



**Written Testimony of**

**Dean Garfield**

**President and CEO**

**Information Technology Industry Council (ITI)**

**U.S. Senate Committee on Finance**

**Subcommittee on International Trade, Customs, and Global  
Competitiveness**

***Market Access Challenges in China***

**April 11, 2018**



**United States Senate Committee on Finance**

**Subcommittee on International Trade, Customs, and Global Competitiveness**

**“Market Access Challenges in China”**

**Dean Garfield, President and CEO, Information Technology Industry Council (ITI)**

**April 11, 2018**

**Introduction**

Chairman Cornyn, Ranking Member Casey, and members of the Committee, thank you for inviting me to testify this afternoon.

The Information Technology Industry Council (ITI) represents over 60 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 the U.S.-China relationship stands at a crossroads. If we continue down our current path of tolerating China’s blatant disregard for international norms governing free trade and market access, we will continue to lose ground on both technological and economic fronts. Yet, altering course poses a unique challenge of navigating uncharted waters. The U.S.-China relationship is as complex as it is important. The relationship has always been – and likely will continue to be – one of both competition and cooperation. We need to approach managing difficulties in the bilateral trade relationship with the nuance and deliberation they deserve, recognizing that both action and inaction will have consequences for years to come, in positive and negative respects.

The tech sector has been at the forefront of the competitive and cooperative balance with China for decades. While competition and collaboration between our companies can and should be a driver of innovation and growth, it is clear that China does not compete fairly. The Chinese have run a robust effort to rewrite the rules of the game in their favor – and this needs to change. Foreign companies must be able to compete on even footing with domestic companies in China and around the globe.

While we must address China’s problematic policies and practices, that is only half of the equation. We also need to rebalance our approach to strengthening the U.S. economy and our



own capacity for innovation. To that end, we must invest in our own people, our own research and development, and foster emerging technologies here in the United States.

Regardless of whether China plays by the rules or not, it will continue to develop significant capacity for technological development, innovation, and growth. The United States must be prepared to compete.

In my testimony, I will outline some of the key market access problems 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 in the Chinese Market**

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 intellectual property. Over the last decade, China has made a concerted effort not only to address legitimate cybersecurity and privacy concerns 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 September 2017 alone, accounting for nearly half of all standards it has ever released for comment. Implementing regulations and standards that the Chinese government promised would clarify compliance questions often seem hastily drafted by individuals without relevant expertise, leading to more questions than answers. While the Chinese government has addressed certain concerns through solicitation of comment, often industry finds that issues go unaddressed or appear again in other regulations or implementing guidelines – leaving us to play an endless game of “whack-a-mole.” 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 IP, the ambiguity and uncertainty surrounding China’s numerous “security review regimes” create conditions ripe for coercion of companies to expose these valuable trade secrets. 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 seems to favor domestic companies and products as inherently more secure. This provision appears to be 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. Given that President Xi Jinping and other officials have publicly stated an official preference for Chinese technologies, industry remains concerned that this policy empowers agencies to focus disproportionate regulatory attention on foreign technology products and services, relying on a broad justification of “public interest” concerns rather than true national security.

## *Implicit and Explicit Technology Transfer Requirements*

Intellectual property and source code are the lifeblood of American companies, and they make a concerted effort to safeguard these secrets. In addition to ambiguous security review regimes, 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 this invaluable information 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 the term “joint venture” has come to carry a negative connotation, JVs can serve as an asset in China and other markets – allowing foreign companies to operate under otherwise rigid investment restrictions as well as leverage local expertise, support, and connections. There is nothing inherently wrong with JVs and partnerships if they are voluntary. They become problematic, however, when they are forced and regulations stipulate that the Chinese partner must maintain majority control of the JV or required product licenses can only be obtained by a Chinese company, thereby necessitating a partnership.<sup>1</sup>

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

---

<sup>1</sup> 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*



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. This top-down direction fosters an environment that actively pursues technology transfer as a prerequisite for doing business in China. These factors create real risks for companies and reduce the competitiveness of American firms as well as their profitability.

### *Restrictions on Foreign Cloud Service Providers*

China's restrictions on U.S. cloud services providers (CSPs) exemplify the lack of reciprocity in the U.S.-China trade relationship. Foreign companies face written and unwritten requirements that could force U.S. CSPs to transfer valuable intellectual property, surrender use of their brand names, and hand over operation and control of their businesses to Chinese companies in order to do business in the Chinese market. Chinese cloud service providers operating in the United States are subject to none of these market access barriers.

Draft and current Chinese regulations – including Regulating Business Operation in Cloud Services Market (2016) and Cleaning Up and Regulating the Internet Access Service Market (2017), would force U.S. cloud computing providers to offer their services through Chinese partners in the market. These measures, together with existing licensing and foreign direct investment restrictions on U.S. CSPs operating in China under the Classification Catalogue of Telecommunications Services (2015), would require U.S. CSPs to turn over essentially all ownership and operations to a Chinese company, forcing the transfer of incredibly valuable intellectual property and know-how to China.

### *Data Localization Requirements*

Despite numerous efforts by the U.S. tech sector to revise problematic Chinese regulations and explain that localization does not equate to security, China continues to publish new and troubling laws, regulations, and standards that restrict data flows. 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.<sup>2</sup> 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 Regulation* (both implementing regulations of the Cybersecurity Law) contain numerous provisions that will force companies to localize certain data in China and create undue and expensive impediments to transferring business

---

<sup>2</sup> <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/>



information out of China in a timely manner.

The Chinese Government's focus on data localization reflects the premium placed on control of content and data as a tool to ensure the stability of the Chinese Government. Though these policies will also have a negative impact on Chinese multi-national companies, thus far the Chinese Government has not heeded these concerns.

### *Proliferation of "China-unique" Standards*

Standards offer yet another avenue for China to expand its regulatory and legal objectives – with even greater international consequences. Since the early 2000s, China has sought to establish a more robust and coordinated national technical standards regime, increase China's participation in international standards setting bodies, and increase the number of Chinese standards adopted by those bodies. This has led to notable improvements in China's standards setting and transparency, but also caused significant problems for U.S. tech companies.

China's use of standards is particularly problematic for a few reasons. First, China uses standards as final implementing guidelines of laws (including the Cybersecurity Law) for companies, meaning the standard is our last chance to clarify and address problematic provisions of laws and regulations. Political pressure in China to produce standards rapidly has also led regulators to offer insufficient comment periods that fall far short of the WTO's recommended 60-day comment period.<sup>3</sup>

Second, China claims that numerous Chinese standards are in line with international standards; however, they frequently contain key differences that require companies to modify products and practices specifically for the Chinese market, which takes time and increases costs for foreign companies. Moreover, China's reluctance to allow foreign experts to participate in the standards-setting process in a truly robust and influential way has limited technical experts' ability to counter these trends.

Third, China seeks to promote its standards in international standards setting bodies. The cumulative effect of China rapidly publishing and promoting "China-unique" standards that favor Chinese companies will not only limit foreign companies' access to the Chinese market but also reshape international standards in favor of Chinese companies.

Recently, China has also sought to codify its standards-setting process in law through revision of its Standardization Law. The Standardization Law presents numerous requirements unique to China, including public disclosure requirements for internal company practices that will add unnecessary costs and risk making public sensitive company data and practices. For example,

---

<sup>3</sup> The WTO TBT Agreement Code of Good Conduct calls for a 60-day comment period and mandatory reply to all comments received by domestic and international stakeholders.



the Law requires that companies disclose “enterprise standards,” which are related to the features and performance of a company’s product. In addition, the inclusion of a preference for indigenous innovations in the Law creates trade barriers that would conflict with China’s obligations under the WTO TBT Agreement. In order to counter these trends, we must ensure that countries’ national standardization practices are fully compliant with international norms and WTO obligations that apply to a central government standardizing bodies.

### 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 2017 alone, the U.S. exported \$23 billion worth of ICT goods to China.<sup>4</sup>And, as of 2015, China was the second largest export market for U.S. commercial ICT services exports in Asia. Put simply, companies cannot be truly global if they give up 25 percent of the global market.

Customer retention is another important factor. Customers operate globally, and they expect leading American companies to offer services where they need them. If U.S. companies cannot operate in China, they risk ceding to Chinese companies in the global market, as customers – particularly those that depend on services such as Cloud – will seek out companies that provide services in all markets in which they operate.

Ultimately, companies face two unappealing options: loss of the Chinese market and diminished global competitiveness OR operating in a risky and highly-restricted but profitable and important market.

### What the U.S. Government Can Do to Change the Status Quo

ITI appreciates that the U.S. government recognizes that there is a market-access problem in China and has taken steps to address it, including USTR’s Section 301 investigation and subsequent report regarding China’s unfair trade policies and practices. 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. consumers, businesses, and the economy. I’d like to outline a few basic tenets below.

#### *Do No Harm to U.S. Consumers and Businesses*

Tariffs are counterproductive. The broad array of products identified by USTR for increased tariffs will have a significant negative impact on the U.S. economy across multiple sectors, increasing prices for consumers and businesses. The administration has claimed that consumer

---

<sup>4</sup> U.S. GDP was \$19.739 trillion in the fourth quarter of 2017.



goods will be exempt from tariffs; however, the structure of the global supply chain and the numerous product inputs from across the globe factoring into final products make it virtually impossible to exempt consumer goods from the increased costs attributable to tariffs. For example, smart home devices like connected thermostats would increase in price as a result of these tariffs,<sup>5</sup> as the final product ships from China though it is the product of U.S. know-how and innovative technology. Additionally, tariffs on key components of televisions, touch-screen devices, and cameras are all captured by the current list of potential tariffs and, if imposed, will yield increased prices on the final product. In short, tariffs ultimately amount to a tax on American consumers.

### *Don't Go It Alone – Leverage International Pressure and Coalitions*

We cannot ignore the global importance of the Chinese market and we cannot unilaterally punish China into changing its behavior. It is misguided to assume that publically – and unilaterally – punching China will change behavior. As we are seeing play out in real-time, this will only prompt China to retaliate in order to demonstrate that it won't be bullied by the United States.

We must focus on what works. Multilateral pressure is one of the few tactics that has caused China to change course. For example, in 2004, China proposed an international standard for wireless security, “Wireless Authentication and Privacy Infrastructure (WAPI).” China subsequently tried to make this mandatory for wireless LAN equipment in China. Members of the International Standards Organization (ISO) refuted the mandatory status of the standard and slow-rolled its approval as an international standard. With the support of business groups and standards group around the world, ISO ultimately rejected the proposal for WAPI to become an international standard in 2006.

In 2009, China required that “Green Dam-Youth Escort” screening software be installed on computers to be sold in China, ostensibly for the purpose of restricting pornographic imagery. However, the software had clear “censor-ware” capabilities with intrusive surveillance potential; cybersecurity experts also noted serious security vulnerability concerns. The international community across businesses, rights groups and NGOs, and the United States, Japanese, and EU governments combined intense pressure on numerous fronts, which led to the delay and ultimate suspension of the program.

Finally, while it is fair to say that bringing China into the WTO has not had the positive impact that we hoped for, it does create the opportunity to hold China accountable. Thus far, China

---

<sup>5</sup> <https://www.federalregister.gov/documents/2018/04/06/2018-07119/notice-of-determination-and-request-for-public-comment-concerning-proposed-determination-of-action>





has not faced any real consequences for its actions. It's time for the international community to stand united and tell China that its market access restrictions will no longer be tolerated.

### *Compete with China and Invest in our Future*

Punishing China and restricting Chinese investment in the United States alone will not help us achieve our goals. We must invest in our own future. This means investing in research and development, education, science and technology, artificial intelligence (AI), and incentivizing innovation – all of which are key to our future economic and societal prosperity.

We 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 we of course want a level playing field, we must also step up our game. China is making a concerted and strategic effort to invest and plan for its economic and technological future. The United States can and should do more. According to [the World Economic Forum](#), in 2016 China had 4.7 million recent STEM graduates while the United States had 568,000 graduates. In 2017, China accounted for 48 percent of the total global investment in AI startup funding, while the U.S. accounted for 38 percent. In monetary terms, China invested \$7.3 billion in AI while the U.S. invested \$5.77 billion.<sup>6</sup>

China is also on track to outpace the United States in other areas. For example, according to a 2018 International Data Corporation (IDC) report, the U.S. will spend \$22 billion on smart city development this year. China is close behind with projected spending at \$21 billion.<sup>7</sup> As of 2015, there were 1,000 smart city pilot plans in the works worldwide, 500 of which were located in China.<sup>8</sup>

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**

The tech sector faces serious challenges in accessing the Chinese market. We must address these challenges aggressively, but we also cannot ignore or deny the significant role China plays

---

<sup>6</sup> <https://www.technologyreview.com/the-download/610271/chinas-ai-startups-scored-more-funding-than-americas-last-year/>

<sup>7</sup> <https://www.techrepublic.com/article/smart-cities-expected-to-invest-80b-in-technologies-in-2018/>

<sup>8</sup> <https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/public-sector/deloitte-nl-ps-smart-cities-report.pdf>



in the global economy as a key piece of the global supply chain, supplier of products and components, and a vital market for U.S. goods and services.

There is no question that it is time to demonstrate to China that there are consequences for its unfair trade actions, and that the international community will not tolerate blatant disregard for international norms and principles of free trade. However, addressing China's behavior must not come at a cost for American consumers and businesses. And we cannot let our efforts distract us from strengthening and developing our own tech sector and economy. We do ourselves a disservice if we downplay the need to invest in our ability to compete with an increasingly innovative and technologically advanced China.

Market access in China is a complex and multi-faceted problem that will require us to be strategic on numerous fronts. With the right approach, we can address these serious issues in a way that benefits, not harms, the United States and the global economy.

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 evolving U.S.-China trade relationship. We stand ready to work with you to address these challenges. I look forward to answering your questions.