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. House Foreign Affairs Committee
Subcommittee on Asia, the Pacific, Central Asia, and Nonproliferation
"The Strategic Importance of a U.S. Digital Trade Agreement in the Indo-Pacific"

January 19, 2022

Chairman Bera, Ranking Member Chabot, and the other distinguished Subcommittee Members: I appreciate this opportunity to speak with you about digital trade with the Indo-Pacific and, more broadly, the strategic importance of data rules. Thank you for your invitation.

It is a rare pleasure nowadays to deal with an issue on which there is strong bipartisan common ground. Many Democrats and Republicans in the House and Senate, including from this Subcommittee, have together urged the Biden Administration to pursue new arrangements for expanding digital trade with America's partners in the Indo-Pacific.

I wish to stress three main points today:

> First, a U.S. digital-trade agreement in the Indo-Pacific would indeed serve American interests economically and strategically.
>
> Second, such an agreement is by no means all that is needed. Our country should improve its overall approach to digital trade – starting by curbing the massive and now unregulated flows of sensitive data from the United States to China.
>
> Third, U.S. diplomacy should seek to cooperate with allies on both of these tracks – to expand digital trade among friends, and to limit it with China.

The Importance of Indo-Pacific Digital-Trade Expansion

The case for expanding U.S. digital trade in the Indo-Pacific is strong because digital trade is important, and the Indo-Pacific is important. 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.[1] The Indo-Pacific, meanwhile, is the world's most economically and strategically important region. The United States has vital interests there, and strong allies and partners with whom we share the strategic imperative of preventing China from achieving regional hegemony.

[1] https://sgp.fas.org/crs/misc/R44565.pdf

Increasing economic engagement with Indo-Pacific partners is a key U.S. objective. Digital trade is a ripe and valuable area to prioritize in this regard. Expanding digital-trade flows, and improving digital-trade rules, would be good for the U.S. economy, good for answering the region's strong demand for greater U.S. economic engagement, and good for long-term U.S. strategy.

As we will surely discuss, there are various ways we could craft better digital-trade rules in the Indo-Pacific. We could build on existing arrangements, such as the 2019 U.S.-Japan Digital Trade Agreement, the digital-trade chapter of the U.S.-Mexico-Canada Agreement (USMCA), and/or the U.S.-Australia free trade agreement of 2005. We could also seek to join the evolving Digital Economic Partnership Agreement (DEPA) involving Singapore, New Zealand and Chile, and/or the Singapore-Australia digital trade agreement of 2020.

The general contours of a desirable deal are visible from previous U.S. agreements. Parties would agree not to impose tariffs on each other's digital content. They would agree not to force technology transfer as a condition of market access (meaning companies would not be required to reveal source code or encryption keys just to participate in digital trade). Parties would agree, in general, to open cross-border data flows (meaning they would limit "data localization" rules requiring that data be stored locally and barred from transfer overseas). And parties could harmonize policies on such matters as labor rights, digital inclusion, and digital-market facilitation for small and medium-sized businesses.

The more that our Indo-Pacific allies and partners honor these rules, the better for regional economic development and for U.S. interests. That's why there is strong bipartisanship in Congress on these issues, and on urging the Administration to prioritize digital trade and data governance in its Indo-Pacific Economic Framework.

The Limits of Indo-Pacific Digital-Trade Expansion

There are notable risks in our current approach, however. To set new global rules for the data age, and to compete with China, it is not nearly enough to expand digital trade with our partners. We also need to limit our digital trade with China. The trade with China gives rise to grave threats to our security and hampers our ability to forge appropriate global rules.

Our most urgent digital-trade challenge may not be in the Indo-Pacific but at home. It is how to begin placing overdue national-security controls on data flows to and from China. Without this, the benefits of improving digital-trade rules with our friends in the region could be far outweighed by the costs of our failure to get our U.S.-China data-trade house in order. Indeed, unless we set better, clearer "rules of the road" at home, our ability to shape such rules abroad will be severely limited.

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. This U.S. blind spot is increasingly damaging.

For nearly a decade, Chinese leader Xi Jinping has spoken of data as the oil of the 21st century—the indispensable input that will fuel 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 adjusted to recognize 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 this 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 asserted the Party's unchecked power to gain access to private data on Chinese networks, whether in China or associated with Chinese firms such as Huawei overseas. Last year, Beijing enacted a new set of laws that go even further, by 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 they can send it 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. Beijing's new laws may make it criminal to comply with foreign sanctions against China that involve data – like shutting off banking or cloud services to a Chinese entity linked to human rights atrocities. In these cases, foreign firms can comply with U.S. law, or they can comply with Chinese law, but not both.

The impact of these laws is clear. 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 foreign sources 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 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.

All 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, where we have 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 coldly effective in designing a strategy of global data mercantilism: data hoarding for me, data relinquishing for thee. If the United States and our allies don’t organize an effective response, Beijing will succeed in commanding the heights of future global power. Any new digital-trade arrangements we make with our Indo-Pacific friends would still operate in the shadow of a global digital-trade order that is fundamentally lawless and fatally exploitable 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 last summer. But no visible strategy has yet 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. Procurement restrictions limit what federal government departments and agencies can buy.

But vast areas of economic life are 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. medical-device company wants to buy Chinese hardware and software for its U.S. operations, or an American teenager wants to download a Chinese social-media app onto her phone, or a U.S. university wants to exchange biotech research with a Chinese university, or a U.S. state government wants to use Chinese drones for power-grid surveillance, the U.S. government has no way now to regulate this activity to protect important American interests.

Washington has begun to address this gap 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 waning days of the Trump administration and maintained by the Biden administration through a June 2021 executive order on "Protecting Americans' Sensitive Data From Foreign Adversaries." Under the ICTS process, an interagency panel, led by the Commerce Secretary, has broad discretion to 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. (A press report this week that the Administration is scrutinizing Chinese e-commerce giant Alibaba's cloud business on data-security grounds point to what ICTS enforcement might look like, but so far the report is unconfirmed.)

Apart from ICTS, the Congress could of course consider legislative approaches. Various bills have been proposed limiting the ability of Chinese social-media apps to operate and collect data in the United States, but without success. Another idea is to create a new export-control regime that would restrict bulk personal data from going to adversary countries. So far, however, such measures have not garnered much support. The issue of Beijing's data mercantilism appears absent from the China-focused U.S. Innovation and Competition Act (USICA) that passed the Senate last June, is pending before the House, and focuses on other matters such as boosting U.S. domestic semiconductor manufacturing.

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, which would be perverse from the perspective of both commercial competition and U.S. national security.

The International Path to 'Data Free Flow with Trust'

As we struggle to develop new standards for our own digital trade with China, it will be difficult to harmonize our approach with partners overseas. Overcoming the challenge, however, is essential, if we are to create a favorable global digital order.

Consider Europe. Across effectively the entire era of digital trade, we have been at cross-purposes with our European allies over data-privacy rules, while far greater data-related harms from Beijing have mounted. In Europe and beyond, Chinese companies processing European data are theoretically 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.

In the Indo-Pacific, the dynamic is more fluid, which is part of the reason why we could benefit from entering the fray. 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 and USMCA. Were we to secure an Indo-Pacific digital deal along these lines, we may be able to cement these high standards, at least among like-minded countries.

Beijing wants to block that outcome. It 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 formally to join both the high-standard CPTPP and the non-binding but potentially high-standard DEPA – 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.

Beijing's CPTPP bid is not just cynical but subversive. In just about every category that should matter, Beijing doesn't meet the agreement's standards. Certainly not in digital trade. But also not in labor rights, environmental protection, state-owned enterprises, or basic respect for trade rules in the first place (like those of the WTO, or of Beijing's free trade deal with Australia, which it violates daily with its lawless embargo on Australian goods). But Beijing is powerful, so it demands that CPTPP members let it in anyway.

Some in Washington believe that CPTPP countries cannot be expected to hold the line and exclude Beijing for too long. But why concede that point? If rules-based trade means anything, it means not letting Beijing corrupt yet another institution such as CPTPP. A critical mass of CPTPP members – Japan, Australia, Canada, others – ought to be able to uphold its principles. Failing to do so could be a decisive blow to hopes for securing proper trade standards rather than rules made by and for China.

Important as it is, however, keeping Beijing from entering CPTPP against the rules will hardly be sufficient for shaping the future of trade in Asia. Fashioning a high-standard Indo-Pacific digital-trade agreement would be a good step. So would visibly 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 former 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.

*Note: Some of the language above is adapted from an op-ed co-authored by David Feith (with Matt Pottinger), "China Is Winning the Big Data War," New York Times, November 30, 2021.