Chairman Hawley, Ranking Member Whitehouse, and Members of the Subcommittee, thank you for the opportunity to testify today.

I am a Senior Fellow at Yale Law School's Paul Tsai China Center and a Cybersecurity Policy Fellow at New America. I have worked as an analyst of Chinese cyber and technology policies for the last decade, in the U.S. national security community and in the private sector.

My previous testimonies before other House and Senate committees over the past two years addressed broader challenges in the U.S.-China technology relationship, providing recommendations on issues such as export controls, market access in China, and the ethical challenges of joint research in emerging technologies.[1] In each of these areas, I argued that it is absolutely vital that we maintain the openness of the U.S. system, but with greater resilience and new guardrails to ensure that openness is not exploited.

Today I will provide remarks on managing the data security risks of U.S.-China technology entanglement. I will focus on three areas:

(1) The reality of China's cyber governance system and how Chinese government access to data works in practice
(2) How to build a stronger U.S. cybersecurity and data privacy system
(3) How to address risks posed by China in a way that strengthens U.S. global technological leadership and competitiveness

Part I. China's cyber governance system and Chinese government access to data

We need to start with an accurate understanding of the nature of the risks posed by China's cyber governance system.

Here I would like to make two points:

1. U.S. policymakers should not conflate the problems of (a) U.S. companies operating inside China with (b) Chinese companies operating in the United States.

Different policy approaches are required to address two separate sets of risks. The first is U.S. companies like Apple operating in China (mainly handling Chinese citizen data) and the second

[1] Samm Sacks, Testimony before the House Foreign Affairs Committee, May 2019), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/samm-sacks-testifies-house-foreign-affairs-committee-smart-competition-china/; Samm Sacks, Testimony before the Senate Commerce Subcommittee on Security on "China: Challenges to U.S. Commerce," March 7, 2019, https://www.commerce.senate.gov/2019/3/china:%20challenges%20for%20u.s.%20commerce.

is Chinese companies like TikTok operating in the United States (mainly handling U.S. citizen data). Because U.S. firms in China manage mostly Chinese citizen data, this poses serious ethical and market access questions. This is distinct from the national security question of Chinese companies having access to massive amounts of U.S. citizen data overseas.

The data handled by U.S. firms operating in China is primarily Chinese citizen data, and in some cases, they segment their global networks to prevent Chinese citizen data from flowing outside of China, in accordance with Chinese law. The challenges for U.S. firms in this context are ethical: how will they respond to pressure from the Chinese government to turn over the content of user emails or search histories to crack down on dissent? Do they have control over and visibility into supply chains to prevent the company's technology from enabling the Chinese government to commit mass human rights violations today or in the future? The mass incarceration of minorities in areas like Xinjiang or Tibet is just one example. A new report by the Australian Strategic Policy Institute describes Uighurs in prison-like forced labor conditions at Chinese factories reported to supply U.S. companies such as Nike.[2]

In my previous testimonies, I argued for the development of new legislation and standards to systematically consider the ethics of specific partnerships in China. This is too big and complex a challenge for individual companies to take on themselves. Existing voluntary guidelines like the Global Network Initiative (GNI) are not up to the task of addressing the problem.[3] But neither of the two extreme positions I often hear—pretending these issues do not exist at all or pushing to sever all research and commercial ties with China—serve U.S. interests and values, either.

U.S. firms also face market access barriers and costs due to Chinese government restrictions around cross border transfer of data. Article 37 of China's Cybersecurity Law requires that certain kinds of data ("important data" and "personal data") must be stored on local servers or undergo a security assessment before being sent outside of China. There still appears to be a regulatory gray zone in which multinationals in China can send certain kinds of data outside the country, but it is not clear the extent to which this will be the case in the future, given the significant weight given to national security in Beijing's approach to data regulation.

This is a separate question from the other key issue: the way Chinese companies handle U.S. citizen data does impact U.S. national security. This could mean a Chinese app collecting data from overseas users (like TikTok) or a Chinese company seeking to acquire a U.S. company that has data collected on Americas (like the Ant Financial/Moneygram deal blocked by CFIUS).

This brings me to my second point:

---

[2] "China Uighurs 'moved into factory forced labour' for foreign brands," *BBC*, March 2, 2020, https://www.bbc.com/news/world-asia-china-51697800.
[3] https://globalnetworkinitiative.org/.

2. The Chinese government does not necessarily have unfettered real-time access to all companies' data.

The government of Xi Jinping has built the most comprehensive cyber governance framework in the world. With the 2017 Cybersecurity Law as the centerpiece, a sprawling framework governs data security and transfer, critical infrastructure, and digital content. This framework underpins the most sophisticated system for online control in the world, which the Chinese government is now using to monitor and restrict population movement in the wake of the Coronavirus.[4] And on March 1, a new sweeping regulation for censoring content took effect.[5]

U.S. and Chinese firms must comply with these requirements to operate in China. But what exactly does compliance mean in practice? Nothing is black and white, particularly when it comes to government access to data. Ultimately the Chinese government can compel companies to turn over their data, but this does not always happen.

U.S. policymakers must start with a fact-based understanding of the reality on the ground, taking into account the internal push and pull of different actors in the system, and the gray zones in the rules. Chinese corporate actors are not synonymous with the Chinese government or the Chinese Communist Party (CCP), and have their own commercial interests to protect. Failure to take into account the friction within the system can lead to dangerous policy outcomes; decoupling and conflict with China are not in the interest of U.S. security or economic prosperity.

Many Chinese companies will say privately that they routinely push back against data requests from the government, but they do not want to talk publicly about the fact that they do often resist because doing so draws attention to themselves. In fact, drawing attention to themselves would be counterproductive to the ultimate goal of fighting against government intrusion. In China, media attention will only lead government officials to double down on their request.

A few examples have come out publicly. The Chinese ride-sharing company Didi initially refused to turn over data to law enforcement authorities investigating the murder of passengers.[6] Tencent and Alibaba refused to feed their transaction data to a government credit reporting program under the People's Bank of China (PBoC).[7] The Chinese app WeChat states that it does

[4] Paul Mozur, Raymond Zhang, and Erik Krolick, "In Corona Virus Fight, Government Gives Citizens a Color Code, With Red Flags," *New York Times*, March 1, 2020, https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.
[5] Translation by Jeremy Daum, "Provisions on the Governance of the Online Information Content Ecosystem," https://www.chinalawtranslate.com/en/governing-the-e-cosystem-2/.
[6] Samm Sacks, "What I Learned at Alibaba's Data Security Summit," *CSIS*, October 11, 2018, https://www.csis.org/analysis/what-i-learned-alibabas-data-protection-summit.
[7] Yuan Yang, "Alibaba and Tencent Refuse to Hand Loans Data to Beijing," *Financial Times*, September 18, 2019.

not store the content of user chats for data mining, which may be driven in part to avoid entanglement with the government, according to an article in the Harvard Business Review.[8]

It is also important to keep in mind that data requests are made in a manual fashion (request, review, respond). Moreover, there is no single government repository of all data. The PboC and the National Development and Reform Commission (NDRC), the state agency responsible for state economic planning, have a history of not sharing data with each other. This is not surprising given the tremendous political power that certain kinds of data can yield in the Chinese system.

I'd like to walk through how the regulatory regime related to government access to data in China works since the system is very difficult for outsiders to understand in English, let alone by reading the original directives in Chinese. Moreover, many commentators in the U.S. have no experience with the process involved for companies undergoing cybersecurity-related audits in China.

Among the concerning parts of this cyber governance framework, the Cybersecurity Law (Article 28) states that "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[9] This vague language (which also is echoed in the 2015 Counterterrorism Law[10] and National Security Law[11]) does provide an opening for the government to compel companies to collaborate with intelligence services and law enforcement. Does "technical support" mean turning over encryption keys? Does it mean data monitoring by the security services? Maybe, maybe not.

Compliance often involves lengthy and complicated negotiations between companies and local officials. Local officials must balance competing demands of security with immense pressure to deliver economic development in their jurisdiction. The Chinese Communist Party (CCP) derives its ruling authority in large part by providing economic prosperity. Furthermore, different local government agencies often have different objectives. Sometimes companies will leverage connections with officials from other agencies to stop security bureau officials from seeking certain kinds of data.[12] These factors creates a kind of backstop on how far the government tends to go in implementing some of the most worrisome provisions of China's cyber governance regime.

---

[8] Willy Shih and Howard Yu, "WeChat: A Global Platform?" *Harvard Business Review*, August 15, 2017.
[9] Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," New America, June 29, 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
[10] "Counter-Terrorism Law (2015)," China Law Translate, December 27, 2015, https://www.chinalawtranslate.com/en/counter-terrorism-law-2015/.
[11] "National Security Law," China Law Translate, July 1, 2015, https://www.chinalawtranslate.com/en/2015nsl/.
[12] Based on a private exchange with a former employee of a Beijing-based U.S. business association.

I'd like to look at recent developments in China's cyber governance system where risk of data access is at issue: a regulatory scheme called the Multi-Level Protection Scheme (MLPS) and the Cryptography Law. Both apply to Chinese and U.S. firms in China.

(a) Multi-Level Protection Scheme 2.0 (MLPS 2.0)

MLPS is a security certification regime that the Chinese government established in 2007. In 2018, China's Ministry of Public Security (MPS) released a draft of a new version (referred to as MLPS 2.0). The draft regulation updates the original MLPS regime based on the new principles set out in the 2017 Cybersecurity Law. MLPS ranks from 1 to 5 all information and communications technology (ICT) systems based on their importance to national security, with Level 5 deemed the most sensitive. Anything ranked level 3 or above triggers a suite of regulatory requirements. Companies initiate the process by conducting a self-assessment and working with a third party auditor (typically linked with the local public security bureaus); the auditor conducts interviews on site and observes testing and verification performed by the company. The auditor then writes a report for the provincial or city-level public security bureau.

To be sure, MLPS 2.0 creates more regulatory scrutiny on foreign technology, along with a host of new market access barriers as the Xi government doubles down on reducing reliance on foreign suppliers and boosting indigenous equipment. While the 2007 version of MLPS only targets information systems controlled by the government, the updated regime covers all information systems (all "network operators"), meaning that all private and foreign companies now fall in scope of the review. In the current environment MLPS 2.0 also appears to have a focus on cloud computing, big data platforms, and the Internet of Things.

While this creates a ton of regulatory headache, there is nothing written down under MLPS that requires firms to provide access to all of their data (or provide encryption keys to the Chinese government). There is a provision that requires information systems graded level 3 and above to undergo "cybersecurity monitoring" connected to the public security agency. But there is no definition of what exactly this entails—does this mean a sleepy security guard sits in a facility or a device is installed in the network? The audit is a negotiation—a give and take in which companies hash out with regulators a way to be compliant but not go as far as the most conservative interpretation of the requirements. Again, local bureaus responsible for economic growth in their jurisdiction do not have incentives to demand that companies turn over all of their data. Chinese government regulators understand that certain MLPS requirements like the use of Chinese domestic encryption (as discussed in the next section) create tremendous costs and challenges for foreign companies, which means the use of domestic encryption by foreign firms is rarely enforced.

(It is important to note that the final regulation for MLPS 2.0 has not yet been released. The latest development in late 2019 is that the core standard of MLPS took effect (spelling out the requirements for each of the five levels of the graded system).)

(b) New Cryptography Law

The two most important things to understand about China's encryption regime are (1) the Chinese government wants all companies to use Chinese encryption algorithms; and (2) the vast majority of foreign companies do *not* do this and regulators *rarely* enforce it.

The problem, however, is it is not clear whether this will be the case in the future.

A major change is underway with the release of the Cryptography Law (which entered force January 1 2020). This law overhauled China's encryption regime after two decades of intense internal debate. The law is concerning on several fronts, but it is too early to determine the impact it will have as we are awaiting follow-on regulations that will offer more details about its scope and how it will be implemented for companies. (New regulations plus standards tied to those will eventually update a 1999 regulation called the Regulation on the Administration of Commercial Cipher Codes.)

This new law introduces two important changes, among other developments:

First, it eliminates a significant carve out that has benefitted foreign companies for years. Under the previous regime (centered on the 1999 Regulation on the Administration of Commercial Cipher Codes), the government granted what is known as the "core function exception." This meant that the government permitted the use of products designed with encryption as a general feature (e.g., commercial software). In contrast, products designed to be encryption or security products as their "core" function would face restriction. So companies like Symantec and encryption hardware manufacturers, for example, were excluded from the Chinese market, leaving domestic firms to dominate these business segments. However, for the past two decades, many companies have benefited from carve out, including server, database, and software companies considered not to have encryption as their core function.

The new law is a potential game changer by removing this exception. It is still too early to know whether this means products allowed under the previous regime could be restricted or if they will still be allowed albeit with a new approval process. Nobody knows yet. In place of the exception, the government has indicated that it will focus on requiring certifications for the fifteen products listed in the "Catalogue of Critical Network Equipment and Network Security-Specific Products" ("The Catalogue" includes items like routers, switches, PLC equipment). This Catalogue came out with the Cybersecurity Law in 2017 and lists network products that must receive a

certification before they can enter the market.[13] It is also possible that the new regime could create some new openings for foreign companies, especially smaller companies.

The second change is that the new law creates a separate category of what is called "commercial encryption" (distinct from "core" and "common encryption," which both apply to state secrets; "core" being the most sensitive). Any item that is identified as a commercial encryption "mass consumption product" will not be subject to an import license. The government has not yet released regulations to clarify the scope of "mass consumption," again creating much uncertainty. Depending on how it is implemented, this could mean lifting the burden of having to navigate a lengthy administrative review process (which is often subject to rent-seeking).

Is operating in a regulatory gray zone—one in which the government has all the power and can change course at any moment—a wise decision for a U.S. company? That is not my area of expertise. I highlight these ambiguities so that U.S. policymakers have an accurate picture of how the process works.

Part 2. Recommendations

This first part of my testimony makes clear that China poses real cyber risks to the United States (ethical, commercial, and national security). If the Chinese government wants something, then they can get it, so why is it even important to understand the nuance of how the process works in China, and the fact that there is an internal push and pull, driven by stakeholders with often conflicting agendas? It's easy to make claims that drive headlines on this issue, but my observations are different and can be more difficult to make into short sound bites. I believe U.S. policymakers must have an accurate understanding of the complexities in China's system so that we can respond to the risks it poses in the most responsible and effective manner.

Here I have two main recommendation for how to do this.

(2.1) Build a better U.S. cybersecurity and data privacy system

In order to address the risks presented by Beijing, we should not be reactive, but actively seek to set out a different vision for U.S. internet governance based on a rule of law system.

The reason why in China there is no guarantee that the Chinese government cannot access data is because China's system lacks clarity of law, oversight mechanisms, and clear pathways for contestation. As U.S. policymakers look to strengthen our own data privacy and cybersecurity

[13] Covington blog, https://www.insideprivacy.com/international/china/chinese-authorities-release-catalog-of-network-and-cybersecurity-products-subject-to-pre-sale-inspection/.

system, there are important lessons we can learn. Establishing clear authorities and oversight capacity enables the U.S. government to conduct legitimate national security and law enforcement investigations in such a way that upholds civil liberties and is subject to review and appeal. Here the United States has an opportunity to set out a different vision for U.S. internet governance, one that strikes the appropriate balances among national security, economic, and privacy concerns in a way that promotes strong democratic norms and protects data flow openness.

The United States would be wise to spend more time working on legislation and the development of standards to better protect privacy and secure data—not just in dealing with China—but for all companies.[14] Lawmakers should accelerate progress on a number of bills addressing algorithmic transparency, strengthening cybersecurity, and mandating higher standards for personal data. Developing a comprehensive federal privacy bill is vital to this effort, along with the creation of strong enforcement mechanisms. Inaction by the United States means ceding leadership and influence to both Europe and China in setting international standards.

Moreover, without higher standards for data security and privacy, U.S. citizen data held by unregulated private companies will be more vulnerable to breaches by hackers from China. Equifax's many security issues are well-documented, such as the company's failure to patch known vulnerabilities that ultimately left exposed the data of 145 million Americans. But the hack was also conducted by a foreign government entity with sophisticated hacking capabilities and access to considerable state resources. Setting minimum standards on what data can be collected and retained by all companies will help protect U.S. personal data, regardless of whether the risk is exacerbated by a state-sponsored hacker, a data broker, or a private company transferring the data to Beijing. Companies should not even have access to so much personal data in the first place that can be hacked or transmitted back to Beijing.

(2.2) How to address cyber risk from China in a way that strengthens global U.S. technological leadership and competitiveness

We must keep in mind that U.S. actions to respond to data security risks posed by the Chinese government are not occurring in a vacuum. Our policy approach should be tailored to take into account the fact that technology competition with China will not only play out in the United States and China, but also in other places from India to Europe. How we respond to Chinese companies operating in the United States will have ramifications for whether other countries are willing to accept our vision of data governance.

[14] Jennifer Daskal and Samm Sacks, "The Furor Over TikTok is about Something Much Bigger," *Slate*, November 8, 2019, https://slate.com/technology/2019/11/tiktok-bytedance-china-geopolitical-threat.html.

The ability of U.S. firms to maintain a high rate of innovation depends upon access to global markets, talent, and, perhaps most important, datasets. But an increasingly obstacle to the ability of U.S. companies to operate internationally—beyond China—is rising data sovereignty in places from Europe to India and Vietnam. Data sovereignty refers to efforts by nation-states to ensure control over data by prohibiting transfers of data out of the country or seeking to limit foreign access to certain kinds of data.[15] In this context, our actions will serve as a reference and a roadmap for other governments that are concerned about U.S. companies and the U.S. government getting access their data.

For example, Indian lawmakers are in the middle of debating a draft data protection bill that would require local storage and processing of Indian citizen data in an effort to boost local technology firms as well as push back against data collection by large U.S. companies.[16] The U.S. government and U.S. industry have lobbied against this law. In this context, the U.S. establishing (or, arguably, contributing to) a precedent of strict data localization rules risks other countries following suit.

If U.S. firms cannot send data out of countries in which they operate overseas, they lose access to the value of being able to create international data sets. This directly impacts economic growth and AI innovation because of the ways large, diverse, international datasets are core to building artificial intelligence applications that work across a variety of different geographies, languages, cultures, and demographics. A language translation system only trained in China, for instance, will likely not accurately and precisely capture all of the world's spoken languages as much as a language translation system with data from many different countries. Skin cancer predictors trained only on lighter skin tones, to give another example, are likely to have poor accuracy and precision when trying to predict skin cancer with darker skin tones. Policies that leave companies without any access to global datasets under any circumstances will lead to a "fracturing" of how AI applications are developed.

We have an opportunity to set the standards for protecting the flow of data that has underpinned economic growth and the free flow of information around the world, but with the right safeguards in place.

---

[15] A forthcoming report by Jennifer Daskal (American University Washington College of Law) and Justin Sherman (Atlantic Council) examines the rise of data nationalism in depth by analyzing the different motivations driving it as well as the different forms it takes, looking at data regimes across India, Europe, Russia, and Vietnam, among others.

[16] Covington Blog, "India Produces Updated Draft of Data Protection Bill," February 5, 2020, https://www.cov.com/-/media/files/corporate/publications/2020/02/india-introduces-updated-draft-of-personal-data-protection-bill.pdf.

The challenge, therefore, is how to maintain this openness but with the right guardrails in place. The first step is to limit companies' access and retention of data across the board, as discussed earlier.

We also need to take a targeted approach to restrictions on Chinese companies. In my previous testimonies I argued for an approach based on the idea of a "small yard, high fence," borrowing a phrase used by former Secretary of Defense Robert Gates to mean be selective about what we protect, yet aggressive in protecting it. The same idea should apply to restrictions on access to U.S. citizen data.

The expanded powers of the Committee on Foreign Investment in the United States (CFIUS)[17] provides one tool to do this. The U.S. government should evaluate the risks when a foreign firm acquires or takes a non-controlling investment stake in an American firm that holds U.S. citizen data. As my Yale colleague Rob Williams writes, CFIUS uses a case-by-case approach to evaluate risk, best understood as a scalpel and not a sledge hammer.[18]

Whether through CFIUS or other policy tools, any new restrictions must take a risk-based approach. Not all data has the same level of sensitivity. The mere fact that a Chinese company handles U.S. citizen data in and of itself may not necessarily warrant banning a transaction or blacklisting a specific company. The U.S. national security risks should be evaluated based on an investigation (with regular audits) to determine (a) what kind of U.S. citizen data is being accessed (e.g., metadata, images, geographic data, critical infrastructure data, etc.), (b) how that data is being used and what data protection measures are in place to protect the rights and interests of U.S. consumers, and (c) with whom that data is being shared and through what mechanisms. If based on the outcomes of such an evaluation, we cannot verify that the interests and rights of U.S. consumers will be protected, then that company should be prohibited from storing and sharing U.S. personal data.

Conclusion

In short, we need a more effective strategy to protect U.S. personal data than one-off bans on companies or where they send their data. We need to address legitimate national security risks where they exist but as one part of a broader U.S. initiative on comprehensive data privacy and higher standards for cybersecurity for all companies (whether U.S. or foreign). These efforts should not name China as a bad actor, but instead create a high bar for how all companies manage their data. Failure to establish a compelling vision for U.S. internet governance will only

[17] Foreign Investment Review Modernization Act, Title XVII, P.L. 115-232 (2018), https://home.treasury.gov/sites/default/files/2018-08/The-Foreign-Investment-Risk-Review-Modernization-Act-of-2018-FIRRMA_0.pdf.
[18] Rob Williams, "Reflections on TikTok and Data Privacy as National Security," *Lawfare*, November 15, 2019, https://www.lawfareblog.com/reflections-tiktok-and-data-privacy-national-security.

allow more space around the world for companies controlled by the CCP to flourish worldwide, and Beijing's vision for the internet with it.