RESPONSES TO CHAIRMAN CORNYN, SENATOR GRASSLEY, AND SENATOR YOUNG

By: Nigel Cory, Associate Director, Trade Policy, The Information Technology and Innovation Foundation

Chairman Cornyn

Question 1: Censorship as a Barrier to Trade and How to Address it in Phase 2 Negotiations between the United States and China

Question: Our nation's technology companies are increasingly being blocked from access to the Chinese market. Meanwhile, the Chinese government is subsidizing its own technology development through companies such as Huawei. Some technology companies are censored entirely out of the market. This has caused billions of dollars in damage to our economy and contributed to our nation's outsized trade deficit with China. The cost has to be much more.

- *What kind of barriers do tech companies face in entering the Chinese market and what are the short- and long-term costs?*
- *What should we be focusing on to ensure censorship is removed as a barrier to digital trade as talks on a Phase Two deal progress?*

China is the leader in digital protectionism. The impact on U.S. firms can be categorized as either direct or indirect:

- The direct blocking of market access via the Great Firewall, restrictive and discriminatory licensing arrangements, and other market access restrictions.
- The direct blocking of digital content (movies, TV shows, and video games) via opaque, restrictive, and/or discriminatory content-review processes.
- The indirect impact on how U.S. firms can operate and compete in China by forcing all Internet traffic through the Great Firewall, which degrades or cuts off data connectivity with the global Internet. For example, this hinders the cross-border sale and service of software.
- The direct impact on how U.S. firms can use corporate virtual private networks (VPN) to connect to intra-firm networks outside of China, which can undermine connectivity, be expensive, and potentially expose corporate communications to Chinese government agencies.
- At the macro level, there is the direct impact of U.S. firms being excluded from China during a formative period of rapid growth in China's digital economy. This leads to the indirect and long-term impact that Chinese firms use their protected domestic market to grow and become competitive, before taking market share from U.S. and other foreign firms in third-country markets.

The Great Firewall of China represents a rare case where U.S. digital exports face a barrier at the border. Most of the foreign online services, apps, or intermediaries that China blocks are rarely revised and lifted (as the list above shows). Firms that have their web services temporarily blocked typically find that this is simply a prelude to a total and permanent block. The impact of being blocked is cumulative in its trade impact, as for many services that are already blocked, if they add innovative new services and products, the block is automatically extended. For example, China's initial blocking of foreign search engines has expanded to encompass many email, cloud storage, and other services. This shows that even if there was a specific politically or socially offensive article to prompt a block, the extension of this block to new services makes it much more impactful from a trade and economic perspective. ITIF's Senate testimony outlines the long list of major U.S. tech firms that have been blocked by the Great Firewall over the last two decades.

The trade impact of censorship in China is much broader than website blocking via the Great Firewall of China. Behind this clear market access barrier, U.S. firms face a complicated, opaque, and changing regulatory framework tied to content moderation and information control. China's use of censorship affects both market entry and operations in China and the provision of digital services and products from overseas. Moreover, in many cases, China's approach to censorship is unwritten, with enforcement often being arbitrary and delegated to private firms. This is in large part a conscious decision to avoid disputes at the World Trade Organization, which would be much easier to put in place if the rules were on paper.

The trade related impact of censorship no doubt plays a role in China's decision to prohibit wholly or partially owned foreign firms from key digital sectors. For example, China uses licenses to strictly control which parties can offer value-added telecommunication services, such as voice-over-internet protocol (VOIP) calls, online database storing and searching, electronic data exchange, online data processing and transactions processing, domestic multiparty communication services, VPN services, and video teleconferencing and as well as limiting what parties can interconnect these services with public telecommunication networks.[1] Similarly, foreign ownership in basic telecommunication services (fixed line, mobile, and broadband) is capped at 49 percent.[2]

In terms of how China's approach to censorship and protectionism affects how U.S. firms operate (in terms of connectivity) in China, it varies along a spectrum: from a minor, periodic constraint on service access to a severely degraded connection that essentially makes it unviable from an operational or commercial perspective to a complete block. Frequent blocking and unlocking of websites (and VPNs) can make it hard for firms to have confidence they will have the communication services they need for day-to-day operations and international trade.[3] U.S. firms also report that pushing all traffic through the Great Firewall adds transmission delays that can significantly degrade the quality of the service, to the point where it's commercially or operationally unacceptable (thus cutting off market access).[4] In a similar way, China has "throttled" access to foreign websites in order to make them so slow as to be unusable. Throttling is also often a precursor to being blocked completely. For example, before Google was fully blocked in 2010, it was

throttled for a long time, which had the effect of making it appear as if Google's search engine was slow and buggy.

The economic impact of being kept out of China due to censorship and protectionism is significant. A generation of Chinese consumers have grown up without knowing that their Internet and consumer experience is completely different than what's available in most other countries. They have little or no idea about Google, Twitter, Facebook, or other U.S. firms and their products, even as Chinese government officials and party "apparatchiks" use these platforms to spread propaganda in the United States.[5]

As detailed in ITIF's written testimony, a host of U.S. industries and firms, in sectors ranging from Internet services to cloud computing, video games, and movies, have likely lost hundreds of billions of dollars in revenues due to Chinese censorship and related market restrictions.[6] Importantly, these revenues would have supported innovation and job creation in the United States, while limiting Chinese firms' ability to grow and capture global market share. While it is not possible to calculate an exact figure, ITIF conservatively estimates (based on market-share comparisons) that Google, which withdrew from the Chinese market in 2010, subsequently lost $32.5 billion in search revenue from 2013 to 2019, while Amazon and Microsoft's cloud services (IaaS, which is restricted in China) lost a combined $1.6 billion over the two-year period from 2017 to 2018. As the China market continues to rapidly grow, these losses will also grow significantly. Beyond this more-immediate impact, the longer-term, indirect impact is that is has provided Chinese competitors with a protected market from which to launch competitive challenges in other regions, such as South America, the rest of Asia, and Africa. This cost will only grow as the global digital economy grows.

The United States needs to prioritize and seek as part of bilateral negotiations with China: clear, meaningful, and enforceable commitments on market access for a range of Internet services; fair, transparent, and predictable digital content review processes for movies, TV shows, and video games; and rules to protect the free flow of data and digital goods. The United States has the model trade law provisions to use for these issues (such as its other modern trade agreements, including the U.S.-Mexico-Canada (USMCA) free trade agreement). The main thing is that the United States needs to prioritize these tech and digital issues as they are of far greater size and significance (in terms of economic productivity, innovation, and competitiveness) as compared to agricultural and commodity exports.

The United States also needs to develop new trade rules to ensure China does not seek to apply its censorship laws and regulations extra-territorially. It's one thing for U.S. firms to abide by local laws and regulations around censorship and content moderation in China, but it's completely different—and unacceptable—for them to change their operations or content outside of China. Alongside this, the United States should explore new domestic transparency and policy tools to identify, track, and respond to cases where China seeks to enforce its censorship on U.S. firms outside of China (detailed below in response to Senator Grassley's question).

Question 2: The Future of the Global Internet and China and Other's Efforts to Export their Own Restrictive Models of Digital Governance

Question: The ongoing pandemic has accelerated the vulnerability of America's ability to produce its own critical equipment and supplies. One area of special focus is the semiconductor space. It underpins everything in the digital trade space—from 5G to the equipment we use to work from home. I recently introduced the CHIPS for America Act that incentivizes the production of semiconductors back home. This will not only help us be prepared for the future but allow the U.S. to remain the global defender of free speech online.

- *Can you talk about the global internet landscape today and where you see it going in the future?*
- *Specifically, I am concerned about China's export of its authoritarian model of a closed off internet to the world. What are China and other countries doing to support authoritarian regimes via digital trade and infrastructure?*

There are three major models for digital governance in the world today. Along a sliding scale of restrictiveness (from low to high), there's the United States' and the Asia-Pacific Economic Cooperation's Cross-Border Privacy Rules (CBPR) risk-based approach to data regulations; the European Union's (EU's) onerous and restrictive precautionary principle-based General Data Protection Regulation (GDPR) and emerging restrictions around artificial intelligence; and finally, China's sovereignty-based model of digital control and protectionism.[7]

China provides a masterclass in how to enact behind-the-border barriers to digital trade in order to give local firms and products an unfair advantage, especially as it relates to digital products, cross-border data flows, and the intellectual property (IP) closely associated with digital trade (such as protections for source code and algorithms).[8] In contrast to the United States and many others, China treats local data storage as the norm and data flows as the exception, asserting that data privacy and cybersecurity are associated with location and control.[9] Data localization is a central theme of China's data governance framework. For example, China's cybersecurity law requires personal data and "important data"—a vague term encompassing data related to China's national security, economy, and other public interests—held by key information communications and technology (ICT) operators to be stored within China. This is in addition to existing data localization measures for health, mapping, and financial data and other data-restrictive policies.[10] Against this backdrop, China has made few substantive commitments on digital governance in its trade agreements, especially on data flows. Nor has it signed on to other international data transfer mechanisms, such as the CBPR.[11]

In separating itself from the global Internet over the last two decades, China is a major contributor to the fragmentation of the global Internet, but its impact is much broader as it provides a poor model of governance—in terms of technology and policies—for other countries to emulate. China's success in exporting its model of digital control is most evident in similarly authoritarian countries, such as Iran, Russia, Venezuela Vietnam, and elsewhere.

These countries' eager embrace of China's model is sad evidence that the global Internet is increasingly fragmented as countries—across every stage of development—have erected barriers to a seamless global digital economy. This includes enacting data-residency requirements that confine data within a country's borders, a concept known as "data localization."[12] It also includes requiring only local firms to manage certain types of data and using arbitrary app or content review processes to ban foreign providers and content.

China's overall approach of restricting and controlling the Internet has also no doubt provided some sort of permissions structure that countries use when enacting broad and arbitrary restrictions on their countries' use and connection to the global Internet. For example, in 2018 alone, at least 25 nations throttled down users' bandwidth, shut off their mobile or broadband Internet services altogether, or blocked access to mainstream Internet sites or applications.[13]

Many countries like China's model of digital protectionism as they like how it has kept out leading U.S. tech companies and led to the emergence of local tech firms, like Alibaba and Baidu. This makes it easy for China to export its restrictive model and the key technologies that facilitate it. However, enacting China's full range of restrictions is beyond the capacity of most nations, so many developing countries (but also parts of the EU) pick and choose parts of China's model when it suits them to either allow control over digital content or tilt the local market in favor of domestic firms. This is especially the case in India, but Brazil, Indonesia, Nigeria, Vietnam, Russia, and others have also sought at times to emulate parts of China's approach.

However, it's important to note that China is not the only model that contributes to the fragmentation of the global Internet. The EU's GDPR is problematic because it pushes for harmonization and tries to make foreign countries responsible for enforcing European data privacy standards instead of using domestic regulations to hold companies responsible for breaches of European data privacy laws. The GDPR imposes a general prohibition on transfers of EU personal data to all but a small group of foreign countries it has determined (as part of an opaque and ad hoc process) provide an "adequate" level of protection equal to data protection at home. A critical flaw in the European Union's approach is the mistaken logic that this country-by-country assessment approach is effective in promoting better data privacy and protection by companies that manage personal data.[14]

Furthermore, the EU's top-down approach is ultimately untenable, as differences in social, cultural, and political values, norms, and institutions are behind countries not regulating privacy the same way. For example, given the country's approach to data protection and privacy, it is inconceivable China would ever be deemed "adequate" from a European perspective. Yet, the fact that Europe has not applied to China the same standards it applies to the United States with regard to EU personal data highlights the arbitrary nature of its approach.[15]

Ultimately, success will depend on whether the United States and likeminded digital trade allies can work with, and convince, the many undecided countries in the middle—those that have not yet chosen which

model they want to follow—that theirs is the best approach from both an economic and regulatory perspective. The United States and its likeminded trading partners—Australia, Canada, Chile, Japan, Mexico, New Zealand, Singapore, the United Kingdom, and others—which want global norms around new technology to reflect their values and trading practices, need to proactively engage with each other and the many undecided countries regarding their preferred model. New digital trade rules are definitely needed to prohibit and roll back the growing range of barriers to digital trade, but these are insufficient on their own to create frameworks that allow firms to engage in seamless digital trade and data-driven innovation across borders.[16] The United States also needs to use its trade agreements and economic statecraft (resources and programs managed by the U.S. Agency for International Development (USAID), the State Department, the Department of Commerce, and others) to help build new norms and rules around data and digital trade.

The United States also needs to do a better job of articulating and advocating for its preferred model of risk-based, permission-less innovation. The U.S. model should be based on the fact that modern technology, especially the Internet and cloud data storage and processing, means that each country's domestic regulatory regime for data (such as for privacy) needs to be globally interoperable given that each country faces the same challenge in applying its laws to firms that may transfer data between jurisdictions.[17] An interoperable system would focus on "global protections through local accountability." The principle idea is that a country can enforce its rules on any foreign or domestic organization with legal nexus. Moreover, a country can enforce its rules on these organizations based on how they handle the data they collect, even if that data handling occurs abroad or with a third party. This accountability-based approach is shared by most nations, after all, including for data privacy, including the United States. For example, foreign companies operating in the United States must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data—even if they move data outside the United States. And, if a foreign company's affiliates overseas violate HIPAA, then U.S. regulators can bring legal action against the foreign company's operations in the United States.

The United States has already embedded the rules that support this model in its trade agreements, such as the USMCA and the United States-Japan digital trade agreement. But the country needs to be far more proactive in advocating for its preferred model.

One idea to do this would be to negotiate an ambitious digital trade agreement with its "Five Eyes" partners (Australia, Canada, New Zealand, and the United Kingdom). Just as the United States works with them on intelligence sharing and to standardize operating practices and technical specifications for defense equipment and operations, it should seek to build out a trade and innovation framework, doing the same for digital trade. It should seek to do likewise with other similarly ambitious partners such as Chile, Japan, and Singapore. An easy way for the United States to engage with a broader range of ambitious countries would be to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).

China's Efforts to Export its Restrictive Approach to Standards

China's model is not just censorship and restrictions on data. China is increasingly trying to export its own restrictive standards as part of an effort to unfairly influence international standards-setting organizations, potentially giving its firms an advantage in gaining global market share and influence in new and emerging technologies. This involves international technical standards for AI, robotics, self-driving vehicles, the Internet of Things, and other new technologies. Standards are one part of Chinese President Xi Jinping's plans for China to become a "cyber superpower."[18]

Standards are an important (but often overlooked) component of global trade, as they foster economies of scale by making it relatively easy for firms to produce a good or service to a mutually accepted standard across markets. China pursues indigenous (i.e., China-specific) technology standards (both at home and internationally) because it believes it will advantage China's domestic producers while blocking foreign competitors and reducing the royalties Chinese firms pay for foreign technologies.[19]

At home, China provides a clear example of how country-specific standards can be used to act as a barrier to trade for high-tech goods and services.[20] As ITIF's report "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" argues, China has made the development of indigenous technology standards, particularly for ICT products, a core component of its industrial development strategy.[21] Most recently, in 2018, China introduced a new standardization law that will likely favor local firms and their goods and services, as it references "indigenous innovation" while failing to reference either its WTO commitments (thereby raising questions about WTO compliance) or its acceptance of existing international standards (approved by the various standards-development organizations (SDOs)).[22] Indicative of China's approach, a report by the German think tank, the Mercator Institute for China Studies (MERICS), shows that Chinese standards for basic smart manufacturing correlate with about 70 percent of relevant international standards—which falls to around 53 percent for key smart manufacturing technology standards, and to 0 percent for standards relating to cloud computing, industrial software, and big data.[23]

The United States needs to pay greater attention to China's efforts to export its restrictive domestic standards as part of efforts to influence SDOs. Thus far, China's approach to international standards—focusing on a large number of submissions, often of relatively poor quality—has not been overly successful, indicating SDOs are largely working as intended. However, as the MERICs report explained, "The ongoing reform of [China's] standardization system and the revision of the standardization law point to a liberalization and internationalization."[24] This transition, from inward-looking protectionism to outward-facing ambition, represents both an opportunity and a threat. There is an opportunity to better integrate the Chinese market with the rest of the world through unified, globally standardized technologies and equipment. However, there is also evidence China has and will attempt to unfairly influence international standards-setting bodies to ensure Chinese technology is at the heart of (i.e., considered essential to) the international standard.

For example, the United States needs to monitor where China's government and its firms use their own restrictive domestic standards as the basis for efforts to influence standards in third countries via government-to-government engagement, foreign investment projects, and commercial contracts (such as those associated with its "Belt and Road Initiative" (BRI)). One of the three main motivations of the "Digital Silk Road" (the digital component of BRI) is to leverage the strength of China's ICT sector to spread its domestic standards.[25]

The United States also needs to be vigilant for where China tries to unfairly coerce its own and foreign firms (such as those relying on financing from China for projects) in supporting votes on standards that favor its local companies and their standards, rather than supporting the best technological solution, such as for 5G technology standards. In particular, the United States should remain wary of attempts by the Chinese government to direct Chinese firms to support a particular proposal for key technologies. The Chinese state media report "Lenovo 5G Incident Shows Need for Chinese Companies to Cease Mindless Competition" is indicative of this scenario, wherein Lenovo was forced to make a public apology after supporting U.S. firm Qualcomm's proposal, rather than Huawei's, for a key coding method for 5G data transmissions.[26]

China is also seeking to export its model through state-supported or private-sector-led foreign investment projects. China could potentially use commercial contracts and operations as part of a "bottom-up" strategy to build acceptance and use of restrictive Chinese standards for new and emerging technologies in markets around the world. China's government and firms follow provisions that stipulate projects must use Chinese standards and equipment, thereby "socializing" them in foreign markets and standards agencies. China has used this approach most extensively for projects involving heavy industry (e.g., oil, gas, and infrastructure), but is expected to take a similar approach with ICT-related projects. China complements this with top-down efforts by the government as part of engagements with specific countries and regions on digital-economy issues. For example, in 2017, standards were part of China's Digital Economy International Cooperation Initiative, which it launched as part of its BRI engagement with Egypt, Laos, Saudi Arabia, Serbia, Thailand, Turkey, and the United Arab Emirates.[27] In other words, Lenovo decided it was in its interest to support the Qualcomm standard, but the Chinese government overruled it.

Semiconductors: Supporting the Technology at the Heart of the Global Digital Economy

The United States needs to do much more to develop and advocate for its preferred model in terms of building an open, rules-based, and innovative digital economy. But it's much more than digital trade and data governance. Ensuring continued American leadership in the world's most important industry—semiconductors—is a critical component.[28] Put simply, a country's leadership in the global digital economy starts with its leadership in semiconductors. American leadership in semiconductors is not pre-ordained, and others crave it—especially China, whose $150 billion National Integrated Circuit strategy seeks to dispossess the United States of its world-leading position, while ideally eliminating all imports of U.S. semiconductors by 2035.[29]

The Creating Helpful Incentives to Produce Semiconductors ("CHIPS") for America Act introduced by Sens. John Cornyn (R-TX) and Mark Warner (D-VA) and the American Foundries Act of 2020 introduced by Sens. Tom Cotton (R-AR) and Chuck Schumer (D-NY) go a long way toward ensuring this. Between them, the proposed legislation would expand federal investment in semiconductor research and technology development, introduce incentives to locate semiconductor manufacturing facilities in the United States, and provide expanded tax credits for investment in the sector. ITIF strongly supports the legislation, which has since been merged as part of the National Defense Authorization Act (NDAA) process, and encourages Congress to fully appropriate funding in the legislation to the maximum extent envisioned. As important as any of this, the CHIPS Act also represents Congressional and bipartisan recognition that the United States is engaged in a fierce contest for leadership in technologies of the future—from biotech and clean energy, to 5G, AI, quantum, and semiconductors—and that effective government policy—innovation policy, not industrial policy—can empower and enable America's private sector to continue to lead in this critical industry.

Some of the important proposals of the CHIPS Act include its commitment to a total of $12 billion for semiconductor research, including $3 billion for a new National Semiconductor Technology Center to research and prototype advanced semiconductors, and its proposal to create a new Manufacturing USA Institute for Semiconductor Manufacturing. It will encourage both U.S. and foreign semiconductor manufacturers to locate new fabs here, with a $10 billion federal matching grant for state/local incentives to attract manufacturers. This will help level the playing field with other nations' incentives, and—unlike China's practices—would be entirely WTO-consistent.

While national, including U.S., policies to spur semiconductor R&D and production are important, it's also important to recognize that self-sufficiency cannot and should not be the goal. The increasing expense, complexity, and scale required to innovate and manufacture semiconductors means that no single nation can afford to go it alone. ITIF's recent report "An Allied Approach to Semiconductor Leadership," outlines why the United States needs to work with a like-minded set of nations committed to open trade and fair economic competition to collaborate in ways that collectively empower the competitiveness of their semiconductor industries.[30]

Senator Grassley

Question 1: How Should U.S. Firm Minimize the Risk of Censorship in China

Critics charge that U.S. businesses should simply not do business in China because of Chinese government censorship. The problem I have with that is that it doesn't change the fact that the Chinese government is still going to impose censorship on its people regardless of whether we do business there or not. If we're not there, the Chinese people would simply have to resort to buying goods and services from Chinese firms that are likely more inclined to accept censorship. I'm interested in figuring out how to protect American businesses.

- *What steps should American companies take when entering the Chinese market to minimize the risk that they'll fall prey to Chinese government censorship practices?*

Overview

The United States and its firms should do four key things to minimize the impact of censorship in China:

- Ensure U.S. firms take reasonable steps to separate operations in China from others around the world;
- The U.S. government—not U.S. firms—should lead the effort to advocate for free speech and democracy in China;
- The U.S. should develop tools to identify and counteract any "spillover" whereby Chinese censorships impacts U.S. firms, goods, and services in the United States (as well as extra-territorial access to data); and
- The United States should work with likeminded, value-sharing partners to develop new trade and economic arrangements as part of broader efforts to develop a better, alternative model for digital governance.

Ensure U.S. Firms Enact Administrative and Technical Firewalls Between China and Non-China Operations

If WTO rules and global norms around international trade and commerce fully applied in China, U.S. and other foreign firms would be able to operate in China and other markets in a fairly seamless manner. Sadly, the last two decades show that China simply decides to ignore or breach the many rules that otherwise create a clear and fair framework for international trade and investment. It means that U.S. and other foreign firms have to enact clear administrative and technical firewalls between China and non-China operations in order to minimize the growing risks that they'll be accused of breaking local laws. The degree and type of segregation obviously depends on the nature of local laws, which, in the case of Internet-related firms in China, is becoming major risk for many firms.

The U.S. government should expect, and respect, when U.S. firms do this to abide by legitimate local laws, such as data privacy and censorship (even if the U.S. government dislikes the laws themselves). Firms do this as it shows that they're committed to following the laws of the country in which they operate, while minimizing potential risks in other countries, including back in the United States. Advocating for U.S. firms to ignore local laws in China is to essentially support anarchy. U.S. policymakers expect Chinese firms to do the same in the United States. Until the United States can negotiate new and improved commitments for its firms in China, U.S. policymaker should not be surprised when U.S. firms segregate their operations to help, in part, ensure that Chinese censorship is contained to China. However, this expectation obviously should not extend to U.S. firms abiding by activities that breach U.S. and international laws around egregious human rights issues, such as playing a role in, or benefiting from, the mass detention camps China operates for ethnic minorities in Xinjiang.[31]

Take Apple, Airbnb, and Zoom as examples. Apple has major operations in China. In the 2019 financial year, Apple made $44 billion of revenues in Greater China, mostly from selling iPhones.[32] However, to do so it had to agree to host Chinese user data rules in the country and to remove offensive apps (as requested by government authorities), such as news and VPN apps, from its Chinese app store. Apple removed 805 apps in China from 2018 to 2019.[33]

Airbnb setup local operations to both abide by local laws and to ensure its services were tailored to the market. In 2016, Airbnb setup a new business entity to manage operations in China. It has moved to store its data in China and has cancelled bookings during politically sensitive events (such as China's National People's Congress).[34] In March 2018, Airbnb stated that it will send customer details to Chinese government authorities to abide by local regulations that require foreigners to register their accommodations with police (hotels have done this for a long time).[35] Listings and non-China operations are not affected by these requirements. In November 2019, Airbnb's China president Tao Peng highlighted that localizing its platform is the key to the company's success in China.

Zoom provides a case study in why (and how) U.S. firms need to separate and contain their operations in China from the rest of the world. It (rightly) faced considerable criticism in how it was dealing with Chinese users and user data. In April 2020, Zoom encountered significant public scrutiny when the University of Toronto's Citizen Lab released a report that showed that Zoom meeting encryption keys were sent via China-based servers and that it used non-industry standard cryptographic techniques that may mean calls could be intercepted (which raised concerns about China's laws concerning encryption key disclosure).[36] Zoom responded, removing these servers from the list of backup servers for users outside of China. It also enacted new safeguards and internal controls to prevent unauthorized access to data, including by staff, regardless of where data gets routed. Most recently, it updated its encryption protocols and said that it will introduce end-to-end encryption for all calls (for both free and paid services, but it will be an optional feature as it limits some meeting functionality).[37]

Zoom encountered another major issue when it briefly blocked, and then restored, the accounts of Chinese human rights activists (including Zhou Fengsuo) who wanted to use the platform to organize a public commemoration of the 1989 Tiananmen Square crackdown.[38] Mr. Fengsuo is an American who lives in the United States. China asked Zoom to terminate four meetings scheduled to be hosted on Zoom and three accounts (one in Hong Kong and two in the United States) hosting the calls. Zoom cancelled the three meetings that involved participants from mainland China.[39] Zoom rightly committed to "not allow requests from the Chinese government to impact anyone outside of mainland China."[40] It has developed technology to remove or block participants based on their country, which will allow the firm to take a much more granular action in response to requests from local authorities when they determine that certain activity on the platform is illegal in that country.

Develop Mechanisms to Identify, and Respond to, Cases of Extra-Territorial Censorship (and Access to Data) by China

The U.S. government should focus on ensuring that U.S. firms only apply local laws—like those for censorship and government requests for data—in local jurisdictions and come up with tools to counteract it if it spills over into the United States. Recent cases with the NBA being penalized in China for remarks from one coach in the United States is not only evidence of China's sensitive and punitive nature, but also its extra-territorial application of censorship in selectively targeting people and firms for what they say and do in the United States. This is unacceptable. However, there are few mechanisms and details about the true extent of the issue and few tools for the United States to use in response. As a first step, the U.S. Congress should discuss the issue of extra-territoriality in today's global digital economy and enact transparency arrangements to better understand the extent of the key issues (censorship and access to data).

The new national security law in Hong Kong is the latest and clearest example of the challenge that U.S. policymakers need to respond to, as it targets content removal and access to data on a potentially global basis.[41] While observers don't yet know how China will use the new law (Macau has had a similar law in place for 11 years and there have been no enforcement cases), there's the potential for it to be used on a global basis as it applies to offences committed outside Hong Kong and it allows authorities to ask the publisher, platform, host, or network service provider to remove or restrict access to "illegal content" or produce information about a user.[42] Furthermore, investigations into national security crimes can be deemed a state secret, any trials may be heard in closed court, and tech companies may be forbidden from disclosing what the police ask them for.

Hong Kong is important to U.S. tech companies, in part, as it's often their base for marketing their global advertising services to customers in mainland China. In 2019, Hong Kong's government made just over 5,500 requests for user data and just over 4,400 requests for removal of content.[43] Microsoft, Facebook, Telegram, Twitter, LinkedIn, and Zoom have suspended processing of requests for data from Hong Kong government authorities. While admirable, this does not absolve them of complying with the law.[44] The Hong Kong and Chinese government would surely retaliate against these firms if they did this.

The potential extraterritorial application of domestic law for Internet-related issues is not unique to China. Privacy regulators in Europe have tried to dictate what information U.S. firms make available to people in Europe, but also to the rest of the world, through their "right to be forgotten" requirement that gives European Union citizens the power to demand that data and information about them be deleted. Germany requires social networks to remove Nazi symbols. In 2017, the Supreme Court of Canada upheld orders for Google to "de-index" a website, and asserted the jurisdiction of Canada's courts over Internet intermediaries in other countries.

The United States needs to identify and respond to cases where China (and other governments) try to enforce censorship (as well as access to data) overseas. Some of these cases (like the NBA case) are easy to identify, but

there may well be others. There is a lack of transparency about the extra-territorial application of Chinese censorship and requests for data. Some recent draft legislation in the U.S. Congress provides some ideas for analysis and potential action.

For example, it's misguided to force firms to publicly disclose where their data is stored, such as in China, (as Congressman Jeff Duncan's (R-SC) TELL Act does) as labeling and treating all firms from China as guilty does not address the underlying question about countries respecting each other's sovereignty.[45] It's one thing for these firms to be held accountable for any breach of U.S. laws in the United States, but it's another to assume (without evidence) that Chinese firms (and U.S. firms with operations in China) are automatically breaching U.S. law. Using such a broad brush could also easily be re-used by China or other nations to discriminate against U.S. firms given the Snowden revelations. The same applies to Congressman Adam Kinzinger's (R-IL) Internet Application Integrity and Disclosure Act's requirement for websites or apps owned by the Chinese Communist Party or any Chinese firm to be made clear.[46]

There is a potential policy path ahead. Senator Cory Gardner (R-CO) and Senator Jeff Merkley's (D-OR) bill (S.2743) establishes the China Censorship Monitor and Action Group (an interagency taskforce) to develop and maintain a public database describing all punitive actions taken by the People's Republic of China toward U.S. companies that involve economic or diplomatic retaliation for the exercise of free speech by those companies.[47] It would meet and report to Congress periodically, including an annual report.

There are some ways this bill could be improved:

- Focus on the extra-territorial enforcement of censorship and requests for data: It should not seek to punish U.S. firms for having to abide by censorship laws in China.
- Bring transparency to the vagueness of China's laws: At the heart of the issue is the lack of transparency about how China applies its laws extraterritoriality in both seeking to remove content and access data stored in another jurisdiction. The transparency mechanism is a good idea, but it should include coverage of both issues.
- Broad open source research, (voluntary) firm engagement, and cross-checking of details: U.S. agencies should use both public and confidential sources to gather information about relevant cases. However, reporting by firms should be voluntary and confidential (in order to protect U.S. firms from retaliation in China). Any cases should be verified to avoid companies submitting anecdotal stories about other firms (like their competitors) that may not be correct and otherwise smear their reputation. Sensitive reporting could be covered in unidentified general, aggregated analysis.
- Cover cases involving U.S. trading partners: Any U.S. reporting mechanism should use publicly available information to detail cases of extra-territoriality involving firms in U.S. trading partners.

Do More With Value-Sharing, Digital Free Trade Partners: "DATO" and "Five Eyes" Trade Negotiations

China's approach to human rights is abhorrent. Its use of digital protectionism runs counter to U.S. interests and values. The U.S. government should directly make the case to the Chinese Communist Party that it improve its approach to both issues and to also highlight them in international forums as part of broader efforts to build international pressure on China to change its policies. However, the United States needs to be putting similar energy and attention into developing an alternative model of trade that better reflects its values.

On April 4, 1949, compelled by the threat of Soviet military aggression, the United States and 11 other nations formed the North Atlantic Treaty Organization (NATO), a security pact holding that an attack against any of the signatories would be considered an attack against them all. Today, Chinese economic aggression requires that the United States and its allies form a NATO for trade.[48] In many ways, this would be an extension of the "Five Eyes"-based model detailed above, given that Australia, Canada, New Zealand, and the United Kingdom also share similar political, economic, and social values. However, it could obviously be expanded beyond this to the many other trading partners that are also finding themselves in China's cross-hairs for economic retaliation due to cases whereby China thinks its been "unfairly" singled out over action they've taken against China.

The campaigns of intimidation usually begin with claims of victimhood and accusations that any criticism smacks of racism or of efforts to deflect attention away from the critics' domestic failures. But if that fails to produce the desired obsequious result, China quickly moves to direct economic threats. Australian Prime Minister Scott Morrison found this out when he did nothing more than call for a formal inquiry into China's actions at the outset of the pandemic. In response, Beijing threatened a boycott of Australian universities and tourist operators as well as trade sanctions against Australian beef and wine.[49] Likewise, when Sweden supported human rights victims in China, Beijing's ambassador responded, "For our enemies, we have shotguns." The ambassador threatened that China would restrict Swedish exports. When Germany considered banning procurement of 5G gear from the Chinese telecom giant Huawei due to security concerns, China's ambassador in Berlin abandoned any pretext of global trade rules, asking: "Could German cars be deemed unsafe by Chinese authorities?"[50]

Such an organization would be broader than just new digital trade rules. It could become a new approach under which democratic, rule-of-law-nations agree to come to each other's economic aid against an outside adversary. This new organization—call it the Democratically Allied Trade Organization (DATO)—should be governed by a council of participating countries, and if any member is threatened or attacked unjustly with trade measures that inflict economic harm, DATO would quickly convene and consider whether to take joint action to defend the member nation. Success would depend upon DATO members not engaging in economic aggression against each other, as the Trump administration regrettably did in 2018 when it imposed tariffs on Canadian and European steel products.

DATO nations should cooperate to deter individual episodes of Chinese economic aggression against individual members and to provide a mutual defense umbrella against broad Chinese policies that harm all nations—particularly mercantilist policies such as the "Made in China 2025" initiative, which is crafted with a goal of achieving global dominance in strategically important technologies. Given the United States' still-indispensable role in defending freedom globally, only it can lead in establishing a DATO. The next administration, whether it be Republican or Democratic, should embrace the idea. Any democratic government, including Taiwan, should be welcome to join, but all must be prepared to take the steps necessary to enact a DATO decision, or lose the right to membership.

SENATOR YOUNG

Question 1: Censorship, the Great Firewall, and the Impact on U.S. Competitiveness and the U.S. Digital Economy

Question: As noted in your testimony, China has currently blocked over 10,000 websites and has shut down another 3,000 websites in 2018. I see a troubling nexus between a booming tech sector and an inability – or severely restricted ability – to access the Chinese market. In my home state of Indiana, we have seen multiple tech companies choose us to open business, which creates jobs and opportunity for families in need. These exciting trends have also led to career pathways and better business collaboration and partnership that is truly engrained in our communities. Because of brazen censorship in China, much uncertainty faces the tech sector when trying to predict access to international markets. This has an impact on entrepreneurship and job creation.

- *What do barriers like the "Great Firewall" mean for the future of the digital economy? More specifically, how could these barriers impact job creation?*
- *How can market access for the digital economy improve America's global competitiveness? If we continue to see Chinese actions that escalate and uphold censorship practices, how can Congress and the Administration work with American firms to ensure we retain a competitive advantage?*

As per the response to question 2 from Senator Cornyn (above), China represents one of the biggest threats—both in terms of its digital protectionism, but also its broad use of censorship and surveillance—to the U.S. goal for an open, rules-based, and innovative global digital economy. Its approach at home is obviously problematic for U.S. firms (and runs counter to U.S. values), but the broader risk is that it represents a model that other countries want to emulate. As countries grapple with the challenge of adapting local laws and regulations to the Internet and other new digital technologies to address (in many cases, legitimate) concerns over data privacy, security, and other issues, they're looking for models to follow.

Policymakers in some countries are simply misguided in inadvertently considering or enacting restrictive policies like data localization. This is understandable to an extent, given there is no one way to address many of these issues, and these issues can be complicated. However, policymakers in many countries are using

debates around legitimate policy objectives (like privacy and cybersecurity) as cover to pursue other China-like political or economic objectives, such as digital protectionism and censorship.

The challenge for the United States and other value-sharing, free trade-supporting partners is to both demonstrate the best approach at home and to work together in advocating in third-party countries how they should follow their policy model—and not China's. This is a complicated and challenging task given the constantly changing nature of technology and given that it involves a broad range of government agencies, but it'll be essential if the United States wants to build a global digital economy around its human rights and trade values.

Ultimately, if the United States does not lead the charge in advocating and helping other countries adopt its preferred policy model, it'll undermine the major role that global markets play in supporting job creation in firms across the country, as data and digital technologies become central to their ability to compete and innovate. As ITIF's report "Cross-Border Data Flows Enable Growth in All Industries" highlights, the global Internet matters greatly to agriculture, manufacturing, retail, services, and every other sector of the economy.[51] If these companies' ability to enter and operate across markets becomes restricted, it would restrict their ability to support well-paying jobs back in the United States.

Indeed, the economic evidence shows the importance of foreign operations and sales to the U.S. economy. Dartmouth University Professor Matt Slaughter has found that "investment at U.S. parents and foreign affiliates also tend to complement each other." He cites research that finds that "a 10 percent increase in foreign-affiliate employee compensation causes an average response of a 3.7 percent increase in that affiliate's U.S. parent employee compensation. Growth in affiliates tends to bring growth in parents as well."[52] In other words, preventing American companies in China from using Chinese apps or Internet platforms to gain access to Chinese customers will directly hurt U.S. workers back home.

The Global Digital Economy and American Competitiveness

Question: *How can market access for the digital economy improve America's global competitiveness? If we continue to see Chinese actions that escalate and uphold censorship practices, how can Congress and the Administration work with American firms to ensure we retain a competitive advantage?*

The openness of the global Internet has been instrumental in helping U.S. firms become leaders in the global digital economy. Open market access provides critical economies of scale for U.S. firms to use the Internet to access more customers via a relatively small investment footprint (e.g., a single global ICT system), thus earning them revenues they can use to support U.S. jobs, R&D, and other investments.

In no small part due to China, the nearly default openness of the Internet has been shrinking bit-by-bit over the last twenty years as countries realize that the digital economy is central to the battle for technological and economic competitiveness and that they can use non-tariff barriers to favor local firms and products over foreign ones. The EU and countries like China realize that current trade rules at the WTO are non-existent,

woefully out-of-date, and/or not enforced as it relates to the digital economy, so they can get away with enacting barriers at home, while still allowing their local firms to take advantage of countries that remain committed to the rules-based global trading system.

U.S. firms have long championed new digital trade rules to provide protected, enforceable market access. The United States has enacted, and continues to pursue, digital trade rules in new bilateral trade negotiations and as part of e-commerce negotiations at the WTO. But it's incumbent upon firms and the U.S. Congress and government to continuously revise and update digital trade objectives given the changing nature of technology and the barriers trade partners are enacting. For example, U.S. digital trade strategy is currently based on USMCA, but this is based in large part on the discussions that immediately followed the Trade Promotion Authority as provided by the Bipartisan Congressional Trade Priorities and Accountability Act of 2015. USTR and the U.S. International Trade Commission hold investigations and hearings into specific issues and negotiations, but this would benefit from broader, higher level direction and discussion. The U.S. Congress needs to continuously push for new hearings about the latest state of digital trade and new ideas for U.S. trade and economic policy.

For example, Congress could go further by holding hearings about what the United States should be doing (in terms of a holistic strategy) to support its overall model of digital trade and development. As China and the EU's own models have evolved, so too has the need for the United States to develop a more-comprehensive response to better push back on those parts that don't align with U.S. values and interests (whether this is censorship, data-driven innovation, and digital free trade).

However, a more comprehensive U.S. strategy for an open, rules-based, and innovative global digital economy won't mean as much without a supportive domestic innovation agenda, including in advanced-industry production. For many decades after WWII, the United States could afford its ad hoc innovation strategy which mostly worked by throwing massive amounts of money at defense and space spending (in the early 1960s, the U.S. federal government invested more in R&D than all other nations', public and business funding, combined). But after three decades of declining government support for R&D as a share of GDP, the U.S. strategy of winning innovation through overwhelming "force" can no longer work.

The United States needs to be strategic. Thankfully there is a growing consensus from both Democrats and Republicans that the federal government needs to play a stronger role in that process. First, as ITIF has long argued, the United States needs to recognize the nature of the challenge and the need for a detailed response. One place to start would be to pass the Senate Global Economic Security Strategy Act of 2019, introduced by Senators Young (R-IN), Merkley (D-OR), Rubio (R-Fl), and Coons (D-DE).[53] Further, ITIF's report "The Case for a National Industrial Strategy to Counter China's Technological Rise" provides the "why, what, and how" of a national industrial strategy—explaining why advanced industrial competitiveness is important, particularly vis-à-vis China; what is the nature of the U.S. advanced industry competitiveness challenge and why markets acting alone are not enough to address the challenge; what a strategy should look like, both

institutionally and substantively, and how policymakers should approach developing one; and finally, why common objections to such a strategy are misguided.[54]

America needs a national strategy that fortifies traded-sector technology industries that are "too critical to fail," such as advanced machinery, aerospace, biopharma, electrical equipment, semiconductors and computing, software, transportation, and more.[55] To develop and implement a national industrial strategy, the federal government will need to significantly strengthen its institutional capabilities to conduct thorough sectoral analysis. This is because when it comes to industrial strategy, America's institutional structures are holdovers from the Cold War era while our thinking remains stuck in the 1990s' free-market, globalist-based Washington Consensus. Congress should also act in four key areas: support for R&D targeted to key technologies, tax incentives for key building blocks of advanced production, financing for domestic production scaleup, and adding a competitiveness screen for regulation. Congress should task the administration with creating a national advanced industry strategy, as Sens. Chris Coons (D-DE), Jeff Merkley (D-OR), Marco Rubio (R-FL), and Todd Young (R-IN) have proposed.

Question 2: China's Social Credit System

Question: In examining Chinese strategies to insert censorship, the use of the social credit system should not be overlooked. China has developed a systemized process for determining how much or how little a business adheres to government-sanctioned ideals and principles. The social credit system then rewards or punishes a business by increasing or restricting market access. This seems obvious that the Chinese government is simply picking winners and losers, which is not what we, as Americans, believe to be the role of the federal government. Adhering to the Chinese government's rules has its benefits – ability to conduct business and secure market access. But, companies who secure market access are not guaranteed it, and can lose it at any time as we have seen in numerous circumstances.

- *In your opinion, how should American businesses consider the implications of participating in the social credit system when trying to secure access to the Chinese market? Does the social credit system provide meaningful stability or certainty to businesses that are simply trying to expand on a global playing field?*
- *How should American companies be more vigilant in evaluating the risks associated with entering the Chinese market and participating in this government-sponsored ranking system?*

ITIF has not commented on the impact of China's social credit system.

Question 3: How the United States Should Work with Partners to Confront the Threat of Chinese Censorship

Question: Adverse action taken against American enterprise can impact our relationship with other countries as well. In fact, China has imposed the same censorship retaliation on other countries for adhering to our rules or aligning with free speech and free market principles. Chinese influence also transcends into other

international markets; other nations have taken proactive action by using censorship as a regulation tool for e-commerce and digital markets.

- *How can the United States proactively work with other international partners on e-commerce regulation, particularly by not using censorship as a default strategy to protect domestic enterprises?*
- *How should Congress think about the broader effects of Chinese censorship on the U.S. relationships with other international countries when designing trade policy?*

As per the answers to question 2 from Senator Cornyn and the question from Senator Grassley, the United States will need to develop new censorship-related trade rules to ask for in its negotiations for a Phase Two deal with China, to embed these in its other trade agreements (thus building defenses against the spread of China's use of censorship for protectionism), and to advocate for likeminded trading partners to do the same (thus helping build a new global norm). As a world leader in the global digital economy, U.S. firms have faced the brunt of China's use of censorship for protectionism. However, they're far from alone. But, thus far, other countries have not prioritized the issue and developed a plan and policies to respond to it (both in China and elsewhere around the world).

Given that censorship may relate to legitimate content moderation concerns online (whether related to inciting violence and terrorism, fraud, intellectual property theft, or other valid issues), the United States should work with value-sharing trade partners and international organizations (such as the Organization for Economic Cooperation and Development (OECD)) on how to build a policy framework that balances these objectives alongside free speech and other related values, while also including clear guidance and a fair legal process for both firms and users to navigate what can be a tricky issue.

This is important as the United States needs to be able to present an alternative set of policies for countries to use to address their legitimate concerns about illegal material online so that they don't feel they have to resort to overly broad censorship policies, like in China. Having a better, alternative framework to account for legitimate content moderation concerns would make it harder for countries to misuse censorship or content moderation as a disguised trade barrier given there is a clear alternative that is non or least trade restrictive.

REFERENCES

1. United States Trade Representative (USTR), *Section 1377 Review On Compliance with Telecommunications Trade Agreements* (Washington, D.C.: USTR, 2015), https://ustr.gov/sites/default/files/2015-Section-1377-Report_FINAL.pdf.
2. State Council, Provisions on Administration of Foreign-Invested Telecommunications Enterprises. Decree of the State Council of the People's Republic China No.333, December 11, 2001.
3. United States Trade Representative (USTR), *2018 Report to Congress On China's WTO Compliance*, (Washington, D.C.: USTR, 2019), (Washington, D.C.: USTR, 2015),.
4. Ibid
5. Li Yuan, "A Generation Grows Up in China Without Google, Facebook or Twitter," *New York Times,* August 6, 2018, https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html.
6. Nigel Cory, "Testimony: Censorship as a Non-Tariff Barrier to Trade" (The Information Technology and Innovation Foundation, June 30, 2020), https://itif.org/publications/2020/06/30/testimony-us-senate-subcommittee-trade-regarding-censorship-non-tariff.
7. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (The Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost; Nigel Cory, "China and the United States: Digital Protectionism vs. Digital Free Trade" (The Information Technology and Innovation Foundation, October 18, 2019), https://itif.org/publications/2019/10/18/china-and-united-states-digital-protectionism-vs-digital-free-trade; Nigel Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules" (The Information Technology and Innovation Foundation, May 9, 2019), https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital.
8. Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules"; Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?"; Stephen Ezell, "ITIF Filing to USTR on Section 301 Investigation of China's Policies and Practices Related to Tech Transfer, IP, and Innovation" (The Information Technology and Innovation Foundation, October 25, 2017), https://itif.org/publications/2017/10/25/itif-filing-ustr-section-301-investigation-chinas-policies-and-practices.
9. Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules."
10. Cory, "Cross-Border Data Flows"; Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018," Information Technology and Innovation Foundation, January 28, 2019, https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018; Nigel Cory, "The Worst Innovation Mercantilist Policies of 2017," Information Technology and Innovation Foundation, January 22, 2019, https://itif.org/publications/2018/01/22/worst-innovation-mercantilist-policies-2017; Robert Atkinson and Nigel Cory, "Comments: Circular of the State Internet Information Office on the Public Consultation on the Measures for the Assessment of Personal Information and Important Data Exit Security," Information and Technology and Innovation Foundation, May 11, 2017, http://www2.itif.org/2017-china-handling-data.pdf; Martina F. Ferracane and Erik van der Marel, "Patterns of Trade Restrictiveness in Online Platforms: A First Look," (European Center for International Political Economy, January 2019), https://ecipe.org/publications/pat-terns-of-trade-restrictiveness/.
11. Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules."
12. Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?."
13. Berhan Taye, "The State of Internet Shutdowns Around the World," (Access Now, July 2019), https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf.
14. See: Robert Atkinson, "Don't Just Fix Safe Harbor, Fix the Data Protection Regulation," *Euractiv,* December 18, 2015, https://www.euractiv.com/section/digital/opinion/don-t-just-fix-safe-harbour-fix-the-data-protection-regulation/.
15. For example, a report for the European Parliament on data protection in China states that there is "no common ground… found between two fundamentally different systems both in their wording and in their raison d'etre." The report takes a relativist approach by saying China's culture and approach to human rights means the European Union should treat China differently when it comes to trade and privacy issues, despite the fact that "China does not have a

general data protection act but traces of data protection may be found in a multitude of sector-specific legal instruments." Paul de Hert and Vagelis Papakonstantinou, "The Data Protection Regime in China" (Brussels: report for the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, October 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

16. Cory, "Testimony: Censorship as a Non-Tariff Barrier to Trade"; Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?"; Nigel Cory, "Response to the Public Consultation for the European Commission's White Paper on a European Approach to Artificial Intelligence" (The Information Technology and Innovation Foundation, June 12, 2020), https://itif.org/publications/2020/06/12/response-public-consultation-european-commissions-white-paper-european.

17. Nigel Cory, Robert Atkinson, and Daniel Castro, "Principles and Policies for "Data Free Flow With Trust"" (The Information Technology and Innovation Foundation, May 27, 2019), https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust.

18. For example, the CCP's "Office of the Central Cyberspace Affairs Commission" depicted China's tech giants' growing global market share, the spread of Chinese standards, and increasing influence on discourse and legal norms as part of the same effort. Thomas Eder, Rebecca Arcesati, and Jacob Mardell, "Networking the 'Belt and Road' - The future is digital" (The Mercator Institute for China Studies, August 28, 2019), https://www.merics.org/en/bri-tracker/networking-the-belt-and-road; (translation) "In-depth implementation of General Secretary Xi Jinping's strategic thinking of network power, solidly promote network security and informationization," Central Information Office network theory study group, September 15, 2017, http://www.qstheory.cn/dukan/qs/2017-09/15/c_1121647633.htm; Elsa Kania et. al, "China's Strategic Thinking on Building Power in Cyberspace" (New America, September 25, 2017), https://www.newamerica.org/cybersecurity-initiative/blog/chinas-strategic-thinking-building-power-cyberspace/.

19. Stephen J. Ezell and Robert D. Atkinson, "The Middle Kingdom Galapagos Island Syndrome" (The Information Technology and Innovation Foundation, December 15, 2014), https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.

20. Office of the United States Trade Representative (USTR), "2018 National Trade Estimate Report on Foreign Trade Barriers" (Washington, D.C.: USTR, 2018), https://ustr.gov/sites/default/files/files/Press/Reports/2018%20National%20Trade%20Estimate%20Report.pdf.

21. Stephen J. Ezell and Robert D. Atkinson, "The Middle Kingdom Galapagos Island Syndrome: The Cul-De-Sac of Chinese Technology Standards" (Information Technology and Innovation Foundation, December 2014), https://itif.org/publications/2014/12/15/middle-kingdom-galapagos-island-syndrome-cul-de-sac-chinese-technology.

22. Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018."

23. Bjorn Conrad, Jaqueline Ives, Mirjam Meissner, Jost Wübbeke, and Max Zenglein, "Made in China 2025" (MERICS, August 12, 2016), https://merics.org/en/report/made-china-2025

24. Ibid.

25. Thomas Eder, Rebecca Arcesati, and Jacob Mardell, "Networking the 'Belt and Road'" (MERICS, August 28, 2019), https://merics.org/en/analysis/networking-belt-and-road-future-digital.

26. Ben Sin, "The Key For Huawei, And China, In 5G Race Is A Turkish Professor," *Forbes,* July 27, 2018, https://www.forbes.com/sites/bensin/2018/07/27/the-key-for-huawei-and-china-in-5g-race-against-the-u-s-is-a-turkish-professor/#5f335880222b; Xiao Xin, "Lenovo 5G incident shows need for Chinese companies to cease mindless competition," *Global Times,* May 16, 2018, http://www.globaltimes.cn/content/1102630.shtml.

27. Guo Yiming, "Digital economy cooperation to empower Belt, Road," *China News,* December 4, 2017, http://www.china.org.cn/world/2017-12/04/content_50083923.htm.

28. Stephen Ezell, "New legislation required to secure US semiconductor leadership," *The Hill,* June 30, 2020, https://thehill.com/opinion/technology/505054-new-legislation-required-to-secure-us-semiconductor-leadership.

29. John VerWey, "Chinese Semiconductor Industrial Policy: Past and Present" (United States International Trade Commission, July, 2019), https://www.usitc.gov/publications/332/journals/chinese_semiconductor_industrial_policy_past_and_present_jice_july_2019.pdf.

30. Stephen Ezell, "An Allied Approach to Semiconductor Leadership" (Information Technology and Innovation Foundation, September 17, 2020), https://itif.org/publications/2020/09/17/allied-approach-semiconductor-leadership.

31. Austin Ramzy and Chris Buckley, "'Absolutely No Mercy': Leaked Files Expose How China Organized Mass Detentions of Muslims," *New York Times,* November 16, 2019, https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html.

32. "Apple's Chinese troubles," *The Economist*, February 20, 2020, https://www.economist.com/business/2020/02/20/apples-chinese-troubles.

33. Masha Borak, "Apple removed 805 apps in China from 2018 to 2019," *Abacus News*, January 29, 2020, https://www.abacusnews.com/tech/apple-removed-805-apps-china-2018-2019/article/3047325; Nick Statt, "Apple's iCloud partner in China will store user data on servers of state-run telecom," *The Verge*, July 18, 2018, https://www.theverge.com/2018/7/18/17587304/apple-icloud-china-user-data-state-run-telecom-privacy-security.

34. Pei Li and Cate Cadell, "Airbnb to start sharing Chinese host information with government," *Reuters*, March 28, 2018, https://www.reuters.com/article/us-airbnb-china/airbnb-to-start-sharing-chinese-host-information-with-government-idUSKBN1H41JJ; Tara Francis Chan, "Airbnb has removed listings in Beijing and canceled bookings during China's annual parliament because it wants to be 'good neighbors'," *Business Insider*, March 5, 2018, https://www.businessinsider.com/airbnb-removed-china-listings-during-national-peoples-congress-2018-3.

35. "What do I need to know in order to sign up for an Airbnb account as a resident of China, or if I change my residence to China?," Airbnb website, https://www.airbnb.com/help/article/1035/what-do-i-need-to-know-in-order-to-sign-up-for-an-airbnb-account-as-a-resident-of-china-or-if-i-change-my-residence-to-china.

36. Marczak and Scott-Railton, "Move Fast and Roll Your Own Crypto A Quick Look at the Confidentiality of Zoom Meetings"; Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China," New America blog post, June 1, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

37. Kari Paul, "Zoom will provide end-to-end encryption to all users after privacy backlash," *Guardian*, June 17, 2020, https://www.theguardian.com/technology/2020/jun/17/zoom-encryption-free-calls; https://blog.zoom.us/end-to-end-encryption-update/.

38. Paul Mozur, "Zoom Blocks Activist in U.S. After China Objects to Tiananmen Vigil," *New York Times*, June 11, 2020, https://www.nytimes.com/2020/06/11/technology/zoom-china-tiananmen-square.html.

39. "Improving Our Policies as We Continue to Enable Global Collaboration," Zoom blog, June 11, 2020, https://blog.zoom.us/wordpress/2020/06/11/improving-our-policies-as-we-continue-to-enable-global-collaboration/.

40. "Improving Our Policies as We Continue to Enable Global Collaboration," Zoom blog.

41. "Silicon Valley weighs whether to leave Hong Kong," *FT,* July 8, 2020, https://www.ft.com/content/9c06e9df-0ca2-485b-8afe-98e51f529373; Bill Bishop, "One country, one Internet?; TikTok; Gaokao; Floods in China; US FBI head on China." Sinocism, July 7, 2020, https://sinocism.com/p/one-country-one-internet-tiktok-gaokao.

42. Articles 38 and 43

43. "Council question: Requests made to information and communication technology companies for disclosure and removal of information," May 6, 2020, https://www.charlesmok.hk/legco/council-question-requests-made-to-information-and-communication-technology-companies-for-disclosure-and-removal-of-information/.

44. Newley Purnell, "Google, Facebook and Twitter Suspend Review of Hong Kong Requests for User Data," *Wall Street Journal,* https://www.wsj.com/articles/whatsapp-to-suspend-processing-law-enforcement-requests-for-user-data-in-hong-kong-11594034580.

45. "Duncan Introduces the "TELL" Act," Press Release, May 26, 2020, https://jeffduncan.house.gov/media/press-releases/duncan-introduces-tell-act.

46. "H.R. 6942 (IH) - Internet Application Integrity and Disclosure Act," https://www.govinfo.gov/app/details/BILLS-116hr6942ih.

47. "S.2743 - A bill to establish the China Censorship Monitor and Action Group, and for other purposes," https://www.congress.gov/bill/116th-congress/senate-bill/2743/text.

48. Robert Atkinson and Clyde Prestowitz, "China's reaction to the pandemic shows why the U.S. and its allies need a NATO for trade," *The Washington Post,* May 20, 2020, https://www.washingtonpost.com/opinions/2020/05/20/chinas-reaction-pandemic-shows-why-us-its-allies-need-nato-trade/.

49. Gerry Shih, "Bristling at calls for coronavirus inquiry, China cuts Australian beef imports," *The Washington Post,* May 12, 2020, https://www.washingtonpost.com/world/asia_pacific/bristling-at-calls-for-coronavirus-inquiry-china-fires-trade-salvo-at-australia/2020/05/12/29c53058-93fe-11ea-87a3-22d324235636_story.html.

50. Joseph de Weck, "China's COVID-19 Diplomacy is Backfiring in Europe," Foreign Policy Research Institute, April 21, 2020, https://www.fpri.org/article/2020/04/chinas-covid-19-diplomacy-is-backfiring-in-europe/.

51. Daniel Castro and Alan McQuinn, "Cross-Border Data Flows Enable Growth in All Industries" (Information Technology and Innovation Foundation, February 24, 2015), https://itif.org/publications/2015/02/24/cross-border-data-flows-enable-growth-all-industries.

52. Matthew Slaughter, "How U.S. Multinational Companies Strengthen the U.S. Economy" (Business Roundtable andThe United States Council Foundation, 2009), https://www.uscib.org/docs/foundation_multinationals.pdf.

53. Robert Atkinson, "How the U.S. Government Falters on Support for Innovation," *Innovation Files Post,* August 28, 2019, https://itif.org/publications/2019/08/28/how-us-government-falters-support-innovation.

54. Robert Atkinson, "The Case for a National Industrial Strategy to Counter China's Technological Rise" (Information Technology and Innovation Foundation, April 13, 2020), https://itif.org/publications/2020/04/13/case-national-industrial-strategy-counter-chinas-technological-rise.

55. Ibid.