the greater protection of their privacy and the strengthening of their national security.

Thank you for the opportunity to testify. I look forward to your questions.