July 31, 2017

Mr. Ed Gresser
Chair of the Trade Policy Staff Committee
Office of the United States Trade Representative
600 17th Street N.W.
Washington, DC 20508

RE: Comments in Response to Executive Order Regarding Trade Agreements Violations and Abuses.

Dear Mr. Gresser:

I write in response to your Federal Register Notice requesting public comments regarding the administration’s performance review of U.S. trade agreements.

The following written submission draws on previous reports published by the Information Technology and Innovation Foundation—the top-ranked science- and technology-policy think tank in the United States—including its expertise and previous work on a range of trade- and innovation-related issues.

Sincerely,

Nigel Cory
Trade Policy Analyst, The Information Technology and Innovation Foundation
CONTENTS

Introduction........................................................................................................................................3

  The Nature of U.S. Innovation Industries.........................................................................................4
  Market Conditions Needed to Maximize Innovation...........................................................................5

China....................................................................................................................................................6

  Targeting and Undermining Foreign Intellectual Property...............................................................9
    The Use of Anti-Monopoly Laws to Target Intellectual Property......................................................11
  Failing to Live Up to Commitments on Government Procurement ...................................................11
  Discriminatory Laws and Regulations..............................................................................................12
    Discriminatory Cybersecurity Policies ............................................................................................12

Discriminatory Technology Standards..............................................................................................14

Ongoing Use of Production and Export Subsidies.............................................................................15

Weak to Non-Existential Transparency and Reporting of Trade Policies.............................................16

Restrictive Market Access for Cloud Computing and Telecommunication Services .........................17

China’s Non-Market Economy Status ...............................................................................................19

Central and South America ..............................................................................................................19

  Colombia........................................................................................................................................20
  Costa Rica .......................................................................................................................................20
  Guatemala .......................................................................................................................................21
  Honduras .......................................................................................................................................21
  Nicaragua .......................................................................................................................................21
  Panama ........................................................................................................................................21
  Peru ...............................................................................................................................................21

South Korea – Stopping or Making it Hard to Transfer Data...............................................................22

Vietnam – Restrictions on Over-the-Top Services .............................................................................24

Endnotes..............................................................................................................................................26
INTRODUCTION

International trade is a crucial enabler for innovative sectors at the heart of U.S. economic competitiveness, including renewable energy, aerospace, life sciences, semiconductors, information communications technology (ICT), and digital content. Trade agreements provide the market access and rules that allow firms in these sectors to maximize their potential to innovate, and in doing so, help drive further improvements in U.S. consumer welfare and standards of living. However, the U.S. government needs to ensure that all counterparties to U.S. trade agreements live up to the commitments they made in signing them.

The U.S. Trade Representative’s (USTR’s) investigation into U.S. trade agreements is a welcome review of the status of U.S. trade agreements, the policies of its trading partners, and whether they’re living up to their side of the agreement. Most U.S. trade partners generally play by the rules. However, as this submission outlines, some U.S. trade partners have violated, abused, and/or discriminated against U.S. firms and their goods and services in contravention of bilateral/regional trade agreements with the United States or in joining the multilateral trading system under the World Trade Organization (WTO). On the latter, China stands out for the way it has systemically broken, ignored, and/or gamed the world trading system to advance its own development, to the detriment of many sectors of the U.S. economy. These unfair trade policies deserve greater scrutiny and action by the U.S. government.

America’s most-innovative sectors deserve to be a central factor in USTR’s investigation as they drive long-term economic growth. The U.S. Department of Commerce reported in 2010 that technological innovation can be linked to three-quarters of the United States’ growth rate since the end of World War II. Technological innovation shapes the entire U.S. economy, as the Information Technology and Innovation Foundation (ITIF) reports in “High-Tech Nation: How Technological Innovation Shapes America’s 435 Congressional Districts.” The U.S. economy is extremely diverse, and different regions specialize in different products and services, but all industries have an opportunity to capitalize on technological innovation to increase their productivity and competitiveness. The role of U.S. trade policy should be to support these firms by ensuring they have clear and fair access to foreign markets.

America’s innovative industries are among the country’s most dynamic and impactful. One recent study found that America’s 50 most-advanced industries (in terms of having the highest research and development (R&D) intensities and highest share of STEM [science, technology, engineering, and mathematics] workers) accounted for 17 percent of U.S. GDP and employed 9 percent of workers. Moreover, those 50 industries employed 80 percent of the nation’s engineers; performed 90 percent of private-sector R&D; generated approximately 85 percent of all U.S. patents; and accounted for 60 percent of U.S. exports. America’s innovation-based, high-tech industries are a vital driver of the country’s traded-sector competitiveness and a key provider of high-wage, high-value-added jobs. Protecting the ability of these sectors to compete fairly on global markets by enforcing trade commitments America’s trade partners have made in multilateral, plurilateral, and bilateral trade commitments should be a paramount objective of the Trump administration’s trade policy.
The Nature of U.S. Innovation Industries

Around the world, countries are competing for market share in high-wage, innovation-based industries. Unfortunately, as this global race for innovation advantage intensifies, many countries have turned to “innovation mercantilism”—a strategy that seeks prosperity by imposing protectionist and trade-distorting policies that tip market scales to expand domestic technology production.

These destructive, “beggar-thy-neighbor” tactics—such as forcing companies to transfer the rights to their technology or relocate their production, research and development (R&D), or data-storage activities—are intended to either replace imports with domestic production or to unfairly promote exports. Countries increasingly are using such innovation mercantilist policies in high-value tech sectors such as life sciences, renewable energy, computers and electronics, and Internet services. To understand how countries can enact policies that detract from U.S. innovation, it’s important to understand the nature of innovation industries and market settings that are needed to maximize innovation.

True innovation industries share four key characteristics in common. First, innovation—the regular development of new products and processes—is central to their competitive success. While all industries, even “traditional” ones, innovate to some extent, true innovation industries are ones where the rapid and regular development of new processes, products, or services—many of them disruptive in nature—is critical to their competitive advantage. For example, biotechnology and semiconductors are innovation industries, as their success depends not on making the current product marginally cheaper, but on inventing the next-generation drug or semiconductor.

A second key characteristic of innovation-based industries is that their marginal costs significantly exceed their average costs. The software industry provides the most extreme example of this. It can cost hundreds of millions of dollars to produce the first copy, but additional software can be produced at virtually no cost. Likewise, the cost to develop a new prescription medicine that gained marketing approval in 2013 reached $2.6 billion. Additional post-approval R&D costs of more than $300 million “boost the full product life cycle cost per approved drug” to close to $3 billion.\textsuperscript{iv} However, incremental copies of the initial medicine (one more pill off the production line) can be produced at cost. Similarly, it took Boeing almost eight years of development work and more than $15 billion before a single 787 Dreamliner was sold.\textsuperscript{v} Total 787 Dreamliner costs have now reached $32 billion.\textsuperscript{vi} That $32 billion gets built into the cost of every 787. Economists describe such industries as experiencing increasing returns to scale, but not all industries share this characteristic. For example, a study of more than 1,000 European companies found increasing returns to scale for high-tech firms, but decreasing returns to scale for low-tech ones.\textsuperscript{vii}

Third, innovation industries depend more than other industries on intellectual property (IP), both science- and technology-based IP but also the IP embodied in creative works. For example, software depends on source code; content creators depend on copyrights to protect their work from expropriation; life sciences firms depend on discoveries related to molecular compounds; and aerospace depends upon materials and
device discoveries. The challenge, of course, is that intangible capital assets, such as IP, are more easily appropriable than tangible capital assets.

Finally, precisely because innovation industries are so knowledge intensive, they depend upon the unfettered movement of knowledge, information, and data across borders.³⁸ That is because creating value in the modern economy increasingly depends upon generating actionable insights from data. For example, 50 percent of global services trade depends on underlying data flows.³⁹

These four factors that characterize an industry as an innovation industry—constant innovation, high fixed costs relative to marginal costs, dependence on IP, and dependence on information—have significant ties to globalization and trade, and therefore, to the policies that trading partners enact as part of trade agreements with the United States or as part of the WTO.

**Market Conditions Needed to Maximize Innovation**

Assessing the impact of trading partners’ trade and economic policies on U.S. innovation also requires an analysis of the three factors that innovation industries depend on to maximize innovation through international trade:

1. ** Ensuring the largest possible markets.** Firms in many innovation-intensive industries are global because they require scale. For innovation industries with high fixed costs of design and development but relatively low marginal costs of production, larger markets better enable them to cover those fixed costs, so that unit costs can be lower, and revenues for reinvestment in innovation higher. Higher sales allow more revenue to be invested back into generating more innovation. Therefore, trade barriers—such as high tariffs, localization barriers to trade, or restrictions on the ability of service enterprises to compete across international borders—limit scale economies at both the firm and establishment level (a firm being comprised of multiple establishments). Barriers that limit market access by foreign firms—in favor of domestic firms—raise global innovation costs by enabling more firms than necessary.

2. **Limiting nonmarket-based competition.** Large markets enable firms to sell more. But if larger markets come with more competitors, total sales per firm can remain the same or even fall. But isn’t this competition good for innovation? In fact, many studies have shown that innovation and competition can be modeled according to an inverted “U” relation, with both too much and too little competition producing less innovation. One study of U.K. manufacturing firms found this relationship.³⁷ Others, including Scherer and Mukoyama, have found similar patterns.³⁸ In a study of U.S. manufacturing firms, Hashmi found that too much competition led to reduced innovation in a slightly negative relationship.³⁹ Normally, markets will not produce an excess number of competitors. But governments often do—through financial bailouts, discriminatory government procurement, or other policies favoring weaker domestic firms. These policies let weak firms remain in the market, drawing sales from stronger firms and reducing their ability to reinvest in innovation.
3. **Ensuring strong IP protections.** Firms in innovation-based industries depend on intangible capital, much of it embodied in IP. Strong IP rights spur innovative activity by increasing the appropriability of the returns to innovation, enabling innovators to capture more of the benefits of their own innovative activity. By raising the private rate of return closer to the social rate of return, intellectual property addresses the knowledge-asset incentive problem, allowing inventors to realize economic gain from their inventions, thereby catalyzing economic growth. In addition, as they capture a larger portion of the benefits of their innovative activity, innovating companies obtain the resources to pursue the next generation of innovative activities. However, if competitors can enter and/or remain in the market because they obtain an innovator’s IP at less than the fair market price (either through theft or coerced transfer), they are able to siphon sales that would otherwise go to innovators.

All three factors get to the core challenge for innovation industries: Investment in innovation is uncertain, and therefore higher than normal profits on those innovations that succeed are necessary. Because innovation is about risk and uncertainty, failure is common; for every Apple succeeding with an iPad, there are many IT companies that fail. Moreover, innovation industries face not just loss of market share from competition, but loss of existence. This reality evokes Schumpeter’s dictum that “every piece of business strategy must be understood against the perennial gale of creative destruction.”

Innovation industries depend on so-called “Schumpeterian profits”—the profits that arise when firms are able to appropriate the returns from innovative activity. For if firms are assured at best only normal returns on successful innovation, none would undertake the enormous risk of investing in it. Moreover, because innovation is so expensive, higher returns endow companies with the capital to invest more in R&D and other innovation-based activities, perpetuating a virtuous cycle of innovation.

**CHINA**

Now more than 15 years after China joined the WTO in 2001, the vision of China embracing a rules-governed, market-based global trade system has yet to materialize. To be sure, China did reform thousands of domestic laws and has complied with many of its WTO commitments—such as joining the Information Technology Agreement (ITA) and reducing average tariffs on industrial products. But all too often, one step forward has been met with two steps backward, as China has erected new, often behind-the-border non-tariff barriers (NTBs) to more than compensate for concessions elsewhere. To be clear, a China that participates in the global trading system while abiding by the rules and norms of the WTO system is a positive for the global economy. However, a China that uses the WTO as a shield to protect its innovation mercantilist policies is not.

China’s innovation mercantilism stands in stark contrast to the picture painted by many officials when China joined the WTO. For instance, Mike Moore, the WTO’s director-general in 2001, gushed that “China’s decision to join the WTO is momentous. Committing itself to WTO rules will entrench market-based reform and strengthen the rule of law. … China’s opaque and arbitrary trade and investment rules will
become transparent, stable, and more predictable.”

Moore assuaged those concerned China might not live up to its commitments, intoning that, “A more open China brings benefits for everybody. … China knows it has to stick to its WTO commitments. If it doesn’t, the U.S. or any other WTO member government can use the organization’s dispute-settlement procedures to ensure it does.” For its part, the WTO itself stated:

China has agreed to undertake a series of important commitments to open and liberalize its regime in order to better integrate into the world economy and offer a more predictable environment for trade and foreign investment in accordance with WTO rules.

Yet the reality is that China’s aggressive innovation mercantilism has only grown stronger in recent years, as China seeks absolute advantage across an ever-wider range of advanced-technology industries. In fact, as a recent The Economist article noted, even Long Yongtu, who as China’s chief trade negotiator in 2001 helped the country win WTO admission, has admitted that China is now moving further away from the organization’s principles. As The Economist writes, “to modernize its economy, China has remained wedded to industrial policies, state-owned enterprises, and a ‘techno-nationalism’ that protects and promotes home-grown technologies.”

The seminal document outlining China’s pursuit of absolute advantage in many high-tech sectors (and particularly ones in which U.S. firms have long been global leaders) was the “National Medium- and Long-Term Program for Science and Technology Development (2006-2020),” the so-called “MLP.” The MLP outlined China’s plan to master 402 core technologies, everything from intelligent automobiles to semiconductors and high-performance computers. The MLP essentially announced that modern Chinese economic strategy sought absolute advantage across virtually all advanced industries. It fundamentally rejected the notion of comparative advantage—which holds that nations should specialize in the production of products or services at which they are the most efficient and trade for the rest. Instead, China’s goal today is to dominate in production of both advanced-technology products such as airplanes, semiconductors, computers, pharmaceuticals, and commodity manufacturing.

Ultimately, Chinese policymakers wish to autarkically supply Chinese markets for advanced-technology goods and services with their own production while still benefitting from unfettered access to global markets for their technology exports and foreign investment, the latter designed to acquire and integrate into Chinese firms’ know-how, often based on foreign technology. The MLP has been reinforced and expanded through other strategies, such as China’s “Made in China 2025” plan. As the Mercator Institute for China Studies (MERICS) in Germany writes in its report, “Made in China 2025: The Making of a High-Tech Superpower and Consequences for Industrial Countries,” “Made in China 2025 in its current form [means that] China’s leadership systematically intervenes in domestic markets so as to benefit and facilitate the economic dominance of Chinese enterprises and to disadvantage foreign competitors.” This is diametrically opposed to the fundamental principles that underpin the multilateral trading system embodied in the WTO.
As the ITIF has documented across a series of reports—including “False Promises: The Yawning Gap Between China’s WTO Commitments and Practices,” “The Worst Innovation Mercantilist Policies of 2016,” “Stopping China’s Mercantilism: A Doctrine of Constructive, Alliance-Backed Confrontation,” and most recently in testimony before the congressionally chartered U.S.-China Economic and Security Review Commission on Chinese investment in the United States—China has deployed a vast panoply of innovation mercantilist practices that seek to unfairly advantage Chinese producers over foreign competitors.\textsuperscript{six}

As this submission outlines, these practices have included forced IP and technology transfer or forced local production as a condition of market access; theft of foreign IP; curtailment and even outright denial of access to Chinese markets in certain sectors; manipulation of technology standards; special benefits for state-owned enterprises (SOEs); and capricious cases designed to force foreign companies to license technology at a discount.

One of the challenges is that many of China’s policies violate the spirit, if not always the letter, of trade rules the country agreed to uphold in joining the WTO. In response, America often pushes back bilaterally rather than by initiating a trade dispute at the WTO. A contributing factor to the lack of more cases is that U.S. companies face the real threat of retaliation from the Chinese government if they provide evidence against it in a trade case. Nevertheless, USTR should bring forth more cases, whether industry supports them or not (assuming the facts can be adequately developed). In particular, USTR should be more aggressive in initiating trade disputes, or using the threat of disputes, to change China’s behavior.

Put simply, the United States needs to take a more assertive lead in defending, promoting, and building upon the open and rules-based global trading system. It must lead determined efforts to contain and roll back Chinese mercantilism and enroll like-minded countries in that task. Our allies may follow, but they will not act without U.S. leadership. The reality is that the United States is the leading representative of a community of nations that have chosen market-led capitalism over state-led capitalism, and so it bears particular responsibility for containing and rolling back Chinese mercantilism, thus encouraging other nations to choose a more rules-based approach to trade and investment.

Rolling back Chinese innovation mercantilism will be vital for the competitiveness of both the U.S. economy and U.S. enterprises, particularly those in advanced industries. U.S. enterprises across virtually all manufacturing sectors and every advanced-technology sector—from aerospace and biotechnology to ICT products, Internet, digital media, and clean energy—have been harmed by China’s aggressive use of innovation mercantilist policies. Moreover, China’s policies have inflicted considerable harm upon the U.S. economy, its exports, and employment.

Achieving real change in China will not be easy. China’s unique economic system is at the heart of the challenge facing the United States and the international community’s efforts to painstakingly set up (and defend) a market- and rules-based trading system. China is unique due to the interaction of several factors,
but especially the Communist Party’s central role in governing the economy, including many parts of the private sector, as well as the lack of transparency and rule of law.” China’s unique approach was neither fully appreciated nor accounted for by negotiators at the time of China’s WTO accession. Since accession, China has not converged (as negotiators hoped) toward an economic model of the type which the WTO was built to accommodate. This mismatch has become much clearer now that China has grown into a major player in the global economy yet still unabashedly uses its unique system to manipulate loopholes in the system. It is becoming even clearer now that a special, time-limited “nonmarket economy” WTO accession provision, which was supposed to provide time for an economic transition, has run out without China’s transition to a market economy occurring. This clash of systems requires the United States and other major economies to confront head on—and beyond mere WTO litigation—the challenge that China’s actions pose to their individual trading relationships and to the trading system as a whole.

As part of this, the United States should not rush into negotiating a new Bilateral Investment Treaty (BIT) with China without getting China to fully abide by its prior WTO commitments. China is already obliged under existing WTO commitments to address many issues that a potential BIT would contemplate, such as those that prohibit forced technology transfers as a condition of market access, yet China has made extensive use of such policies in a variety of sectors. China needs to fundamentally recommit to the rules of the international trading system and abide by the letter and the spirit of the rules, lest the United States again allow China to benefit from international trade rules without having to abide by them.

**Targeting and Undermining Foreign Intellectual Property**

Intellectual property issues remain a major issue for U.S. companies operating in China. China is a regular designee on the U.S. Trade Representative’s Priority Watch List of worst offenders in terms of IP protection and enforcement. In addition, in December 2016, USTR announced the results of its 2016 Out-of-Cycle Review of Notorious Markets, which identified online and physical markets that exemplify key challenges in the global struggle against piracy and counterfeiting. Several Chinese markets were among those named as notorious markets.

Although China’s WTO accession agreement contains rules forbidding the country from tying foreign direct investment or market access to requirements to transfer technology to the country, it remains commonplace to require that firms transfer technology in exchange for being granted the ability to invest, operate, or sell in China. This despite the fact that in the November 2001 Report of the Working Party on the Accession of China to the WTO, “The representative of China confirmed that China would only impose, apply or enforce laws, regulations or measures relating to the transfer of technology, production processes, or other proprietary knowledge to an individual or enterprise in its territory that were not inconsistent with the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) and the Agreement on Trade-Related Investment Measures (TRIMs Agreement).”
Nevertheless, USTR annual reports to Congress on China’s WTO compliance continue to highlight its use of such discriminatory practices. Unfortunately, this shouldn’t be a surprise, as China has explicitly outlined aims for domestic production in many sectors, including through forced joint ventures (JVs) and tech-transfer provisions, as part of its “Made in China 2025” strategic plan.xxx As Harvard Business School professors Thomas Hout and Pankaj Ghemawat document in their report China vs the World: Whose Technology Is It?, Chinese technology transfer requirements as a condition of market access have affected scores of companies in industries as diverse as aviation, automotives, chemicals, renewable energy, and high-speed rail.xxxi To be sure, because such conditions contravene China’s WTO commitments, officials are careful not to put such requirements in writing, often resorting to oral communications to pressure foreign firms to transfer technology.xxxii In 2011, then-U.S. Treasury Secretary Timothy Geithner laid such concerns about China’s technology transfer requirements in the open, stating that “we’re seeing China continue to be very, very aggressive in a strategy they started several decades ago, which goes like this: you want to sell to our country, we want you to come produce here. If you want to come produce here, you need to transfer your technology to us.”xxxiii

China often denies such practices by pointing out that they are not in writing. But government action in China can and does occur by informal “administrative guidance” and this is very much the case with coerced technology transfer. Not only does this continue to happen, it’s actually getting worse, with Chinese officials insisting on transfers of more valuable technology. For instance, global auto brands are only allowed to manufacture cars domestically in China through joint ventures with local partners.xxxiv For example, China made General Motors’ access to subsidies for electric-vehicle purchases contingent on the company handing over the IP behind its electric hybrid car, the Volt. Ford was forced to do the same.xxxv In November 2016, Volkswagen was compelled to enter a JV if it was to be permitted to sell battery-electric and plug-in hybrid cars in China.xxxvi This continues despite the fact that China promised to remove these types of measures at the U.S.-China Joint Commission on Commerce and Trade (JCCT) in 2011.xxxvii

Indeed, the U.S.-China Business Council’s 2014 China Business Environment Survey reports that 62 percent of companies had concerns about transferring technology to China, while 20 percent reported that they had been requested to transfer technology to China within the past three years.xxxviii Likewise, a 2012 American Chamber of Commerce in China survey reported that 33 percent of its respondents stated that technology transfer requirements were negatively affecting their businesses.xxxix Put simply, technology transfer requirements as a condition of doing business in China remain a key pillar of China’s innovation mercantilist strategy.

Furthermore, in joining the WTO, China committed to uphold the TRIPS agreement, which provides protections for patents, copyrights, trademarks, service marks, industrial designs, digital content, and other intangible property. Unfortunately, Chinese IP theft grows unabated. As a recent MIT Sloan Management review article, “Protecting Intellectual Property in China,” noted, “Intellectual property protection is the No. 1 challenge for multinational corporations operating in China.”xxxx According to the U.S. International Trade
Commission, in 2009, U.S. IP-intensive enterprises conducting business in China reported losses of approximately $48.2 billion in sales, royalties, or license fees due to Chinese IPR infringement. That figure has continued to increase. Subsequently, The IP Commission Report on the Theft of U.S. Intellectual Property found that China accounted for nearly 80 percent of all IP thefts from U.S.-headquartered organizations in 2013, amounting to an estimated $300 billion in lost business annually. Likewise, a recent European Union-commissioned study found that, among European manufacturers, the loss of IP in China reduces their potential profits by 20 percent annually. Meanwhile, China still has one of the highest rates of unlicensed software usage in the world, with 74 percent of the software in use unlicensed and the market value of unlicensed software usage exceeding $8.7 billion in 2013. In a recent survey of the China Business Environment conducted by the U.S.-China Business Council, 98 percent of companies surveyed report that IP rights enforcement in China remains a concern for them.

The Use of Anti-Monopoly Laws to Target Intellectual Property

U.S. companies have also been targeted by China’s discriminatory use of anti-monopoly laws as an industrial development tool. China’s anti-monopoly law has been designed to treat legitimately acquired intellectual property rights as a monopolistic abuse, with Article 55 stating, “This Law is not applicable to undertakings’ conduct in exercise of intellectual property rights pursuant to provisions of laws and administrative regulations relating to intellectual property rights; but this Law is applicable to undertakings’ conduct that eliminates or restricts competition by abusing their intellectual property rights.” For the Chinese government, “abuse” means charging market-based IP licensing fees to Chinese companies.

This provision has been used to take legal action against companies whose only “crime” is to be innovative and hold patents. Indeed, the Chinese law allows compulsory licensing of IP by a “dominant” company that refuses to license its IP if access to it is “essential for others to effectively compete and innovate.” And with Chinese courts largely rubber-stamping the government’s dictates, foreign companies have little choice but to comply. All too often, complying means changing their terms of business so that they sell to the Chinese for less and/or transfer even more IP and technology to Chinese-owned companies, often after paying substantial fines. To be clear, this tying of IP to monopolistic behavior is unique to China, and is not part of antitrust law in Europe or the United States.

Failing to Live Up to Commitments on Government Procurement

In joining the WTO, China agreed to join the Government Procurement Agreement (GPA), which prohibits restrictions on government purchases between member countries in accordance with national treatment principle and further committed “to full transparency and non-discrimination (MFN) in government purchases.” But while China has now tabled five offers (relating to the levels of government and types of procurement activities that would be covered by its GPA commitment), USTR notes that, “To date, the United States, the European Union, and other GPA parties have viewed China’s offers of coverage as highly
disappointing in scope and coverage. In other words, more than 15 years after it joined the WTO, China has yet to make a credible offer for GPA coverage, despite its commitment to do so swiftly in 2001.

Beyond GPA-related commitments regarding well-recognized government agencies (such as Ministries of Health and Transportation) in joining the GPA, China also “agreed that it will ensure that state-owned and state-invested enterprises will make purchases and sales based solely on commercial considerations, such as price, quality, availability and marketability, and that it will provide U.S. firms with the opportunity to compete for sales and purchases on non-discriminatory terms and conditions.”

Yet these commitments fly in the face of explicit Chinese efforts to curtail Chinese government agency and state-owned enterprises’ procurement of U.S. enterprise-developed or manufactured information and communications technology products. For example, in 2014, the Chinese central government ruled that government offices were prohibited from running Windows 8 (even though most versions were pirated rather than paid for). Around the same time, the Chinese government also announced its scarcely concealed “De-IOE campaign” designed to pressure Chinese companies, especially SOEs, to replace their IBM, Oracle, and EMC products with Chinese-made products and services.

**Discriminatory Laws and Regulations**

China continues to discriminate against U.S. firms across a range of industries, something USTR notes in its 2014 Report to Congress on China’s WTO Compliance. As the report explains, “China’s industrial policies on automobiles and steel call for discrimination against foreign producers and imported goods … discriminatory treatment also remains prevalent in a variety of services sectors.” Moreover, certain aspects of China’s legal framework, such as China’s extensive use of administrative licensing, “create opportunities for Chinese government officials to treat foreign companies and foreign products less favorably than domestic companies and domestic products.” This is despite China’s agreement to abide by the WTO’s core principles—those of most-favored nation (MFN) and national treatment—that constrain and guide WTO members’ policies relating to trade in goods.

**Discriminatory Cybersecurity Policies**

The Chinese government continues to use national security, cybersecurity, and other legal reforms as vehicles for mercantilist objectives. On November 7, 2016, China enacted a new Cybersecurity Law that introduces (further) restrictive requirements on foreign technology companies: *The Economist* aptly described it as a “techno-nationalist Trojan horse.”

China’s new cybersecurity law—through discriminatory standards and forced local data-storage requirements—reinforces existing policies that segment its citizens and tech firms, in addition to its broader Internet ecosystem, from the rest of the world. The law is significant, as it is China’s first to enact rules on the collection and use of personal data. The law forces companies in “critical information infrastructure” to store
users’ “personal information and other important business data” in China, a concept known as “forced localization.”

The cybersecurity law affects a large portion of China’s technology market, as the country is taking an expansive view of what is “critical information infrastructure” (CII). The basis of China’s position is thus far broadly defined as information infrastructure in sectors that may seriously jeopardize national security, the national economy, and people’s livelihoods or public interest, should such infrastructures malfunction or be subject to damage or data leakages. Indicative of this broad reach, sectors that have been cited for inclusion include public communication and information services, energy, transportation, water resources utilization, finance, public service, and e-government affairs.

China may use the law to expand an existing—and controversial—cybersecurity regulation that is highly discriminatory toward foreign tech firms and products. The cybersecurity law states that China will introduce a cybersecurity multilevel protection scheme (MLPS) for ICT products used in network security by CII sectors. This requirement is perhaps based off an existing MLPS that China has applied for information security (although this is unclear from the wording in the law). This potential relationship raises serious concerns for foreign technology companies, as this earlier MLPS was highly discriminatory—it prohibited certain sectors from using foreign IT products and forced foreign companies to transfer IP and source code to China for review.

Equally troubling is the potential for China to use the law to revive the use of a high-discriminatory standard for IT products—the so-called “secure and controllable” concept—and intrusive security audits, both of which can be used to discriminate against foreign firms and to steal valuable intellectual property. The law calls for the use of “secure and trusted” network services and productions, without defining the term. Current deliberations by China’s National Information Security Standards Technical Committee (NISSTC) on what this concept means (see below) and past Chinese government policy proposals point toward its mercantilist intent. This concept, along with its analogous “independent and controllable,” “secure and controllable,” or “indigenous and controllable” terms have been a part of Chinese technology policymaking debates ever since the country backed down on implementing such a rule as part of a banking law in 2015. That proposed banking law used a “secure and controllable” provision as part of an explicit aim to replace foreign technology goods with local ones. China decided to “withdraw” this provision after it generated significant opposition from tech companies and trading partners, especially the United States.

China essentially wants to force software companies, network-equipment makers, and other tech companies to disclose source code to supposedly prove their products can’t be compromised by hackers. Source code—the instructions that make a computer program run—enable technology to do the amazing things it does. For companies developing software, protecting source code is necessary to prevent other entities from stealing and free riding on the large research and development costs associated with software development. Source code is at the heart of a company’s competitive advantage, but being digital, it is at heightened risk of duplication.
Given China’s poor protection of intellectual property, not to mention its role in the cybertheft of foreign trade secrets, it’s unsurprising that foreign firms and trading partners, such as the United States, have reasonable fears that such intrusive inspections are simply a way to access and steal valuable intellectual property.

Fears about China’s mercantilist intent have been confirmed during the process to define standards and key concepts under this law. Foreign companies submitted comments on implementing provisions, such as the definition of “secure and controllable,” to China’s NISSTC after the law was released. Some of Microsoft’s comments focused on legitimate concerns about the utility in viewing source code for cybersecurity purposes, stating in its comments to NISSTC that “sharing source code in itself can’t prove the capability to be secure and controllable. It only proves there is source code.”

Yet, indicative of China’s ulterior motives, the NISSTC rejected this feedback, saying that this comment was “not accepted.” This is despite the fact that Microsoft had already taken the significant step of providing Chinese authorities with viewing access to its source code at its “Transparency Center” in Beijing, a step that most other technology companies have not taken, given the risks of unauthorized disclosure. China’s reaction to Microsoft’s comments on the draft law is indicative of how intrusive the law is likely to be and how it may get even tougher than it already is for foreign technology companies to operate in China.

China’s underlying mercantilist intent was further evident in comments and feedback provided to the NISSTC by the chief engineer at China’s Ministry of Public Security’s Network Security Bureau, who commented on the draft regulations by stating “the big trend is called shifting to favour domestic production … but it can’t be written that way, so one calls it independent and controllable.” NISSTC’s response was to mark the comment “approved.”

**Discriminatory Technology Standards**

The more than 500,000 global technology standards in existence today provide the underlying foundation of the global technology marketplace, governing the design, operation, manufacture, interoperability, and use of nearly everything that humanity produces. As Panitchpakdi and Clifford note, in joining the WTO, China agreed to abide by the Agreement on Technical Barriers to Trade, which “prohibits the use of tests and standards as a way of discriminating unjustly against trading partners or protecting domestic industries.” In other words, the TBT prevents WTO members from using certifications and standards as a barrier to trade.

But as ITIF explains in “The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards,” China has made the development of indigenous technology standards, particularly for ICT products, a core component of its industrial development and economic growth strategy. China has committed to developing unique national standards for dozens of high technology and ICT products—in many cases where international standards already exist—developing homegrown standards for everything from 3G mobile telecommunications services and wireless local area networks to encryption technologies and...
the Internet of Things. In some cases, such as with WAPI (the Wireless Local Area Network Application and Privacy Infrastructure standard that China developed as an alternative to the WiFi standard), China attempted to require that all wireless networking products sold in China would have to be WAPI-compliant and use its encryption method, in contravention of its commitment to let foreign enterprises use desired technologies in the provision of telecommunication services.

As USTR notes, “China has continued to pursue unique national standards in a number of high technology areas where international standards already exist, such as 3G and 4G telecommunications standards, Wi-Fi standards and information security standards. More commonly, however, Chinese officials “pressure foreign companies seeking to participate in the standards-setting process to license their technology or intellectual property on unfavorable terms.” Clearly, China has not met its commitments in the telecommunications sector, either in terms of market access or in refraining from promulgating technology standards that allow companies “to use any technology they choose to provide telecommunications services.”

**Ongoing Use of Production and Export Subsidies**

China’s entry into the WTO has done little to curtail its use of production or export subsidies. The subsides for China’s steel, energy, glass, paper, and auto parts industries have been particularly intensive, contributing substantially to Chinese firms’ competitiveness in global markets and to global overcapacity in these industries. As Usha and George Haley document in *Subsidies to Chinese Industry: State Capitalism, Business Strategy, and Trade Policy*, from 2000 to 2007, total energy subsidies to Chinese steel reached $27.1 billion. Meanwhile, China’s glass and glass-products industry received $30.3 billion in subsidies from 2004 to 2008, while the paper industry enjoyed $33.1 billion in government subsidies from 2002 to 2009, and the Chinese auto-parts industry received $27.5 billion in subsidies from 2001 to 2011. Moreover, since joining the WTO in 2001, China has yet to submit to the WTO a complete notification regarding the export or production subsidies maintained by China’s central and sub-central governments.

Furthermore, Chinese SOEs, many of which compete directly with foreign firms, receive significant benefits from all levels of Chinese government even if they are not profitable. For example, an in-depth 2011 study by the Unirule Institute, an independent Chinese think tank, found that in 2009 Chinese SOEs’ return on equity was about half the rate of non-state-owned enterprises, a substantial “subsidy” in and of itself. Moreover, without their government-granted advantages, including preferential financing from state banks and free land, Chinese SOEs would have operated at a 6.29 percent loss from 2001 to 2009. The ability to consistently lose money is a considerable subsidy compared with private foreign firms that must charge enough to make a reasonable profit. Another is the ability to get preferential government financing. As one study stated, “Our finding reinforces the widely held view that the Chinese financial system allocates resources towards poorly performing SOEs.” Such benefits for state-owned enterprises are a key reason why a 2013
survey by the American Chamber of Commerce in China found that 35 percent of firms stated that they were at a competitive disadvantage as a result of Chinese industrial policies that favored state-owned enterprises.\textsuperscript{xvi}

**Weak to Non-Existent Transparency and Reporting of Trade Policies**

Despite agreeing to do so when China joined the WTO, the Chinese government has consistently failed to provide the WTO and its trading partners with required information, translated into English (or another official WTO language), regarding policies related to trade in goods, services, intellectual property, subsidies, and foreign investment. Such transparency requirements may appear mundane and bureaucratic, but they are critically important to judging whether a country is abiding by its WTO commitments and whether grounds exist for a trade dispute.

The lack of transparency is part of the reason why USTR needs more people on the ground—to better monitor Chinese government actions. China’s governance system is notoriously opaque, complex, and multi-layered with overlapping and often inconsistent national, provincial, and municipal government policies. While such an approach is unnecessary for most trade partners, there is as noted an ongoing need for more USTR officials in China, as USTR has repeatedly reported that many aspects of Chinese policy are hidden away in unpublished measures (including legally unrecognized normative or regulatory documents), oral directives, and Communist Party secret red letter documents. These transparency concerns extend to the provincial and municipal governments which also regularly fail to publish their measures.\textsuperscript{xvii}

China also regularly fails to provide at least a 30-day period for public comment on drafts of trade- and economic-related regulations and rules as it agreed to at the U.S.-China Strategic and Economic Dialogue in 2008 and 2011. And Chinese agencies frequently adopt measures that take effect immediately when China’s WTO obligations require it to allow comments by other agencies and then to translate the measures into a WTO official language and officially publish them before implementation, except in certain cases (such as emergency). Multiple USTR reports show that China’s repeated failures to be transparent are part of a consistent pattern to avoid scrutiny for discriminatory and trade-distorting regulations rules and other measures involving subsidies, preferences, anti-competitive government practices, etc.\textsuperscript{xviii}

A specific example is China’s extensive use of subsidies and its blatant disregard for WTO-required transparency regarding such measures, as well as its failure to release detailed information in the government’s budget, the state capital operating budget (SCOB). Despite WTO commitments to submit regular notifications on what subsidies it provides, China did not file its first notification after WTO accession (in 2001) until 2006. Five years later, in 2011, it submitted a second notification for subsidies provided during the period 2005 to 2008. In 2015, it provided a third notification for the period 2009 to 2014. Beyond the delay, all three notifications were significantly incomplete and excluded numerous subsidies that the United States knows the Chinese central government provides. Moreover, none of these notifications included any of the extensive subsidies provided by provincial or local governments.\textsuperscript{xix} Since 2011, the United States has made formal requests (e.g., counter-notifications) for information from China regarding over 350 unreported
Chinese subsidy measures. China has failed to provide a complete and comprehensive response. Furthermore, China fails to provide a period for public comment for new trade-related laws and regulations—as it agreed to as part of its WTO accession and (again) at the U.S.-China Strategic and Economic Dialogue in 2011. Multiple USTR reports show that this is part of a consistent pattern by China to avoid scrutiny for discriminatory and trade-distorting rules, regulations, and subsidies.\footnote{xxx}

As USTR explains, China’s WTO notifications have “rarely included measures from other agencies that appear to require notification, such as the Ministry of Health, the Ministry of Industry and Information Technology, or the Ministry of Environmental Protection … China’s TBT [technical barriers to trade] measures continue to enter into force without having first been notified to the TBT Committee, and without foreign companies having had the opportunity to comment on them or even being given a transition period during which they could make necessary adjustments.”\footnote{xxxxi}

**Restrictive Market Access for Cloud Computing and Telecommunication Services**

China is contravening a number of WTO commitments in the telecommunications sector, including liberalizing foreign investment, agreeing to implement “pro-competitive regulatory principles,” and agreeing “to allow foreign suppliers to use any technology they choose to provide telecommunications services.”\footnote{xxxxii} As USTR notes, however, “China’s restrictions on basic telecommunications services, such as informal bans on new entry, a requirement that foreign suppliers can only enter into joint ventures with state-owned enterprises, and exceedingly high capital requirements, have blocked foreign suppliers from accessing China’s basic [telecommunications] services market.”\footnote{xxxxiii}

New regulations regarding cloud-computing services in China confirm its persistence in erecting barriers between its tech sectors and digital economy and that of the rest of the world. In March 2016, China made significant changes to the licensing and regulatory regime of Chinese telecom and Internet services that essentially exclude U.S. technology firms involved in cloud computing, big data, and other information services from operating in China. These regulations, again, reinforced the requirement for forced local data storage.\footnote{xxxxiv} For the vast majority of leading U.S. cloud-service providers, these regulations have essentially closed access to the Chinese market.

China enacted regulatory changes to make it even harder than it already was for U.S. companies to establish and operate Internet-based information services in the country. First, China released regulations for several services it considers valued-added telecommunication services (VATS). By categorizing Internet-based services (e.g., cloud computing, big data, and other information services) as telecommunication services, and not as “computer and related services,” China has given itself much greater freedom to restrict market access to U.S. firms. This is because China made commitments as part of its accession to the World Trade Organization (WTO) in 2001 to provide nondiscriminatory treatment and market access to foreign firms in “computer and related services.”\footnote{xxxxv} This category of Internet-based computer services includes email, voicemail, online information and database retrieval, electronic data interchange, and enhanced facsimile services, code and
protocol conversion, and online information and/or data processing.\textsuperscript{\textsuperscript{xxxvi}} Essentially, China’s approach is a technical work-around to avoid its commitment to open its market for Internet-based computer services to foreign competition.

Second, China introduced a requirement for telecom and Internet Service Providers (ISPs) to apply for licenses for each subcategory of services, raising the potential for government agencies to discriminate against foreign firms. For example, China’s new subcategory, “internet-based resources collaboration services,” means that providers of cloud computing application services, platform as a service, and software as a service would potentially have to apply for multiple licenses, given some firms and services cross over into multiple categories.

Third, China released new requirements that articulate the very small and restricted cloud-computing services space where foreign firms are allowed to operate. In October 2016, the Ministry of Industry and Information Technology released the “Notice on Regulating Business Behaviors in the Cloud Service Market,” which outlined how foreign cloud companies are forbidden from working via local partnerships in any capacity beyond “technical assistance.” It is not specified what is allowed under “technical assistance,” but based on current practice, it is likely to mean that foreign companies are only allowed to license their goods (software and hardware) to their (forced) local partners and show them how to use them. The notice further specifies several activities that cloud service providers cannot perform, such as sign contracts directly with end users.

These new restrictions on U.S. cloud service providers make an already restrictive situation that much worse. Strict entry requirements and (an already highly) discriminatory licensing process have largely kept foreign firms out of China’s market. To operate in China, foreign firms must set up a joint venture with a Chinese partner, which must be granted majority ownership (i.e., greater than 50 percent). A joint venture was a prerequisite for foreign firms to even apply for a license from Chinese authorities. Although there are over 20,000 local companies licensed to provide VATS in China, only 30 or so licenses have been issued to foreign companies, including five U.S. companies.\textsuperscript{\textsuperscript{\textsuperscript{xxxvii}}}

A few U.S. firms have successfully run the gauntlet and decided to operate in China within the confines of these strict conditions by partnering with large Chinese firms—for example, Microsoft with 21Vianet (China’s largest private data center operator) and IBM with a group of local companies.\textsuperscript{\textsuperscript{\textsuperscript{xxxviii}}} As described, these firms are severely restricted in what they can do, often being constrained to arrangements whereby they license their products to their local partners, who set up and run the data centers and cloud services and manage relations with end users.

This mercantilist approach to cloud computing is consistent with China’s ongoing efforts to develop a local cloud-computing sector that uses indigenously developed technology. China’s ambitions in the sector started as part of the country’s National Medium and Long-Term Plan (MLP) for Science and Technology Development (2006-2020). Building on this in 2010, China identified cloud computing as one of 11 strategic emerging
industries that would receive special attention and funding, all in pursuit of the goal of expanding access to cloud resources in China, developing indigenous cloud-computing technology, and creating an internationally competitive Chinese cloud-computing sector. More recently, the Ministry of Science and Technology’s 12th Five-Year Plan (2011-2015) paid particular attention to cloud computing, where the aim became to develop a cloud-computing standard based on indigenously developed technology. These policies, taken together, show China’s efforts to use mercantilist policies at home to support the development of “local champions,” who, ideally for China, will eventually become more innovative and competitive and able to compete in overseas markets—against the very tech firms that are unable not allowed to or impeded from competing in China.

**China’s Non-Market Economy Status**

Whether or not the United States recognizes China as a market-based economy or a nonmarket-based economy has significant implications, including in making key economic calculations of prices and costs estimated in antidumping and countervailing duty cases. The United States should continue to recognize China as a nonmarket economy. China’s continuing use of production and export subsidies, provision of below-market-cost inputs such as financing and access to land, continuing prevalence of state-owned or state-directed enterprises, and state-influenced procurement decision-making of SOEs and “private sector” firms alike (among other factors), as well as state planning around technology and intellectual property means the United States should continue to recognize China as a nonmarket economy.

The issue pertains to Article 15 of China’s Protocol of Accession to the WTO, which allowed WTO members to “disregard Chinese prices and costs in antidumping cases and instead base the calculation of dumping margins using external benchmarks.” Specifically, Article 15(a)(ii) states, “The importing WTO member may use a methodology that is not based on a strict comparison with domestic prices or costs in China if the producers under investigation cannot clearly show that market conditions prevail.” Chinese officials have argued that this practice should no longer be permitted after December 2016, pursuant to Article 15(d) of the Protocol, which states, “In any event, the provisions of subparagraph (a)(ii) shall expire 15 years after the date of accession.” But, as Hufbauer and Cimino-Isaacs point out, Article 15(a) (which informs article 15(d)) only really disappears “once China has established, under the national law of the importing WTO Member, that it is a market economy.” (They also argue that there need not only be a binary choice between “market” and “nonmarket” economy.) Regardless, as this submission has documented, China continues not to behave like a market-based economy, and should not be recognized as such.

**CENTRAL AND SOUTH AMERICA**

A thriving digital economy needs to have the right legal framework in place to encourage legal digital commerce to take place, especially as it relates to IP. Crucial to this are laws to establish how digital intermediaries are liable or not for their users who infringe copyright and if/how these intermediaries work with rights holders to remove this material. When this “safe harbor” framework is unbalanced—i.e., when
intermediaries are not liable, or when they have limited liability protections, but without corresponding responsibilities and mechanisms to help ensure IP is effectively protected—it undermines the ability of U.S. rights holders to benefit from their IP in today’s digital economy.

There are clear societal benefits to removing infringing content from the Internet. Widespread piracy has a negative economic impact, seriously harming the artists who create content and the technicians who produce it. Piracy limits the ability of content producers to create legitimate business models for selling digital content. It hurts U.S. competitiveness as the U.S. economy has a competitive advantage in content industries. Digital piracy remains a major issue despite the growth of innovative, legitimate alternatives to piracy. This is why it is critical for the United States to press those countries to follow through on the commitments they made in trade agreements with the United States to enact laws that would allow U.S. rightsholders to better protect their IP online.

**Colombia**

Colombia’s digital economy continues to grow, with digital music sales growing 94.9 percent in 2014. However, digital piracy remains a major issue in Colombia. In 2016, there were an estimated 500 million visits from Colombia to the top 108 Spanish-language piracy websites. Colombia is also ranked among the top 25 countries in the world in the number of peers discovered in peer-to-peer groups in which illegal copies of console video games were distributed. Colombia made commitments in its trade agreement with the United States that could help reduce this so that U.S. and local content providers (such as Google Play, iTunes, and YouTube) can better protect and use their IP.

Colombia committed to implement a liability framework for Internet service providers as part of the U.S.-Colombia Trade Promotion Agreement, but it has failed to do so after a number of failed legislative attempts. For example, in 2011, Colombia’s parliament passed Draft Law No. 241, which included liability exemptions for ISPs, including for mere conduit, caching, hosting, and information location tools (e.g., search, hyperlinks, and directories). It included exceptions for ISP liability for copyright infringement, so long as the ISP met the conditions for removing or disabling access to copyright infringing material. A subsequent attempt to implement a range of relevant IP laws was deemed unconstitutional on procedural grounds by Colombia’s Constitutional Court.

**Costa Rica**

In 2009, Costa Rica ratified the Dominican Republic-Central America free trade agreement (CAFTA-DR), which included commitments to enact liability limitation against service providers for copyright infringement, if conditions are met in terms of their service and their reaction to requests to remove copyright infringing material (Ch. 15, Section 15.11.27). Service providers also need to setup a “notice and takedown” mechanism to remove copyright infringing material. Despite this, in 2011, Costa Rica only adopted a “notice and notice” system in Decree No. 36,880 COMEX-JP.
Guatemala

Guatemala does not have any specific legislation regarding ISP liability, despite being a member of the U.S.-CAFTA-DR free trade agreement. This agreement included commitments to enact liability limitation against service providers for copyright infringement, if conditions are met in terms of their service and their reaction to requests to remove copyright infringing material (Ch. 15, Section 15.11.27). Service providers also need to setup a “notice and takedown” mechanism to remove copyright infringing material.iii

Honduras

Honduras does not have any specific legislation regarding ISP intermediary liability, despite being a member of the U.S.-DR-CA free trade agreement. This agreement included commitments to enact liability limitation against service providers for copyright infringement, if conditions are met in terms of their service and their reaction to requests to remove copyright infringing material (Ch. 15, Section 15.11.27). Service providers also need to setup a “notice and takedown” mechanism to remove copyright infringing material.iv

Nicaragua

Nicaragua does not have any specific legislation regarding ISP intermediary liability, despite being a member of the U.S.-DR-CA free trade agreement. This agreement included commitments to enact liability limitation against service providers for copyright infringement, if conditions are met in terms of their service and their reaction to requests to remove copyright infringing material (Ch. 15, Section 15.11.27). Service providers also need to setup a “notice and takedown” mechanism to remove copyright infringing material.v

Panama

Panama does not have any specific legislation regarding ISP intermediary liability, despite commitments it made in the U.S.-Panama Trade Promotion Agreement to enact a limited liability framework for services providers on copyright-infringement issues. Under Ch. 15.11, Article 15.11, Section 27(a), Panama committed to adopt “legal incentives for service providers to cooperate with copyright owners in deterring the unauthorized storage and transmission of copyrighted materials.”vi However, Panama does not appear to have adopted any such “incentives” through a notice and takedown system or a notice and notice system.

Peru

Similar to other South American countries, Peru’s digital market is growing strongly, including through legal distribution platforms, with digital music sales almost doubling in 2014. Yet digital piracy remains a major issue in Peru. From December 2015 through June 2016, individuals in Peru made 133 million visits to the top 108 Spanish-language piracy websites. Peru made commitments in its trade agreement with the United
States that could help reduce this so that U.S. and local content providers (such as Google Play, iTunes, and YouTube, etc.) can better protect and use their IP.

Peru does not have any specific legislation regarding ISP intermediary liability, despite commitments it made in the U.S.-Peru Trade Promotion Agreement concerning liability limitations and copyright, which included a “notice and takedown” system. However, Peru has not yet implemented these provisions. In late 2012, Peru’s government committed to enact these intermediate liability provisions, however no follow up action was taken.

SOUTH KOREA – STOPPING OR MAKING IT DIFFICULT TO TRANSFER DATA

The U.S.-South Korea free trade agreement (KORUS) provided meaningful new market access commitments in many areas, including services supplied across borders (such as through electronic means). Since coming into force in March 2012, U.S. services exports to Korea have substantially increased—from 2011 to 2014, U.S. services exports to Korea rose from $16.7 billion to $20.7 billion, an increase of 24.4 percent. Among the services industries that are benefitting are: audiovisual; finance; insurance; energy services; transportation, logistics, and express delivery services; information technology services; and telecommunications.

The free flow of data is essential to enabling the cross-border supply of many modern services. In this, KORUS set a first for U.S. trade policy by including binding rules on cross-border data flows. Article 15.8 states that:

“Recognizing the importance of the freeflow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.”

Furthermore, in Annex 13-B Korea committed to allow:

“…a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the institution’s ordinary course of business. Korea shall give effect to this commitment no later than two years after the date this Agreement enters into force.”

However, the first commitment was only hortatory in nature, so it was unclear at the time of signing what impact this would have on U.S.-Korea data flows. Since coming into force, U.S. firms have faced a number of issues regarding data flows.
For example:

- In South Korea, the Personal Information Protection Act requires companies to obtain consent from “data subjects” (i.e., the individuals associated with particular data sets) prior to exporting that data.\textsuperscript{ciii} The act also requires “data subjects” to be informed of who receives their data, the recipient’s purpose for having that information, the period that information will be retained, and the specific personal information to be provided. This is clearly a substantial burden on companies trying to send data across borders.

- South Korea had rules in place that impeded U.S. financial firms’ ability to transfer data overseas for processing, contravening the commitment in Annex 13-B. These restrictive rules included: getting approval before outsourcing data processing overseas; getting pre-approval before allowing data transfers; and restricting data transfers to the company’s head office, branches, or affiliates, thereby making it illegal to use third-party data processors. In mid-2015, Korea’s Financial Services Commission issued revised rules on the regulations of how financial institutions could outsource data processing to make this process much easier.\textsuperscript{ciii}

- South Korea has used data localization requirements to protect local e-commerce and online payment operators. Korea’s Regulation on Supervision of Credit-Specialized Financial Business prohibited e-commerce firms from storing Korean customers’ credit card numbers outside the country. In 2013, Korea slightly revised this rule by allowing certain foreign e-commerce firms (those with stores in more than five countries) to store such data abroad.\textsuperscript{civ}

- In 2014, South Korea enacted a law—Act on the Establishment, Management, Etc. of Spatial Data—that prohibits mapping data from being stored outside the country due to security concerns.\textsuperscript{civ} Korea has defended the policy as it wants to limit the availability of high-resolution commercial satellite imagery of Korea for national security reasons, even though such imagery is already available commercially.

- In 2015, Korea enacted the Act on Promotion of Cloud Computing and Protection of Users. Subsequent guidelines—the Data Protection Standards for Cloud Computing Services Guidelines—contain rules that effectively require data localization as cloud computing networks serving public agencies have to be physically separate from networks serving the general public. While these guidelines are only “recommended” and there is no penalty for non-compliance, Korean institutions usually follow such guidelines. This discriminatory policy may have a significant affect as it applies to thousands of institutions, such as educational institutions, public banks, and public hospitals.\textsuperscript{cvi}

These cases show that Korea has not been very “restrained” from enacting barriers to cross-border data flows to the United States, and in doing so, highlights the risk of relying on hortatory, and not legally binding, commitments. Even where it did make a binding commitment on financial data flows, Korea’s use of
regulatory rules to undermine this commitment highlights the need for future U.S. trade agreements to have clear dispute settlement procedures in place given the potential for discriminatory and arbitrary rules to undermine commitments on data flows. These cases also highlight how countries can use a broad application of national security (as with mapping data) and government procurement requirements to force companies to cut off data flows and/or setup local IT facilities. These lessons need to be applied to future trade agreements to ensure that any exceptions to rules that prohibit barriers to cross-border data flows are clear and narrowly tailored to legitimate public policy goals.

VIETNAM – RESTRICTIONS ON OVER-THE-TOP SERVICES

Vietnam’s restrictions on U.S. over-the-top (OTT) service providers violates a number of Vietnam’s WTO commitments. In January 2016, Vietnam released a draft regulation—Draft Decree Amending Decree 72—for OTT services that forces foreign firms to store data locally and for some foreign OTT service providers of chargeable services (i.e., not offered for free) to form an undefined commercial relationship with a local telecommunication company as a condition of market entry.\textsuperscript{cvii}

OTT services are those delivered via the Internet and are some of the most popular and innovative services available, especially with the spread of smart phone ownership. For messaging and communications, U.S. OTT service providers, such as WhatsApp and Messenger (both owned by Facebook), Skype (owned by Microsoft), and Google Allo, provide instant-messaging and calling services as an alternative to those provided by traditional mobile and fixed-line network operators. Globally, OTT services market is expected to grow 16.4 percent a year between 2017 and 2025, which would make the sector worth an estimated $2.5 billion by 2025. Business models such as subscription and premium, adware, and ecommerce constitute the various types of models through which the global OTT services market generate revenue. Of these the premium and subscription model segment accounted for a dominant 48 percent of the overall market in 2016.\textsuperscript{cviii}

In using the Internet, OTT service providers and their customers can bypass traditional telecommunications network service providers to compete with services (such as voice) from telecommunications companies. These technological innovations have changed consumer behavior in media and telecommunications markets, among others, allowing consumers to change how they access and consume media and communicate. This is especially the case in developing countries that have deployed mobile-phone services before (or instead of) traditional phone services, thereby leapfrogging costly fixed-line infrastructure, which has also led to a vibrant app and digital economy.

Vietnam did not carve out exceptions that could account for the measures in Decree 72 when it joined the WTO in 2007. Instead, Vietnam’s commitment for Internet Access Services only states that the “service must be offered through commercial arrangements with an entity established in Viet Nam.” The nature of Vietnam’s OTT requirement shows that these measures violate this commitment and other WTO rules by discriminating against foreign firms.
First, the targeted and discriminatory nature of the requirement is shown by the fact other OTT services face no such requirements, such as chargeable services other than voice and messaging services (e.g., on-line gaming services) and free OTT voice and messaging services.\textsuperscript{cix}

Second, differences between OTT service providers and traditional telecommunications companies show why these requirements are a disguised trade barrier. OTT service providers are not traditional network providers and therefore do not need to setup an interconnection arrangement with a telecommunications operator (e.g., agreements between different networks in different countries in order to exchange data). An interconnection requirement makes sense for traditional, circuit-switched networks and services, which require physical interconnection arrangements, negotiated under contract or set by tariff. However, the nature of OTT services is that they can be provided over the Internet completely independent of any underlying transmission provider.\textsuperscript{cxi} Given this, there is no legitimate reason for OTT firms to store data locally or to establish a commercial arrangement with local telecommunications companies.

Given this, Vietnam’s requirement for foreign OTT firms to enter into a commercial arrangement with a local telecommunications company violates GATS commitments that prohibit such arbitrary and discriminatory measures. GATS Article VI states that “all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner.” Furthermore, GATS Article XIV requires that “[s]ubject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.” Furthermore, forcing foreign OTT service providers to locate a server in Vietnam or to enter into a commercial arrangement with a local telecommunications company in order to provide their service violates Vietnam’s commitment to provide National Treatment—i.e. treating foreigners and locals equally—to foreign suppliers.

Given Vietnam’s WTO commitments, U.S. firms should be free to decide how they structure their operations and whether they store their data locally or elsewhere. There is no reasonable basis for these regulations besides discriminating against foreign firms and disadvantaging them by raising their costs (by forcing them to setup or use duplicative IT infrastructure for data storage). It is clear that Vietnam seems intent on using regulation to protect traditional telecommunications providers that are unable to (or simply do not want to) compete with innovative OTT service providers. Indicative of this approach, Vietnamese media reported that Vietnam’s prime minister ordered the Ministry of Information and Communications to restrict other OTT apps due to the impact these apps were having on traditional mobile carriers, such as Vietnam’s largest mobile network operator Viettel (which is owned by Vietnam’s Ministry of Defense). As a Zalo representative (a local OTT firm) rightly pointed out, free email services took over from postal services, but no one banned these services, yet the government seems intent on trying to do this with OTT services.\textsuperscript{cxii}
ENDNOTES


xv. Ibid.


Mark Wu, “The ‘China, Inc.’ Challenge to Global Trade Governance,” Harvard International Law Journal 57 (2016): 1001–1063, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2779781. Wu outlines how China’s “state capitalism,” or “China Inc.” as he prefers to call it, is not found anywhere else in the world and would not be easily replicated by other societies. The Chinese economy significantly differs from the economic models that influenced the Uruguay Round agreements. Wu outlines six elements that make China Inc. unique, some of which on their own resemble elements found elsewhere, but the interactions of these six elements cause the Chinese economy to be exceptional. This gives rise to an economy where the Party-state remains all powerful, but significant economic activity is driven by private enterprises. Furthermore, it is difficult to apply typical differentiating labels in China, such as market vs. non-market and private-led vs. state-led. The six elements are: the state (SASAC) as a corporate holding entity; state control of financial institutions; state control over planning and inputs (NDRC); Chinese-style corporate groups and affiliated networks; Communist Party involvement and control; and the intertwined nature of private enterprises and the party-state. Although China has become more transparent and market-oriented than it was prior to WTO accession, it has not converged along the lines of either a market economy or one of the alternative structures seen elsewhere in the world, such as a command economy, a “transition” economy from command to market-based, or the conglomerate-led structure of East Asia. Hence, the China Inc. model remains a distinct form of its own.

To the extent they could, negotiators set specific provisions in China’s WTO protocol to address them. But this raises the question as to why there are not more WTO rules dealing with issues specific to China’s economic model. The belief that China would converge along the lines of other economies, such as a market economy, have proven false. While negotiators may have disagreed as to where China’s economic model would end up, they shared a common (now mistaken) belief that China would converge toward an economic model already considered by the WTO framework. This has not happened.


xlvii. Ibid.


xlix. USTR, Report on China’s WTO Compliance, 56.

I. Ibid.


v. In 2007, the MLPS for information security was formally launched by the Ministry of Public Security (MPS), National Administration for Protection of State Secrets (NAPSS), and the Office of State Cipher Code Administration (OSCCA), led by the State Council.

vi. This MLPS classifies information networks in China according to their relative impact on national security, social order, and economic interests if the system is damaged or attacked. The classification levels range from one to five, one being the least critical and five being the most critical. A level five ranking indicates extremely significant networks, such as for military and defense. According to MLPS regulations, systems classified at level three or above must procure IT security products containing only domestic IP. “China – Information and Communications Technology Equipment and Software” (Washington, DC: International Trade Administration, May 31, 2016), https://www.export.gov/article?id=China-Information-Communication-Technology.

vii. The definition of what is involved is being considered by China’s National Information Security Standards Technical Committee (also known as Technical Committee 260) under the Cyberspace Administration of China, which is the cybersecurity standards maker, as part of its efforts to craft technical specifications for the new cybersecurity law. Eva Dou, “Microsoft, Intel, IBM Push Back on China Cybersecurity Rules,” The

The comments were made in a discussion log made public by Technical Committee 260, the national cybersecurity standards maker, as it released technical parameters of its omnibus cybersecurity law adopted on November 7. Ibid.

Panitchpakdi and Clifford, China and the WTO, 225.


Ibid.


Ibid.

Ibid.

Panitchpakdi and Clifford, China and the WTO, 225.

Froman, 2015 National Trade Estimate, 78.


xci. Ibid.

xcii. Ibid.

xciii. Ibid.


ci. Ibid.

cii. Ibid.


cviii. Ibid.


cxi. Ibid.


cxiv. USTR, The 2017 National Trade Estimate report.


cxx. Ibid.