Written Testimony of

Josh Kallmer
Executive Vice President of Policy
Information Technology Industry Council (ITI)

U.S. Senate Committee on Commerce, Science, and Transportation

Subcommittee on Security

China: Challenges to U.S. Commerce

March 7, 2019

Global Headquarters
1101 K Street NW, Suite 610
Washington, D.C. 20005, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
itic.org

U.S. Senate Committee on Commerce, Science, and Transportation

Subcommittee on Security

"China: Challenges to U.S. Commerce"

Josh Kallmer, Executive Vice President of Policy

Information Technology Industry Council (ITI)

Introduction

Members of the Committee, thank you for inviting me to testify today.

The Information Technology Industry Council (ITI) represents 64 of the world's leading information and communications technology (ICT) companies. We are the global voice of the tech sector and the premier advocate and thought leader in the United States and around the world for the ICT industry. ITI's member companies are comprised of leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, internet companies, and companies using technology to fundamentally evolve their businesses. Trade issues are critical to our members, and China is always a subject of much concern and interest.

Today's hearing is particularly timely, as China, trade, and security issues garner significant attention from the administration and Congress. Media attention and the potential for conflating these issues make it even more important to clarify and address these complex subjects. China's blatant disregard for international norms governing free trade and market access has been well-established and must be addressed. China's role and impact on the global economy is as complex as it is important, however, and its relationship with the United States is by nature both competitive and cooperative.

China has a well-established record of shifting the playing field in its favor – whether it is creating conditions for technology transfer through forced partnerships with Chinese companies; establishing ambiguous and intrusive security review regimes; or circumventing U.S. export controls laws, these unfair practices not only create an unfair economic advantage but may also, in some cases, pose a national security risk. Numerous policymakers have voiced concern regarding the security implications of China's practices. ITI members take security very seriously, including taking measures to ensure protection of their networks, customer data, IP, and threats to national security. ITI has demonstrated this commitment through our active engagement with policymakers on a number of issues, including the Committee on Foreign Investment in the U.S. (CFIUS) and export controls

reform, and we welcome the opportunity to work with policymakers on the issues before us today.

While we must address China's problematic policies and practices, that is only half of the equation. The U.S. government must also rebalance its approach to strengthening the U.S. economy and the capacity for innovation in the United States. To that end, we encourage the U.S. government to invest in education and skills training and basic research and development, and to foster the growth of emerging technologies in the United States.

Regardless of whether China plays by the rules or not, it will continue to improve in technological development, innovation, and growth. We are no longer in a situation in which China makes technological gains simply by virtue of stealing U.S. technology. Therefore, efforts to wall the U.S. off from competition with China will not solve the problem. The United States must be prepared to compete.

In my testimony, I will outline some of the challenges that our companies face as well as what we can do about it, why the Chinese market is so important, and how we can ensure that the United States continues to foster an environment that gives the best and brightest individuals the necessary tools to develop tomorrow's most innovative technology.

Key Problems Foreign Tech Companies Face from China

Our companies face real and persistent challenges in the Chinese market, including data localization requirements, cloud services restrictions, and intrusive and undefined security review regimes that may lead to exposure of source code and other intellectual property.

Over the last decade, China has made a concerted effort not only to address legitimate cybersecurity and privacy concerns of Chinese citizens and companies but also to foster a protected space for domestic companies to gain an unfair market advantage. As the Office of the United States Trade Representative (USTR) laid out in its comprehensive Section 301 investigation findings report, China has created a tapestry of laws, regulations, standards, and practices that collectively advantage Chinese companies and create conditions for direct and indirect tech transfer.

Despite this clearly strategic approach to boost Chinese innovation and indigenous technology, the Chinese government is not a monolith. Infighting, discord, and pressure from Chinese leadership for agencies to issue regulations and demonstrate enforcement has added another layer of uncertainty and unpredictability to the Chinese market. Following passage of China's 2016 Cybersecurity Law, the tech sector has seen an unprecedented onslaught of implementing regulations, notices, measures, and standards drafted by numerous agencies within the Chinese bureaucracy, often contradicting one another. For

example, the information technology standards body known as TC 260 released 110 standards for comment between November 2016 and December 2017 alone, followed by another 53 standards in 2018 – accounting for two-thirds of all standards that TC 260 has released for public comment. While these standards are often classified as voluntary, they may become de facto mandatory standards, making the short comment windows even more critical. These hastily enacted regulations also allow enforcement agencies to both interpret obligations unevenly and, potentially, target foreign companies.

Broad and Ambiguous Security Review Regimes

While the Chinese government has for the most part been careful not to explicitly outline requirements for transfers of technology, source code, or other IP, the ambiguity and uncertainty surrounding China's numerous "security review regimes" create conditions ripe for coercion of companies to expose valuable intellectual property. For example, the Cybersecurity Law requires that companies subject themselves to intrusive security reviews for products and infrastructure to qualify as "secure and controllable." While the meaning of this term is ambiguous, the provision favors domestic companies and products as inherently more secure and is, in effect, a thinly-veiled attempt to encourage consumers to "buy domestic." Specifically, *the Cross-Border Data Transfer Measures* outline highly intrusive procedures, including background investigations of network suppliers and inspections of corporate offices.

Implicit and Explicit Technology Transfer Requirements

Chinese requirements outlined in various laws and regulations – including those that require firms to locate production or facilities in China and establish a joint venture (JV) with a Chinese partner in order to operate in China – can put their valuable technology and other intellectual property at risk. Disclosure of sensitive information can be forced through a contract (e.g., JV, partnership), direct pressure from local or central governments, or governmental review or certification mechanisms. While there is nothing inherently wrong with voluntary JVs and partnerships, they become problematic when they are forced on foreign parties and when regulations stipulate either that the Chinese partner must maintain majority control of the JV or that only a Chinese company may obtain required product licenses.[1]

China has made its technology transfer objectives clear through its national strategy to promote indigenous innovation, *Made in China 2025*. The strategy explicitly promotes the

[1] See *Law of the People's Republic of China on Chinese-Foreign Joint Ventures; Provisions on Administration of Foreign-Invested Telecommunications Enterprises; The People's Republic of China Foreign Investment Catalogue 2017*

transfer of technology as a means of advancing technological capability, competitiveness, and strategic emerging industries. Further, it outlines a wide-ranging effort to employ funding and the investment of significant government resources in support of key industries. While the Chinese government intended *Made in China 2025* as a means of setting aspirational goals for a domestic audience, it has nonetheless fostered an environment that makes forced technology transfer more likely and may yield overcapacity in targeted sectors. These factors create real competitiveness risks for companies and can significantly distort market supply and demand.

Restrictions on Foreign Cloud Service Providers

China's restrictions on U.S. cloud services providers (CSPs) exemplify the lack of fairness in the U.S.-China trade relationship. Foreign companies face written and unwritten requirements that do not allow foreign companies to obtain licenses to operate without a Chinese partner; force U.S. CSPs to surrender use of their brand names; and require companies to hand over operation and control of their businesses to Chinese companies in order to do business in the Chinese market. Chinese cloud services providers operating in the United States are subject to none of these restrictions.

Data Localization Requirements

Cross-border data flows are essential to digital trade. In 2016, over 53 percent of total U.S. service exports relied on cross-border data flows.[2] Data flows are also important for purposes of network protection, as companies rely on real-time exchanges of information across borders to identify and "patch" vulnerabilities and receive timely system and software updates. Despite numerous efforts by the U.S. tech sector to explain that data localization does not enhance - and may diminish - data security, China continues to publish new and troubling laws, regulations, and standards that require the storage of data in China. For example, China's Cybersecurity Law and other regulations seriously harm many U.S. exporters by restricting cross-border data flows and requiring firms to store and process data in China. Draft regulations – including *the Cross-Border Data Transfer Measures* and *the Critical Information Infrastructure Protection Regulatio*n (both implementing regulations of the Cybersecurity Law) contain numerous provisions that would force companies to localize certain data in China and create undue and expensive impediments to transferring business information out of China in a timely manner.

[2] "Cross-Border Data Flows, the Internet and What is Means for U.S. and EU Trade and Investment" (Brookings, https://www.brookings.edu/blog/up-front/2014/10/21/cross-border-data-flows-the-internet-and-what-it-means-for-u-s-and-eu-trade-and-investment/).

China's Standards Development

Chinese standards work and implementation of the 2017 revision of the *Standardization Law* presents a unique set of challenges, as China aims to codify the standards-development process in China.

The Law includes problematic elements such as unclear public disclosure requirements that may reveal business-sensitive information. Implementing policies of the Law, such as the *Pioneer Standards Program*, incentivize public disclosure of standards that companies use in their products. Disclosure is not mandatory, yet companies that do not disclose standards will not be recognized as standards "pioneers," which may influence consumer purchasing preferences and also renders the product ineligible to compete for government procurement contracts.

ITI supports industry-led, consensus-based international standards development, which fosters an environment in which standards are market-driven and only adopted if they benefit current technology and consumers. However, China and other nations have utilized "country-unique" standards as a policy tool to establish market access barriers and give domestic companies a competitive advantage. Given the size and influence of China's market, these national standards may influence regional trends and product development. China's exclusion or strict limitations on the participation of foreign companies in standards development bodies means that Chinese standards are developed in way that weakens interoperability and the global standards system. ITI urges Congress and the Administration to promote and strengthen the standards development process worldwide to ensure that development is fully consistent with international norms and the World Trade Organization (WTO).

China's reliance on a top-down model to promote its standards does not mean that the U.S. government should take a similar approach. While China may propose many more standards in international standards organizations, the market should ultimately choose the most appropriate standard for consumers and the current technology. Regardless of quantity, a robust industry-led international standards development process leads to adoption of the most appropriate standard. In this regard, there is no "first mover advantage" that would give China an advantage in the development of 5G or technologies related to artificial intelligence (AI). The best way to counter China's growing influence in international standards bodies is to work within and support the international standards system. The U.S. government can assist by promoting reliance on international standards and by investing in research and development, which will allow U.S.-based companies to continue to innovate and lead in the market.

Why Do Companies Stay in the Chinese Market?

While the Chinese market presents clear risks and impediments for foreign companies, its size and impact on the global supply chain cannot be ignored. In 2018 alone, the U.S. exported nearly $21 billion worth of ICT goods to China.[3] China is the third largest market for U.S. services exports in Asia and accounts for nearly a quarter of the global consumer market. These customers operate not only in China but also globally – and they demand products and services that operate globally. If U.S. companies leave the Chinese market, they effectively forfeit much more than the Chinese market to Chinese companies. Customers – particularly those that depend on enterprise services such as cloud computing – will seek companies that provide services in all markets in which they operate.

From both an economic and technological advantage perspective, it is not in the interest of U.S. companies, consumers, or the government to cede market share to Chinese companies. Put simply, if companies want to compete for global consumers and continue to be at the forefront of emerging technology development they must compete with Chinese companies in China and abroad.

What the U.S. Government Can Do

ITI appreciates that the U.S. government recognizes China has instituted problematic tech policies and practices and that the administration has taken steps to address it, including USTR's Section 301 investigation and subsequent report. We routinely hear from policymakers regarding both economic and security concerns related to China, including current and future American economic competitiveness. The tools that the U.S. government uses to address these issues, however, must be tailored and strategic to avoid causing unnecessary harm to U.S. competitiveness and innovation – which are key to the Uniteds States' economic *and* national security. I'd like to outline a few basic tenets below.

Assess Potential Security Problems from Both a Private and Public Sector Perspective

ITI respects and acknowledges national security concerns. We advocate for and work with policymakers to develop thoughtful and tailored policy approaches that consider: the problem or threat from both a public sector and private sector perspective; whether and to what extent a threat can be mitigated; and how to limit adverse or unintended effects on companies' ability to operate, compete, and innovate. It is important to recognize that the public sector often has information and political insights that the private sector does not and vice versa. While the U.S. government has visibility into many security threats, it relies on

[3] U.S. GDP was $20.89 trillion in the fourth quarter of 2018. (Bureau of Economic Analysis, https://www.bea.gov/news/2019/initial-gross-domestic-product-4th-quarter-and-annual-2018).

the private sector to tell it what is happening on its networks and the steps that should be taken to mitigate risks.

While policymakers are rightly concerned about safeguarding American companies' innovations in emerging technology fields such as AI and 5G, it is important to ensure that such safeguards do not hamstring companies' ability to develop the very technologies that the U.S. government values for purposes of economic growth and national security. The tech sector can help in this assessment of future impacts.

The consequences of security policy to tech companies will have significant ripple effects. ITI encourages Congress and the administration to engage with the private sector on these important issues and work together to develop a strategic and coordinated approach to the potential threats and challenges posed by China and others.

Compete with China and Invest in America's Future

Preventing China from stealing technology alone will not help us achieve our goals. The U.S. government must invest in America's future. This means investing in research and development, education, science and technology, artificial intelligence, and digital infrastructure. Strengthening the business environment, the nation's human resources, and incentivizing innovation are all key to generating sustainable economic prosperity.

If the U.S. is to preserve its technological edge, it must be prepared to step up and compete with China. Regardless of whether China plays by the rules or not, Chinese inventors, entrepreneurs, and businesses will continue innovating and will close the technological gap between the U.S. and China. While a level playing field is of course important, it is vital that the U.S. government continue to commit to serious investments in technology to ensure American competitiveness and economic growth. China is making a concerted, strategic effort to invest and plan for its economic and technological future. The clock is running out for the U.S. government to take action. Where the private sector in the U.S. is making significant progress in advancing the next generation of technologies and investing heavily in cutting-edge research, the U.S. government can and should do more to support innovation.

With the world's largest and increasingly educated population, China had 4.7 million science, technology, engineering and mathematics (STEM) graduates in 2016. To put that in perspective, that means half of China's nearly 8 million graduates are focusing on STEM, while in the U.S. less than a third – roughly 568,000 of America's 2 million graduates – major in STEM. The U.S. has invested less and less in R&D spending, where in 2016 R&D constituted about 2.7 percent of GDP.[4] China is catching up quickly with an expenditure of 2 percent of

[4] "How much does your country invest in R&D" (UNESCO Institute for Statistics, http://uis.unesco.org/apps/visualisations/research-and-development-spending/).

its GDP going to R&D.[5] In 2017, China accounted for 48 percent of the total global investment in artificial intelligence startup funding, while the U.S. accounted for 38 percent. In monetary terms, China invested $7.3 billion in artificial intelligence while the U.S. invested $5.77 billion.

China is also on track to outpace the United States in other areas. For example, according to a 2018 International Data Corporation report, the U.S. will spend $22 billion on smart city development this year. China is close behind with projected spending at $21 billion. As of 2015, there were 1,000 smart city pilot plans in the works worldwide, 500 of which were located in China. While 66 percent of U.S. cities are adopting smart city technologies, China's test bed for smart cities is the largest in the world.

These are just a few examples. The bottom line is that the United States is failing itself by not seriously investing in our country's technological and economic future.

Conclusion

China poses serious challenges to the tech sector. We must address these challenges aggressively yet strategically and with an eye to future ramifications for the economy and technological competitiveness. We also can neither ignore nor deny the significant role China plays in the global economy as a key piece of the global supply chain, supplier of products and components, an innovative competitor, and a vital market for U.S. goods and services, and it would be a disservice to downplay the need to invest in U.S. companies' ability to compete with an increasingly innovative and technologically advanced China. With the right approach, we can address these serious challenges in a way that benefits the United States' economic and national security.

On behalf of all ITI members, I thank you for having me before the Committee today and commend you for your interest in examining the various challenges that China poses to the tech sector. We stand ready to work with you to address these challenges. I look forward to answering your questions.

[5] Ibid.