

**Post-Hearing Written Submission
Nigel Cory
Trade Policy Analyst
Information Technology and Innovation Foundation**

**Before the
United States International Trade Commission**

**Regarding Investigation No. 332-585: Foreign Censorship Part 1:
Policies and Practices Affecting U.S. Businesses
August 3, 2021**

Contents

- Overview..... 4**
- What Does Censorship as a Non-Tariff Barrier Look Like? 4**
- The Challenge of Defining, Identifying, and Measuring Censorship as a Non-Tariff Barrier: .. 5**
 - The Potential Use of WTO Trade Law Principles to Assess Censorship-Related Trade Barriers . 7
 - Blocking Content: The Need for a Nuanced Assessment 9
 - Website Blocking for Copyright Enforcement is Not Censorship..... 10
 - “Throttling,” Internet “Blackouts,” and Other Measures that Impact Internet Connectivity... 12
 - Restrictions on Virtual Private Networks have Trade Implications..... 14
 - Using the Growth in Virtual Private Network Use as a Proxy to Measure the Value of Digital Market Access 16
 - Data Localization as a Cudgel for Censorship 18
- The Impact on the United States..... 20**
 - U.S. Content Creators 21
 - The U.S. Video Game Industry 22
 - U.S. Cloud Services 22
- The World Leader: China’s Use of Censorship as a Non-Tariff Barrier to Trade 26**
 - China’s Direct Blocking and Throttling of U.S. Firms..... 26
 - China’s Cloud Market Access Restrictions 30
 - China’s Cloud vs. the Global Cloud 34
 - Censorship Is One of Many Barriers to Trade in Cultural Content in China 38
 - Discriminatory and Opaque Content Review Processes: Video Games, Movies, and TV Shows 39
 - China Use of Quotas and Revenue Sharing Limits to Restrict U.S. Market Access and Profitability 40
 - China’s Use of Distribution Restrictions 40
 - Investment Restrictions Keep U.S. Streaming Services and their Content Out of China 41
 - U.S. Firms in China Show the Difficulty in Navigating China and the Value of Market Access41
 - Airbnb 42
 - GitHub..... 42
 - LinkedIn 43
 - Steam..... 44
 - Zoom 44
- Other Troubling Cases: India, Indonesia, Nigeria, and Turkey 46**

India	46
India and PUBG.....	48
Indonesia and Netflix.....	48
Nigeria and Twitter	49
Turkey and Social Media	50
Vietnam and Facebook	51
Conclusion.....	52
Endnotes	53

The Information Technology and Innovation Foundation appreciates the United States International Trade Commission's (USITC) invitation to provide a post-hearing written submission regarding its investigation into foreign censorship as a non-tariff barrier (NTB) to trade and its impact on U.S. firms and trade.

OVERVIEW

Censorship is becoming a growing barrier to trade as countries around the world enact overly restrictive and discriminatory laws and regulations around digital content they identify as "objectionable." For the United States, a lot is at stake. The United States is a world leader in both the broad set of services that make up the global digital economy and the creative sectors that make movies, TV shows, video games, e-books, and other content.

The focus of the USITC's investigation should be government action. Trade policy targets policies and practices that act as a barrier to trade. Whether individuals and firms create content (or not) and engage online is obviously related to the impact of censorship, but from a trade policy perspective, what matters are the laws, regulations, and practices that affect trade.

This post-testimony written submission highlights key forms of censorship as an NTB, ideas for potential methodology, country and sectoral profiles, and the harms caused by censorship as an NTB.

WHAT DOES CENSORSHIP AS A NON-TARIFF BARRIER LOOK LIKE?

U.S. firms and their increasingly digital goods and services are susceptible to censorship-related barriers to trade in the form of both at-the-border and behind-the-border laws, regulations, and practices. The Great Firewall of China represents a rare case where U.S. digital exports face a barrier at the border. But Internet "throttling" and blackouts are other examples of broad, major economy-wide barriers. Meanwhile, behind these clear market access barriers, U.S. firms face a complicated, opaque, and changing regulatory framework tied to content moderation and information control that together makes for a very difficult and different business environment in China, India, Turkey, and elsewhere around the world. For example, censorship is both explicit and indirectly involved in making China an especially difficult market since, in many cases, requirements are unwritten and enforcement is often arbitrary. This is in large part a conscious decision to avoid World Trade Organization (WTO) sanctions which would be much easier to put in place if the rules are on paper.

U.S. firms and their increasingly digital goods and services are susceptible to NTBs in the form of both at-the-border and behind-the-border laws and regulations.

Censorship as an NTB takes on a few key forms, such as:

- At-the-border blocking of access to websites with legal content, such as China's "Great Firewall."
- Arbitrary, opaque, and discriminatory content review processes for TV shows, movies, apps, software, video games, social media services, and other digital content.
- Quotas on certain foreign content, such as movies.

- Arbitrary, opaque, and discriminatory licensing and control over Internet, content distribution, Internet access, and Internet connectivity services, such as Internet “blackouts” and not granting licensing to video-on-demand streaming and virtual private network (VPN) services.
- Forced local data residency requirements (known as data localization) for “content moderation” frameworks that are in large part driven by censorship as governments want to remove content and speech they deem politically sensitive.

The full scope and impact of censorship-related barriers are broad, given it can be a behind-the-scenes factor in any of the examples above. For example, censorship is obviously a major factor in China’s decision to prohibit foreign firms from operating in key sectors (for example, by not giving them licenses or allowing foreign equity stakes in local firms) and through onerous, unpredictable, and discriminatory content-review processes, such as for video games and movies. Also, the full impact can be hard to estimate as it is not just decisions that block direct market access but also entails decisions to punish U.S. firms for speech or action taken outside of a market. For example, China blocked NBA basketball games due to some remarks by an NBA coach in the United States. This is indicative of the fact that the Chinese Communist Party (CCP) is increasingly assertive in punishing foreign firms for actions or speech that occurs outside of China. But likewise, ever-changing political sensitivities in China, India, Indonesia, Turkey, Russia, and elsewhere make it challenging for U.S. firms to figure out what they need to do to enter and compete in a market.

THE CHALLENGE OF DEFINING, IDENTIFYING, AND MEASURING CENSORSHIP AS A NON-TARIFF BARRIER:

There’s a sliding scale of implications that trade policy makers are dealing with in managing censorship as a trade issue. There are only a few clear-cut categories of data/content (such as those associated with child pornography) that pretty much every country recognizes should be removed or blocked. However, in the vast middle is a broad range of digital content related to political, social, and cultural issues where countries differ in terms of what is “objectionable” and what is not. Analyzing censorship and its impact on trade is therefore challenging and requires nuance.

There is a need to differentiate between good-faith efforts by countries to address legitimate issues about digital content, such as those targeting child pornography, violent extremist material, copyright-infringing material and services, and other issues where many countries mutually recognize there are problems. For example, a growing number of countries allow firms to obtain legal injunctions to get Internet service providers to block their users from accessing certain websites involved in the mass distribution of copyright-infringing material (detailed in a separate section below). This is not censorship, any more than not letting people yell fire in a crowded theatre is censorship.

Not every website should be freely accessible. Some argue that even the legitimate blocking of content helps totalitarian governments justify their own content blocks. These nations don’t need additional justification. Moreover, there is a stark difference between a government that uses transparent means within an independent legal system to block access to illegal content and one

that is engaging in censorship to control its population. Furthermore, just as supporting bans on the importation of ivory does not make one a protectionist, supporting website blocking for sites dedicated to piracy does not make one an opponent of a free and open Internet. However, when countries (such as China, Iran, and elsewhere) block access to Internet services due to the political and social nature of the content, this is censorship. Likewise, many countries have frameworks to review digital content as part of classification schemes (e.g., to designate what is safe for children). This is not censorship. However, when countries use purposely opaque (and politically motivated) assessment criteria and processes or make arbitrary decisions to block foreign services and content (such as is the case in China, Nigeria, and India), this is censorship.

Similarly, not all countries have a constitutional right, and broad legal protections, for free speech like the United States. Differing legal, social, cultural, and political values and systems mean that countries take different approaches to determine what discourse is or is not protected online, even in other democratic countries. Certain discourse and content that is legal in the United States may be illegal in other countries, such as content related to hate speech. While this may raise valid human rights concerns, it's less of a trade issue, as these cases tend to be narrowly focused and within a broader legal framework where U.S. firms have transparent criteria and legal redress to manage country-specific differences.

This highlights the importance of a careful assessment of the underlying motivation behind digital content restrictions when analyzing content moderation versus censorship and considering the trade impact. While censorship may be a primary motivation for many of these policies, by making life hard or simply keeping U.S. firms or content out of the market, the government gets the added benefit of protecting local firms from foreign competition.

Important factors and characteristics for the USITC to consider when assessing a potential censorship related policy that has a trade impact:

- A. What is the publicly stated motivation for the policy (e.g. content moderation) and is this the same as the application being reported by firms, trade associations, NGOs, and U.S. government officials (based off their own discussions with government officials and others)?
 - a. Even if the stated motivation is fair and genuine (such as updating content moderation frameworks for violent material), it may still be an unnecessary and inadvertent barrier to trade. It then becomes an issue for the U.S. government and firms to identify in what specific ways the proposal is a barrier to trade in that some of the legal and regulatory requirements may be unnecessary, disproportionate, and/or overly burdensome.
 - i. For example, are the timeframes that countries set for firms to respond to requests to remove content reasonable? Firms need sufficient time to assess the legal merits of each and every request against local laws and regulations to ensure that the request is fair and valid. Firms need in-house lawyers and others to assess the content and whether it abides by local laws.
- B. How was the policy development process carried out?

- a. Was the policy development process opaque with limited or no engagement? Was engagement superficial rather than genuine and substantive? Was the policy suddenly announced or enacted? These are all indicators that a country is pursuing a policy for censorship-related reasons. It wants to avoid scrutiny and criticism from local firms, NGOs, and foreign firms and trading partners.
 - b. The alternative: was the process open to genuine public consultations (including from U.S. firms and U.S. government representatives), held over a reasonable period of time, and did it result in local government officials using the feedback to make changes to reduce the impact on trade?
- C. How specific, detailed, and transparent are the criteria that countries use to define what exactly they want firms to remove? Is the process that governments use to enforce their criteria clear, consistent, and contestable?
- a. Countries use vague and broad definitions of “public morals” and “national security,” as part of censorship frameworks as they want to retain broad authority to intervene in digital content, free speech, and associated issues. This is usually a clear indicator that a country is using these broad powers for censorship and with little to no regard for the impact on trade.
 - i. If U.S. firms never get clear guidance on exactly what types of content are objectionable, it is tough for them to address this type of content as part of trying to operate in a market. But it becomes a clear barrier if firms never know what exactly is objectionable, which is so often the case in China.
 - b. If countries are engaged in good-faith efforts to develop a framework for a type of content they deem objectionable, but they do so in a clear, specific, detailed, and non-discriminatory manner, then it is not as clear a trade barrier to U.S. firms.
 - i. Again, not every country has constitutional protections for free speech like the United States. The United States may well disagree with the types of content that certain countries want removed (such as those related to religious issues), but it is up to the U.S. government to make the case to the local government about its views on freedom of expression, etc.

The Potential Use of WTO Trade Law Principles to Assess Censorship-Related Trade Barriers

The USITC’s assessment of censorship-related trade policies could also use core principles of WTO trade law—proportionality and necessity—to help identify and assess relevant policies. Trade law allows countries to enact censorship for a range of reasons, such as pornography, gambling, and faith-based objections, but these must be necessary and proportionate. For example, the use of these principles could well be the basis for a WTO dispute case based on the claim that China’s approach to censorship is overly broad, restrictive, and discriminatory, as it can unfairly restrict the domestic and cross-border supply of a service.

For as long as there has been international trade rules, there have been exceptions, including for countries to enact censorship measures to protect public morals. Back in 2006, academics like Tim Wu from Columbia University realized that countries were not considering the trade law

implications of overly broad online censorship.¹ A 2009 WTO trade dispute (initiated by the United States) represents the clearest example of how trade law can address issues like censorship. This case involved trading rights and distribution services for audiovisual entertainment products. China sought to justify restrictions on foreign firms involved in importing and distributing books, movies, and other “culturally sensitive” materials because it wanted to protect public morals and control content. China claimed that control of cultural content is a matter of fundamental importance, which was recognized as legitimate by the WTO dispute panel.² However, the panel’s overall verdict indicated that China’s desire to control online content does not enable it to ignore WTO rules.³

The European Center for International Political Economy (ECIPE) report *Protectionism Online: Internet Censorship and International Trade Law* presents a detailed and convincing case that a WTO dispute panel might rule that China’s permanent blocks on search engines, photo-sharing applications, and other services are inconsistent with the General Agreement on Trade in Services (GATS) provisions, even with the exceptions for morals and security.⁴ Less resourceful countries, without means of filtering more selectively, and with a censorship system based on moral and religious grounds, are more likely to be able to defend broader censorship blocks in the WTO. But the exceptions do not offer a blanket cover for the arbitrary and disproportionate censorship that still occurs despite the availability to the censoring government of selective filtering.

Article XX of General Agreement on Tariffs and Trade (GATT) and article XIV of GATS contain many relevant rules that govern the potential use of censorship. GATT permits governments to take measures “necessary to protect public morals.” GATS permits measures “necessary to protect public morals or to maintain public order.” However, Article XX of GATT outlines that, “subject 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 the same conditions prevail, or a disguised restriction on international trade.”

However, as ECIPE explains, trade law sets limits to a country’s use of censorship for moral reasons. The conditions under which these provisions can be applied tend to be quite strictly applied.⁵ GATS article XIV is even annotated by a footnote stating that the paragraph may only be invoked where a “genuine and sufficiently serious threat is posed” to a “fundamental interest” of society.⁶ They need to be deemed “necessary” when evaluated under a factor-based test.

Such factors include:

- the relative importance of the objective pursued by the measure;
- the contribution of the measure to that objective;
- the trade-restrictiveness of the measure; and
- the existence of “reasonably available” alternative measures.⁷

Given it has never been tested in a WTO dispute, it is unclear how the necessity test relates to the footnote under article XIV. This would be an extremely difficult question for a WTO dispute

panel to answer once faced with questions about how to assess and respond to the threat from certain online content.⁸

As it relates to proportionality, a WTO dispute panel would take into consideration the capabilities of the state in considering whether a measure was reasonable and whether there is a genuine alternative for the desired level of protection. The burden of proof is on the complainant to prove such a measure actually exists.⁹ On this factor alone, it seems clear that active filtering is far less trade-restrictive than a total, permanent ban of a site and service. There's also the related aspect of proportionality and discrimination in that censors in China tend to block entire foreign websites, while a domestic site may simply be asked to remove individual pages.

The growing importance of digital content to trade makes it important to challenge and (hopefully) rectify China's overly expansive use of censorship as an NTB. It also highlights some useful criteria and principles to assess censorship-related measures in determining what is necessary and proportionate versus what is not. A case brought before the WTO over censorship would inevitably prompt a debate about sovereignty and the scope of trade-related issues under the WTO, but it's a fair debate given the original negotiators of GATT and GATS envisaged limits to how countries could use public morals and other exceptions as disguised forms of protectionism. There needs to be a debate about where and how to draw the lines against disproportionate, arbitrary, and opaque censorship. As ECIPE notes in conclusion, although the dispute settlement mechanism of neither the WTO nor other trade instruments could be used to eliminate Internet censorship, they might limit the use of its more commercially damaging forms.¹⁰ Either way, ECIPE's assessment provides some useful analysis for USITC to use to assess censorship-related trade measures around the world.

Blocking Content: The Need for a Nuanced Assessment

Policymakers need a framework to understand the benefits of Internet openness that is more nuanced than the conventional wisdom that "more is better." Indeed, calls for "no online censorship" and that "all Internet packets should be treated the same," or statements that "information wants to be free," imply policymakers should always pursue Internet openness as a goal in itself.¹¹

However, the relationship between an increase in Internet openness and the benefits of the Internet is not linear. For example, allowing child pornography online would technically increase the openness of the Internet. This level of openness, however, creates severe drawbacks. Moreover, some policies that reduce Internet openness, at least in the minds of hardcore net neutrality advocates, such as the prioritization of Internet traffic for first responders, are desirable.¹² Lastly, the social benefits of Internet openness can vary depending on each nation's different cultural values.

On the global Internet, there are universal goods and bads, as well as local goods and bads.¹³ A universal good related to Internet openness is an increase in trade. A universal bad is something most, if not all, nations consider bad, such as the sale of widely banned drugs online. In contrast, a local good or bad is something wherein there is no international consensus. For example, some nations value freedom of speech more than others and thus protect hate speech,

thereby increasing freedom of expression and Internet openness—while countries such as Germany have made certain hate speech illegal.¹⁴ In addition, some nations value privacy more than others. Certain elements of privacy regulations, such as the right to be forgotten, can reduce Internet openness and value. These differences in cultural values mean a framework that only tries to maximize openness cannot universally work.

A more useful approach is one that strives to differentiate between different scenarios. That legitimate and fair efforts by governments to block illegal content online is not censorship, such as child pornography, violent extremist material, and copyright infringing material. There will be other cases where country-specific differences (in religious, cultural, and social norms) mean that they will block some content and discourse that may be legal in other countries, but if this is done in a clear, transparent, and predictable way, then it is not so much a trade barrier. There will be other cases where governments enact opaque and unnecessary, overly broad and onerous, and discriminatory regimes to block content, in which case, it is a barrier to trade.

Practically, the goal should be to achieve a mostly open Internet by maximizing universal goods, reducing universal bads, and creating a high level of technical openness. At the architectural and protocol levels of the Internet, there is a need for commonly shared global standards to prevent the Internet from being balkanized.¹⁵

Many nations block the flow of data on the Internet that falls under the category of “universal bads,” such as child pornography and the sale of drugs. Many nations also block access to content that falls under the category of “local bads”—content that some, but not all, nations find offensive enough to block. For example, India blocks access to certain pornographic websites in order to “protect social decency.”¹⁶ Some nations block access to content most other nations would not block, such as from independent media organizations. For example, between December 2018 and March 2019, Chinese authorities shut down more than 140,000 blogs and deleted more than 500,000 articles.¹⁷

Of course, it’s incumbent on the U.S. government to push China and other countries to improve their approach to human rights and freedom of expression, which thus creates clearer and more open market access for U.S. firms that provide associated goods and services. Blocking legitimate websites clearly reduces Internet openness and the economic and social benefits the Internet provides. However, this argument may not be persuasive in nations that consider the blocked content to be a local bad, such as the *lèse majesté* laws in Thailand that forbid insulting the country’s royalty.¹⁸

Website Blocking for Copyright Enforcement is Not Censorship

A growing number of countries allow copyright holders to get Internet service providers (ISPs) to block access to websites involved in the large-scale distribution of pirated material as these sites are typically based in foreign jurisdictions with weak/non-existent intellectual property rules and enforcement (there would be other legal remedies if these services were hosted domestically). This is not censorship.

Website blocking is not antithetical to a free and open Internet. Even the most vocal supporters of Internet freedom recognize that it is legitimate to remove or limit access to some materials online, such as sites that facilitate child pornography. At the same time, some governments can and do cast too wide a net against Internet content, taking down or limiting access that is not illegal, but only upsetting to those in power. The key issue about Internet freedom, therefore, is not whether the Internet is and should be completely free or whether governments should have unlimited censorship authority, but rather where the appropriate lines should be drawn, how they are drawn, and how they are implemented. An assessment as to the impact of censorship as an NTB needs a nuanced understanding of Internet policymaking in countries around the world. Not everything blocked online should be considered censorship.

According to a 2018 Motion Picture Association (MPA) submission, at least 42 countries have either adopted and implemented, or are legally obligated to adopt, measures ensuring that ISPs block access to copyright-infringing websites.¹⁹ Some countries have had measures in place and used them for some time, others have the means to block websites but have not done so, while others are moving to enact website blocking. For example, in the European Union, at least 17 member states (including the United Kingdom, France, Belgium, the Netherlands, Germany, Denmark, Norway, Ireland, Sweden, Italy, Spain, Portugal, and Greece) have enacted website blocking, while others have relevant laws in place, but have not used them (such as Bulgaria, Croatia, Cyprus, the Czech Republic, Malta, Poland, and Romania).

Countries allow fair and legitimate blocking of websites engaged in copyright infringement given how easy it is for copyright-protected material—including books, movies, music, photos, software, and video games—to be copied and shared online across jurisdictional borders. This makes it challenging for rightsholders to protect their works online as they do offline. Intellectual property rules are territorial, while the Internet is not. Studies show that blocking regimes that target these large-scale piracy sites (not sites that accidentally host pirated material) are an effective tool in reducing piracy and increasing the consumption of legal content and services.²⁰

Critics claim that website blocking will set a negative precedent if used by democratic countries and will weaken the moral authority of democratic nations to criticize totalitarian governments for limiting Internet access unrelated to intellectual property. They claim that these governments would point to democratic nations' use of website blocking to justify their Internet censorship. But the U.S government has not abandoned its long practice of banning the use of U.S. mail to send illegal products because it fears giving an excuse to foreign governments to censor their mail. Likewise, the U.S government has not changed laws that limit the ability of newspapers to publish information that is libelous because it fears it will give comfort to nondemocratic nations that want to control information access.

Likewise, the U.S. government has not abandoned laws requiring child pornography to be blocked because it thinks it gives carte blanche approval to dictatorships that want to block dissenting websites. Governments' responses to rioters who engage in wholesale property destruction and violence isn't based on the fear that they encourage totalitarian governments to use police to suppress citizens. In short, there is no comparison between a country that uses detailed and transparent legal means, supported by an independent legal system to administer

such rules, to enforce intellectual property rights online and a country censoring political speech online.

Some opponents of website blocking have seized upon reports of governments misusing intellectual property enforcement measures for unrelated means, such as the Russian police raid on advocacy groups and opposition newspapers in the name of searching for pirated software.²¹ However, such cases are rare and would not stand up to the type of scrutiny that is involved in the hundreds of cases where website blocking has been used to fight online piracy in recent years. Online intellectual property enforcement is far from alone in being a public policy that could be misused to pursue unrelated and illegitimate objectives. In each case, what matters is the actual intent and the integrity of the process involved in administering these policies.

“Throttling,” Internet “Blackouts,” and Other Measures that Impact Internet Connectivity Governments limit and shut down access to the Internet and specific Internet applications for many reasons, including those related to censorship. For example, to quell antigovernment protests. In such instances, shutdowns can slow the flow of information regarding government wrongdoing.²²

This has obvious trade implications in that U.S. firms depend upon reliable communication networks to function and provide goods and services directly to consumers. For example, in 2021, Facebook reported that its services were interrupted 84 times in 19 countries in the second half of 2020, compared to 52 disruptions in eight countries that took place during the first half of the year.²³

One of the most frequent reasons why governments block Internet access is to slow or prevent protests—particularly violent ones. Two common ways governments engage in application blocks and shutdowns is by directing ISPs to temporarily block specific URLs, and to require providers to completely shut down their services.²⁴ The length of the shutdowns varies widely. Algeria, for example, has shut down mobile and fixed-line Internet access for as little as one hour.²⁵ In contrast, Cameroon blocked access to social media and messaging applications in its Anglophone region for several months in 2018.²⁶

In many of these cases, the goal of governments is to ensure or restore public order.²⁷ Indeed, a spokesperson for the Bharatiya Janata Party, one of India’s two major political parties, stated that shutdowns are acceptable in cases “where rumor-mongering or motivated misinformation could lead to the incitement of violence.”²⁸ There are numerous examples of governments shutting down the Internet to stop protests or the spread of violence. For example, in 2015, the government of Rajkot, a city in the Indian state of Gujarat, suspended mobile Internet services for 10 hours after a politician threatened to hold a protest at a cricket stadium in which India would be playing South Africa.²⁹ In addition, real-time network data revealed that Iraq shut down access to the Internet for roughly 75 percent of individuals in the country during anti-corruption protests in October 2019.³⁰ As with attempting to restrict cheating, shutting down Internet services in order to prevent or slow protests is economically costly. For example, India shut down mobile Internet services for more than a week in 2016 in the city of Rohtak to stop the spread of

rumors that could have exacerbated street protests.³¹ The Brookings Institute estimated that this shutdown cost India \$190 million in GDP.³²

Internet shutdowns and social media blocks are an ineffective way for governments to prevent nonviolent protests. Indeed, research suggests Internet shutdowns and application blocks can actually cause protest participants to substitute violent tactics for nonviolent action that relies on effective communication and coordination.³³ For example, an analysis of network shutdowns in India, which include both the cutting off of access to the Internet and other telecommunication services, found riots increase in intensity over the first three days of a shutdown. This research suggests that, contrary to the goals of many governments, reducing Internet access does not quell violent unrest—and at worst, may intensify unrest.³⁴

Censorship may be just one of several motivations for governments to throttle or block Internet access. Governments have also blocked Internet services to protect the revenue model of legacy telecommunications industries. For example, in 2016, Saudi Arabia banned applications that had voice and video calling functions because domestic telecom operators were losing revenue from individuals choosing to use the cheaper and often-free Internet-based communication services.³⁵ Saudi Arabia and Morocco are not alone, however. Several nations, including Qatar, have strict licensing requirements that limit the number of VoIP services available to the public.³⁶

Policymakers should understand that even temporary Internet disruptions can have significant economic effects. Like electricity blackouts, these Internet disruptions reduce productivity and result in the loss of time-sensitive transactions. For example, shutdowns have caused businesses to lose contracts by preventing them from being able to pay their suppliers and maintain contact with their clients. As a result of lost contracts, businesses have had to fire employees.³⁷ Internet shutdowns also create inefficiencies. For example, shutdowns in African countries have forced individuals to travel across borders to send emails, costing them money and time in the process.³⁸ Shutdowns can also have social costs. For example, medical professionals rely on the Internet to order supplies and treat patients, so shutdowns hamper their ability to overcome medicinal shortages and provide care and medicine to all the individuals who need it.³⁹

For example, Morocco's telecommunications firms blocked access to applications such as Skype, Facebook, and WhatsApp for roughly 10 months in 2016. Morocco's Telecommunications Regulatory National Agency only allows commercial exploitation of IP telephony service through licensed operators; however, Internet-calling applications are often free or relatively cheap.⁴⁰ The Moroccan government supported the ban, stating none of the VoIP services had the required licenses—which represented a policy for a more closed Internet, as these Internet apps should not require a license. Brookings estimated this disruption cost Morocco nearly \$1.8 million per day.⁴¹

Several organizations have quantified the economic costs of Internet shutdowns and blockages, which can range from blocking access to certain mobile applications to cutting off access to the entire Internet. For example, Deloitte estimated that a shutdown of the Internet and all its services would cost well-connected nations nearly \$24 million for every 10 million inhabitants

per day.⁴² The Brookings Institution, ICRIER, and the Collaboration on International ICT Policy in East and Southern Africa (CIPESA) have each created formulas to demonstrate the costs of Internet shutdowns.⁴³ While the formulas vary, they each use a nation's or region's GDP and level of connectedness or size of their digital economy to estimate the costs of shutdowns.⁴⁴ Brookings examined 81 Internet shutdowns and major Internet application blockages that occurred between July 1, 2015, and June 30, 2016, and found these disruptions cost at least \$2.4 billion in GDP globally.⁴⁵ Similarly, ICRIER examined mobile and fixed-line Internet shutdowns in India between 2012 and 2017, finding 16,000 hours' worth of disruptions cost the nation's economy \$3 billion.⁴⁶ Finally, CIPESA found the 176 days of total Internet shutdowns between 2015 and 2017 in 8 different African nations cost \$218 million.⁴⁷

Restrictions on Virtual Private Networks have Trade Implications

Countries like China, Russia, and others increasingly target not just online content and discourse but the tools that people and firms use to connect to the Internet, such as virtual private networks (VPNs). China and other's censorship and information control efforts extend to restrictions over all forms of connectivity, including how U.S. firms use VPNs to allow intra-firm networks and operations and cross-border sales and service.

In the last few years, China has tightened regulations and restrictions around these VPNs, which seriously affects the reliability and quality of connections to the global Internet for China-based U.S. firms and their staff. China has a track record of targeting individuals (consumers) wanting to use VPNs (such as by shutting down Chinese VPN providers). As mentioned, China targets the development and distribution of these services, often via intermediaries such as app stores and cloud storage providers.⁴⁸ Interestingly, periodic clamp downs on VPNs (which are relaxed afterward) show that Chinese authorities realize that there is some need for balance in how they restrict VPNs as they are used by government officials, academics, researchers, and others as a lifeline for must-have global services (such as allowing Chinese government officials to access and use Twitter or for researchers to access academic literature).

Restrictions on VPNs are also a barrier to the cross-border sale, development, service, and use of software. U.S. software firms are reportedly finding it increasingly difficult to license and sell software to users in China (or existing customers that want to use the same software when setting up in China, such as multinationals) that rely on VPNs as these connections are increasingly poor and unreliable. Similarly, some U.S. venture capital firms and software developers are reportedly avoiding China-based investments or partners as poor connectivity with the global Internet makes it uncertain whether the firm would be able to scale globally even if their software product is valuable.

Many U.S. and foreign firms use VPNs for corporate purposes to connect locations and services inside of China with the rest of the world and to protect their communications from hacking and government surveillance.⁴⁹ These firms typically use their own global VPN infrastructure to connect users and business units around the world (such as via Multiprotocol Label Switching (MPLS)). In 2018, China started managing and limiting the connections that U.S. firms use so that they maintain oversight of this connectivity. It enacted new regulations that forced firms to buy and use expensive licensed VPN services, which are from one of China's three state-own

telecommunication firms: China Telecom, China Unicom, and China Mobile.⁵⁰ The Ministry of Industry and Information Technology said these restrictions are in accordance with goals and provisions set out by the government created Cross-border Data Telecommunications Industry Alliance.⁵¹

These restrictions were especially disruptive to businesses that depended on their VPNs for access to cloud services and data security. They can also be more expensive and unreliable, while exposing communications to government surveillance. Indicative of this, the *Financial Times* reported that an American non-profit group and a British company told them that their company-built VPNs had been blocked, disrupting their ability to do business.⁵² It also reported another representative from an American Fortune 500 company as saying that it had become increasingly difficult to access blocked websites from their Beijing office, which similarly uses a corporate VPN.⁵³

With these restrictions in place, U.S. firms have a few options to maintain connectivity with the rest of the Internet—each with their own disadvantages. Firms can use a managed IPsec VPN (one of two common VPN protocols) from one of the Chinese telecommunication firms. But this means that all outbound traffic is forced through the Great Firewall. This allows the provider to block restricted traffic (which of course is hardly ideal for firms) and causes connectivity performance issues (i.e., delays in websites loading).⁵⁴ Where firms setup private connections (such as private leased VPN lines), Chinese regulations state that “the basic telecom operators shall establish a centralized user archive and specify that the lines are leased for the purpose of internal office use only and shall not be used to connect data centers or service platforms at home or abroad for telecommunication services.”⁵⁵

Otherwise, a foreign firm may use an authorized MPLS circuit from within China to connect outside (such as to Hong Kong or Singapore), where it then connects into the firm’s existing VPN network. However, this is very expensive, takes a long time to deliver, and is bandwidth-constrained. A typical Chinese MPLS circuit is somewhere south of 20 MB of bandwidth, and it could cost \$15,000 to \$20,000 for a single circuit.⁵⁶ Similarly, “where multinational companies lease international private lines to build their own office networks, qualified third parties (including enterprises with licenses for domestic IP-VPN services and fixed-network domestic data transmission services) may be entrusted to provide outsourcing services such as system integration and maintenance and management.”⁵⁷ Some providers have recently developed a software defined wide-area network (WAN) that is supposedly compliant with China’s new regulation, which provides supposedly seamless and high-speed access between intra-China and international networks.⁵⁸ But these still provide the Chinese government with access and oversight over these data transfers.⁵⁹

At the heart of these restrictions is the Chinese government’s drive to control content it deems illegal. It tries to create a very narrow and controlled lane for business-specific connections, while strictly prohibiting the potential use of these connections for broader dissemination to the public. Beyond the examples above, this approach extends to those few, limited, and restricted U.S. cloud providers in China. China restricts and manages how cloud service operators connect their China-based cloud service platform servers with the overseas network, which must be done

through the international Internet service portal approved by the Ministry of Industry and Information Technology (MIIT), rather than private lines, VPNs, or other channels.⁶⁰ No matter the connection, the Chinese government wants to have visibility of the network and the data.

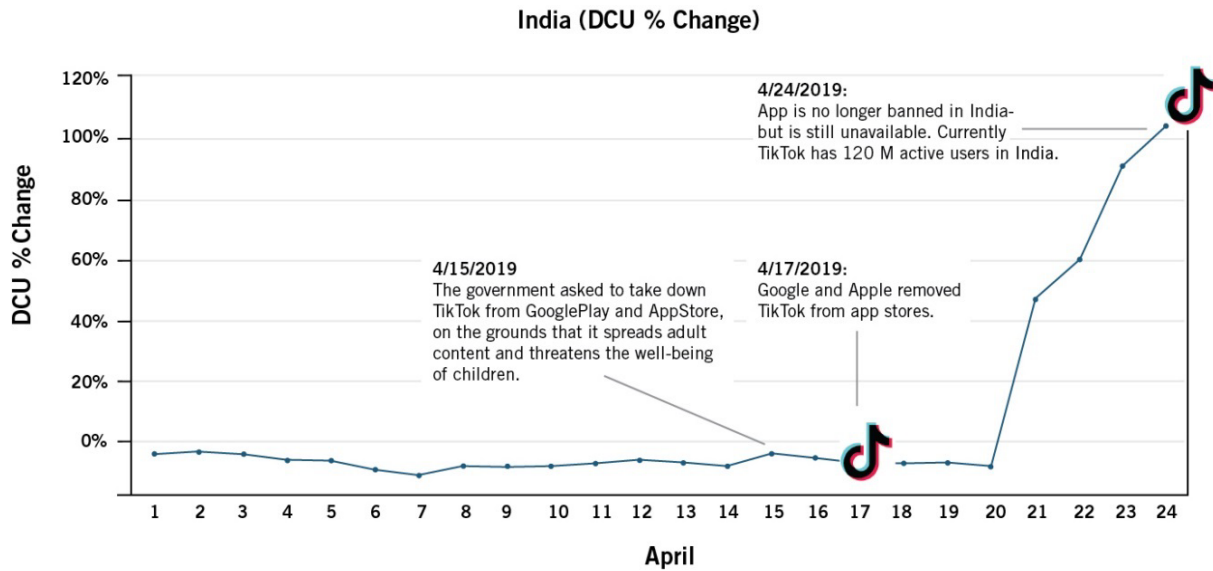
These restrictions give Chinese authorities the capability to oversee and control flows of commercial information and data, but it does not mean that they're necessarily examining company traffic (if there's no specific reason for China's government to focus on a firm's communications). Obviously, firms with sensitive intellectual property may have legitimate fears about how these rules raise the risk of inadvertent disclosures given China's aggressive and comprehensive cyber theft of trade secrets. There are other ways and tools for U.S. firms to mitigate this risk, such as encryption. However, the U.S. government and firms should be concerned as China's restrictions over commercial connectivity services that are needed for day-to-day trade and business operations are unique, complicated, and act as yet another regulatory hurdle for U.S. firms to clear in seeking to simply enter and operate in China.

Using the Growth in Virtual Private Network Use as a Proxy to Measure the Value of Digital Market Access

One way to begin understanding the value of a mostly open Internet and the costs of unnecessary content blocking is to analyze the growth in VPN use when governments block access to certain Internet-enabled services (see figure 1). While it is challenging to use growth in VPN use to place a precise value on a more open Internet, the decision of individuals to use a VPN in order to access blocked Internet services demonstrates the services have value. As a result, policies that block access to websites, applications, or VPNs reduce both the openness of the Internet and its value. High-level aggregate data obtained from Pango, an Internet privacy and security company that also offers a VPN service, allowed for the tracking of the increase in the number of daily connected users in countries in the days before and after bans of websites or mobile applications, which led to a better understanding of the value of certain Internet services.

For example, on April 15, 2019, India's supreme court refused to stay the Madras High Court ban on TikTok, an app that allows users to create and share videos.⁶¹ The court ruled that TikTok could expose minors to sexual predators, pornographic content, and cyberbullying.⁶² Google and Apple subsequently removed the app from their respective app stores by April 17.⁶³ On April 24, the Indian court vacated its original order after TikTok appealed the decision, stating it had removed inappropriate content.⁶⁴ Between April 17 and 24, the number of individuals in India using Pango's VPN more than doubled (figure 1).⁶⁵

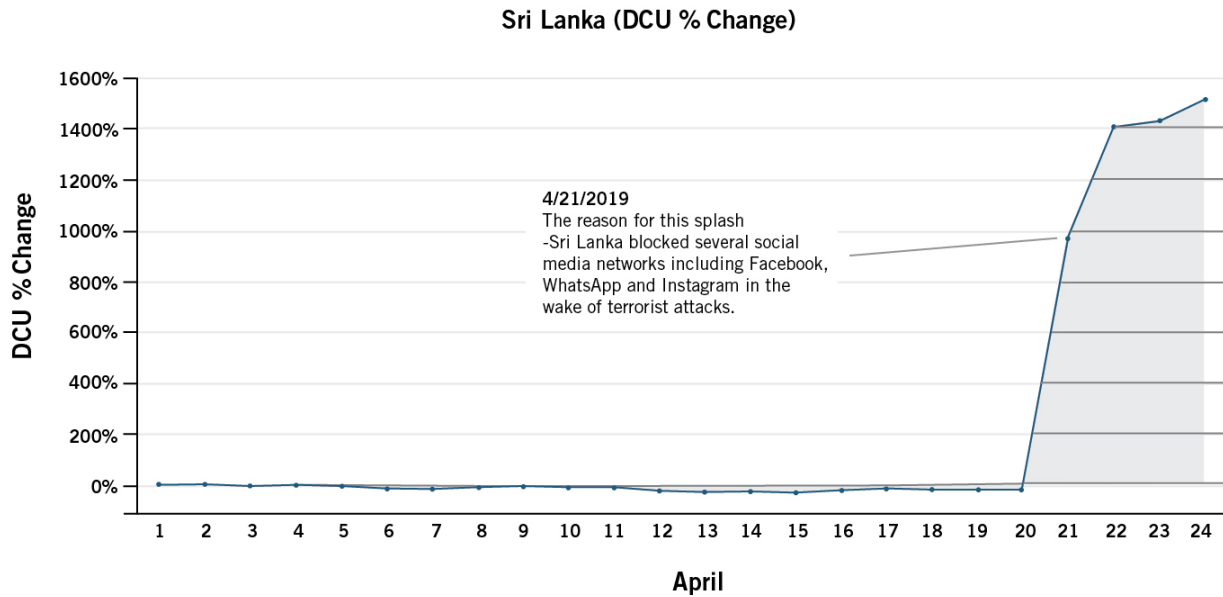
Figure 1: Hotspot Shield VPN by Pango usage before and during India’s ban of TikTok, April 15–24, 2019.⁶⁶



Similarly, on April 21, 2019, Sri Lanka banned the social media networks Facebook, WhatsApp, and Instagram for nine days to stop the spread of misinformation following terrorist attacks that killed or injured hundreds. Over the first four days of the ban, Pango’s number of daily connected users more than tripled (figure 2).⁶⁷

While it is possible other variables besides bans could have caused that increases in the number of daily users, it is important to note Pango’s number of daily users was relatively static in each of the preceding weeks. Consequently, these examples likely show that users, when faced with attempted blocks of Internet-enabled applications, value those applications enough to use a technical workaround. The surge in downloads of TikTok once the application was available again provides further evidence of the value of the application to users. It was the 90th most downloaded app in the Google Play Store in India the first day it was available following the ban, and the 15th most downloaded only a day later.⁶⁸

Figure 2: Hotspot Shield VPN by Pango usage before and during Sri Lanka’s ban of social media, April 21–30, 2019



These examples provide possible ideas to use proxies to develop indicative estimates of the impact that censorship-related trade barriers cost U.S. firms. These examples also provide clear evidence that specific foreign (U.S., Chinese, and other) major tech services are used (and valued) in local markets. Obviously, efforts to provide a more-specific indicative estimate would benefit from firms providing some indicative estimate as to the economic value of users in certain markets, such as via the value of advertising (and other revenue) earned in a market over a year. With these metrics, a model could then provide a very indicative estimate of the impact on a per day/week/month cost to a U.S. firm being blocked.

Data Localization as a Cudgel for Censorship

Countries use data localization as a cudgel to force foreign firms to provide easier access to data for surveillance and political purposes and force compliance with censorship requirements. Commonly mixed into this rationale is the specter—both real and imagined—of foreign surveillance as a rationale for data localization when it actually enables their own surveillance.

Digital authoritarian governments—led by China and Russia—see physical access to data centers as a critical enabler of surveillance and political control. Data localization enables political oppression by bringing information under government control and allowing the government to identify and threaten individuals, impacting privacy, data protection, and freedom of expression.⁶⁹ China retains broad and vague legal authority in its laws to potentially access data for national security, public interest, and political purposes.⁷⁰ The lack of an independent judiciary and the opaque nature of these laws make it hard to judge how China uses these broad powers.⁷¹ Yet, this doesn’t stop these countries from referring to “data privacy” as a motivation for localization.⁷²

Countries are using data localization as a cudgel to force them to require firms to comply with restrictive content moderation and censorship requirements. China is clearly the world leader in using data localization for both surveillance and censorship. Pakistan and Vietnam are considering similar approaches. Meanwhile others, like India, are enacting such short time frames for firms to respond to content takedown requests that it creates a de facto localization requirement as firms would not be able to respond otherwise.⁷³

Data localization is central to Vietnam's evolving online censorship and surveillance regime. Vietnam's Law on Cybersecurity requires online firms to store personal and other types of data and to establish a local office in Vietnam.⁷⁴ Its motivation is broad and vague, to protect national security, social order and safety, social ethics and the health of the community.⁷⁵ Draft decrees implementing the law reduced the number of conditions that trigger data localization from four to three and changed the different types of data that need to be stored in Vietnam. However, it expanded the range of added services that must store data locally. On top of this, Vietnam enacted other regulations on the control of content, data localization, and data retention requirements for social networks and information aggregation websites (presumably covering search engines).⁷⁶ This forces firms to: have a license; have at least 1 server in Vietnam for inspection at any time required; to store detailed information about users and their activities; to setup a filtering system to identify illegal content; and to remove illegal content within three hours.

According to statements from Ministry of Information and Communication officials, foreign companies' compliance with censorship and content moderation requests has increased from 20-30 percent of the time to nearly 80-90 percent.⁷⁷ Even before Law on Cybersecurity came into effect, Vietnamese government officials claimed that Google and Facebook responded to thousands of requests from the government to remove illegal content.⁷⁸ However, Facebook, for example, states that it has only received a few dozen requests for data and that it has only granted access to half of those requests.⁷⁹

Pakistan is taking a similar approach. In November 2020, Pakistan released (draft) rules (the "Removal and Blocking of Unlawful Online Content") that grant the government broad authorities to pressure companies to block content that is critical of the government and facilitate broad access to user data.⁸⁰ An earlier draft of this law was leaked (after already being approved by Pakistan's cabinet) and subsequently suspended following severe criticism from local and international human rights organizations and tech sector representatives.⁸¹ As is often the case with restrictive content moderation frameworks, there has been a lack of transparency and genuine consultation with civil society and businesses.⁸²

Broad data localization requirements remain part of the latest draft.⁸³ It also forces service providers to setup a local office and designate a local representative.⁸⁴ It also makes it mandatory for service providers and social media companies to retain information including traffic data linked to blocked content. It only gives service providers 6 to 24 hours to comply with government requests to remove or block content, which is far too short for companies that deal

with millions of users and massive amounts of content to review the request and determine whether it is de facto illegal under local laws.

Pakistan's draft rules go well beyond content moderation, impacting data privacy.⁸⁵ This draft side-steps Pakistan's Prevention of Electronic Crimes Act 2016 (PECA), of which, Section 37 already gives the Pakistan Telecommunication Authority (PTA) broad powers to block and remove content online. The new draft allows PTA to avoid safeguards in PECA, intervene on behalf of law enforcement agencies, and ask social media companies to directly provide data to law enforcement. In addition, the draft rules require service providers to provide decrypted and readable information about subscribers and their activity and content when required. Failure to provide decrypted data can lead to a \$3 million fine. Forcibly breaking the encryption is a direct attack on data privacy and security as it is an essential tool for both.

Foreign social networks, search engines, and other internet services face far greater legal and financial risks if they do not restrict illegal content and respond quickly to takedown requests from the government. Compliance should not be surprising. The onerous and restrictive nature of Vietnam's framework means that it is likely that only large firms will be able to enact the IT and legal compliance framework to provide services in Vietnam.

THE IMPACT ON THE UNITED STATES

The impact on U.S. trade, competitiveness, and innovation is many, varied, and significant. U.S. firms have already lost billions of dollars in sales in key sectors due to these practices, and this number will only increase as protected Chinese firms grow and expand globally and as other countries emulate its approach or adopt their own. Tech firms and content creators losing access to foreign markets reduces their global market share and revenue, which reduces their ability to support R&D, content creation, and associated U.S.-based operations.

From a potential methodological perspective, the USITC could assess the potential trade-related impact of censorship related policies along a spectrum of scenarios: full, unbridled censorship that acts as a clear and major barrier to market entry and operations to scenarios whereby U.S. firms have a clear understanding of local requirements for local "bads," yet there are specific provisions within this local market that are unnecessarily broad or restrictive.

Similar to ITIF efforts, the USITC could also estimate the trade impact when U.S. firms and products are completely excluded from a market (such as China), but it is still difficult as local market factors (like differing consumer preferences) mean that U.S. firms may not have the same market share as at home or in neighboring markets. However, an indicative estimate is still significantly valuable and worthwhile.

Scenarios that involve arbitrary and ad hoc changes, such as Internet blackouts, may require the USITC to take a different approach, such as using key market metrics and VPN use as a proxy. However, it's challenging to assess the individual and cumulative impact of U.S. firms and products being temporarily banned (as in Internet "blackouts") or when certain content (whether TV shows or video games) are only temporarily blocked or are delayed in being released. However, the impact of each market barrier adds up in similar ways as how increases in tariffs or slow and

costly import customs clearance deleteriously affect trade in physical goods. An alternative idea would be for the USITC to develop generic scenarios that model actual situations U.S. firms have faced in Sri Lanka and elsewhere by using reasonable assumptions about market size, shares, and value to estimate the digital economy impact over varying lengths of time (1 week, 1 month, and 1 year).

ITIF's research on the impact shows that whatever way you look at it, especially in China, the economic impact is not trivial. 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. 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. And it is important to remember that this was all during a time when China was already running significant trade surpluses with the United States.

If U.S. industries lose market share to unfairly competing firms supported by their innovation mercantilist governments, it means two things. First, sales fall. This is true because global sales are largely fixed, and if a mercantilist-supported competitor (unfairly) gains market share, then the market-based competitor loses share. Second, because profits decline more than sales, it becomes more difficult for the market-based innovator to reinvest revenues in the next generation of products or services, meaning that the mercantilist-supported entrant has an advantage in creating the next generation of products.

Related to this, the U.S. International Trade Administration (ITA) estimated in 2016 that every billion dollars of services exports supports over 6,700 jobs.⁸⁶ This study uses input-output analysis to measure the relationship between exports and jobs for 1999-2015. The ITA model to estimate this impact could potentially be adjusted to assess the impact that censorship-related barriers have on U.S. employment based on lost market revenue. The ITA's subsequent report "Jobs Supported by Exports Methodology" could also be useful in this regard.⁸⁷ The USITC could also review the Internet Association's use of ITA methodology for its estimate for the number of jobs supported by digital exports.⁸⁸ Other studies, such as "Estimating the relationship between exports and the labour market in the UK," review the ITA and other methodologies in making their own estimate.⁸⁹

U.S. Content Creators

The U.S. movie industry's role in the U.S. economy is large and inevitably affected by restrictions in China and other countries. In 2019, the movie industry's exports totaled \$16.3 billion, which was a surplus of \$9.4 billion. The movie industry directly supports 892,000 jobs and another 1.6 million jobs indirectly. These jobs are in producing, marketing, and manufacturing motion

pictures, television shows, and video content and in distributing motion pictures, television shows, and video content to consumers (e.g. television broadcasters, cable and pay TV companies, and online video services). Half of these direct jobs pay higher salaries (\$86,000) than the national average (\$57,266).⁹⁰

This trade impact of China's censorship and market restrictions (detailed separately below) has grown over time. Before COVID-19 hit, China was on track to overtake the United States as the world's largest movie market in 2020.⁹¹ While U.S. movie-ticket sales (pre-COVID) remained relatively flat, China's sales have more than tripled since 2011.⁹² China has become an important market delivering profits that support Hollywood's blockbuster franchise offerings. Overseas box office revenue is what often turns somewhat new and ambitious films (like *Interstellar* or *Life of Pi*) into blockbusters. The Hollywood releases that break out in China are generally the same ones that succeed globally.⁹³ While China cannot be counted upon to bail out big-budget movies that bomb in the United States, Hollywood wants to (at least) be able to count on potential revenue to justify the budgets that keep the industry growing.

The problem is that as China's own filmmakers get better (due in part to Chinese government support and protection), U.S. content creators have an even harder time competing for the limited attention and ticket spending that they're allowed. In 2019, China's box office was dominated by local films—eight of the 10 top-grossing films were domestic movies—which is a worrying sign for Hollywood.

Let there be no doubt: China sees the movie industry as a strategic industry of the future, not only for the export revenues it will bring in, but for the opportunity to export the Chinese Communist Party worldview. This is why restricted market access, and calls to limit U.S. access in China, only speed the process by which China gains global market share at America's expense.

The U.S. Video Game Industry

The U.S. video game industry is huge and growing. Restrictions in China have a major impact, and if they're replicated elsewhere, it'll only grow larger. The U.S. game industry is creating high-paying jobs, driving advanced technology development, supporting entrepreneurial efforts, overtaking other entertainment industries, and spreading the wealth to many different states.⁹⁴ A 2019 report estimated that the gaming sector directly generated economic output of \$40.9 billion and provided direct employment to 143,045 people.⁹⁵ Employees in the industry earn an average compensation of about \$121,000 a year. There are over 3 billion people who play video games worldwide. The future of the U.S. video game industry is therefore increasingly dependent on sales in other countries.⁹⁶

U.S. Cloud Services

Given their central role in facilitating the storage and dissemination of digital services and content, cloud services are often the target of censorship-related restrictions, especially in China (detailed below). However, censorship is usually just one of many motivations, including digital protectionism. What is at stake in pushing for fair cloud market access in China is the U.S. cloud sector's ability to earn the revenue that drives ever-greater R&D and business operations in the United States, and globally. Not only are U.S. firms losing out on market access and revenue due

to China's protectionism, but they are also losing market share and revenue in third-country markets as Chinese firms use their protected home market to expand globally, and other countries or regions (such as Europe) seek to emulate China's approach. U.S. cloud firms are in an ongoing race for innovation advantage as their Chinese competitors also commit ever-growing amounts of money and effort to fund the R&D that will define their respective competitive positions in the future.

U.S. policymakers need to support U.S. cloud firms as their innovative capabilities help drive America's long-term economic growth. For instance, at least half of America's economic growth can be attributed to scientific and technological innovation.⁹⁷ However, such innovation does not fall like manna from heaven. Rather, innovation is a product of complex national innovation systems, supported by a thoughtful and comprehensive set of innovation-enabling public policies that collectively impact the capacity and ability of both private and public actors to effectively innovate.

The U.S. cloud sector can be characterized as an innovative industry, which exhibits a few specific characteristics. First, the rapid and regular development of new processes, products, or services—many of them disruptive in nature—is critical to their competitive advantage. Their success depends not on making a particular good or service cheaper, but on creating the next-generation product. Second, the marginal cost of selling the next product or service is significantly below the average cost of producing it in innovation-based industries. The digital content and services industry is perhaps the most extreme example of this. In some cases, the first version of a service costs hundreds of millions of dollars to create, while additional digital copies are produced at virtually no cost. Finally, innovation industries depend more on intellectual property—particularly science- and technology-based IP—than other industries. For example, software depends on source codes.

Chinese digital protectionism undermines the three key factors needed to maximize innovation in the U.S. cloud sector:

1. Ensuring the largest possible markets: For innovation industries with high fixed costs in design and development, but lower marginal costs of production, large markets are critical because they enable firms to cover those fixed costs—so unit costs can be lower and revenues for reinvestment in the next generation of innovation higher. This is why firms in most innovation industries, like cloud services, are global.

2. Limiting nonmarket-based competition: Large markets enable firms to sell more. But if larger markets come with larger numbers of competitors, total sales per firm can remain the same, or even fall. Conventional wisdom holds that this competition is good for innovation. However, many studies have demonstrated that innovation and competition can be modeled according to an inverted “U” relationship, with both too much and too little competition producing less innovation.⁹⁸ Chinese industrial policy has allowed less competitive firms to enter and grow thanks to protectionism. Not only this, but China supports their global expansion.
3. Ensuring strong intellectual property protections: Firms in innovation-based industries depend on intangible capital, much of it intellectual property. Strong intellectual property protections are needed to enable inventors to realize economic gains from their inventions— further giving them the ability to reinvest those profits into the next generation of innovative activities. However, if competitors are able to enter into or remain in a market because they obtain an innovator’s intellectual property for less than the fair market price (through either theft or coerced transfer), they are able to siphon off sales that would otherwise go to innovators. This could ultimately drive innovators out of a particular market or out of business entirely.

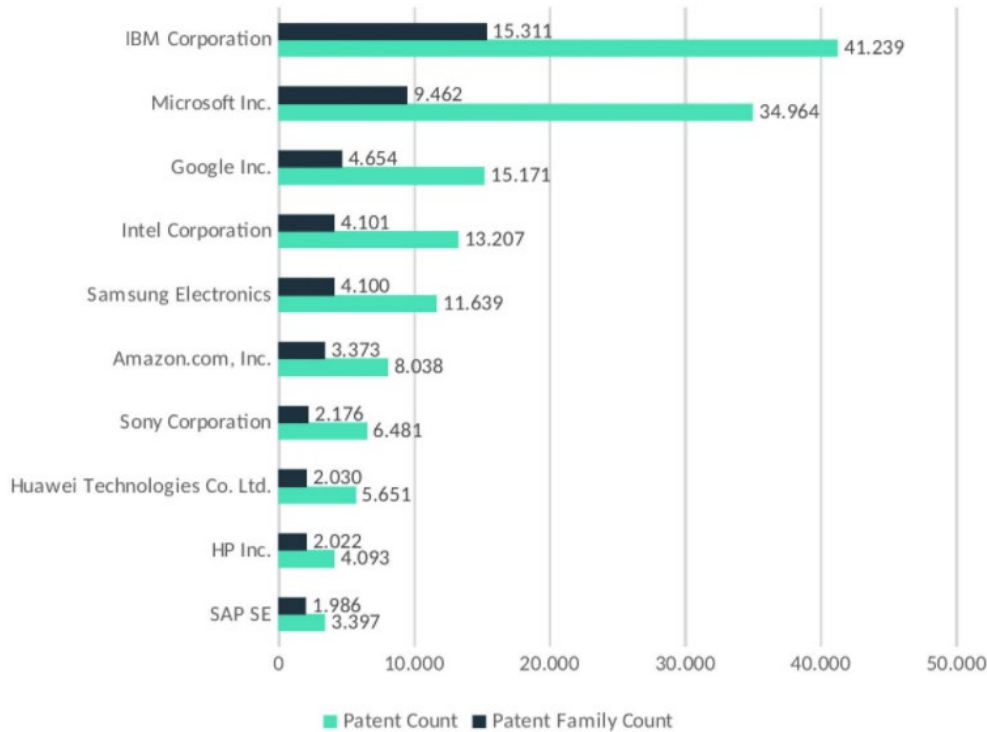
U.S. cloud firms deserve attention as they are among the most innovative in the world. Google, Amazon, Microsoft, and others invest more in R&D than nearly all other firms. In 2020, Amazon invested \$40.4 billion, Alphabet (Google's parent company) invested \$27.3 billion, Microsoft invested \$19.3 billion, Apple invested \$18.8 billion, IBM invested \$6.3 billion, and Oracle invested \$6 billion.⁹⁹ It is not only the total amounts of R&D that’s important to consider, but also where they were directing it: in targeting cybersecurity, cloud computing, AI, analytics, 5G and 6G, and mobility.

For example, Google just announced plans to invest over \$7 billion in new operations and data centers across the United States, creating at least 10,000 new full-time jobs in America in 2021.¹⁰⁰ Google will expand data centers in Nebraska, South Carolina, Virginia, Nevada, and Texas, and the company will establish its newest cloud engineering site in Durham, North Carolina. Google’s 2020 U.S. Economic Impact Report outlines how its services (such as Google Search, Google Play, YouTube, and Google advertising tools) helped provide \$426 billion of economic activity for more than 2 million American businesses, nonprofits, publishers, creators, and developers.¹⁰¹

But Chinese cloud firms are spending more on R&D to close the technological gap with U.S. competitors. In 2020, Huawei invested \$20 billion in R&D, while Alibaba invested \$7.4 billion.¹⁰² China's top 100 Internet companies increased their R&D investments by \$21.9 billion in 2019, which is a 45 percent increase in R&D spending compared to 2017.¹⁰³ Huawei boosted its R&D expenditures from \$12 billion in 2018 to \$20 billion in 2020, with R&D investments now accounting for approximately 20 percent of the telecommunications giant's overall revenue.¹⁰⁴

The U.S. cloud sector’s world-leading innovation is also clear in terms of intellectual property (figure 3).¹⁰⁵ Alphabet, IBM, Intel, Microsoft, and Apple are among the world’s leading developers of valuable patents, with IBM leading U.S. companies for the 26th year in a row with a total of 9,100 patents in 2018.¹⁰⁶ Of those, more than 2,000 were related to cloud computing. Other areas of patenting activity include AI, blockchain, quantum computing, and security.¹⁰⁷

Figure 3: Top owners of cloud computing patents (2010-2018, global, IPLytics analysis)¹⁰⁸



U.S. cloud firms’ global operations and research network support all this R&D spending and patenting. Market access is one driver of where U.S. firms setup AI R&D labs, but it’s far from the only one. For example, in 2019, AWS established an IoT labs in Shenzhen (and Taiwan). It also operates an AI R&D lab in Shanghai. However, research shows that U.S. tech firm’s global research operations still greatly benefit R&D in the United States. A Center for Security and Emerging Technology (CSET) report shows that Amazon, Apple, Facebook, Google, IBM, and Microsoft have AI R&D labs and staff around the world.¹⁰⁹ For the four companies where CSET could find information on labs—Facebook, Google, IBM, and Microsoft—they found 62 labs conducting AI R&D. While most of these labs (68 percent) were located outside of the United States (with 10 percent in China, with six labs), 68 percent of AI staff at these companies are in the United States.¹¹⁰

Global R&D networks are also necessary to access local talent. A Microsoft Research representative told CSET, “some of the people we are hiring today in China and India are the exact same people we would normally be hiring in Redmond, Boston, or NYC, but today they are not able to get visas to immigrate to the U.S.”¹¹¹ This is indicative of the need for the U.S.

immigration system to make it easy for highly-skilled workers to migrate and work in the United States.¹¹² But it also shows how global research and market operations benefit R&D in the United States.

THE WORLD LEADER: CHINA'S USE OF CENSORSHIP AS A NON-TARIFF BARRIER TO TRADE

China is by far the worst offender in using censorship as a barrier to digital trade. U.S. firms have lost significant revenue by being blocked or inhibited from accessing and operating in the Chinese market. Within the Chinese context, censorship means broad, discriminatory, and arbitrary control over data, digital content, distribution platforms, IT infrastructure, and the respective firms involved in each. China uses opaque, discriminatory, and arbitrary content moderation and control rules to severely limit or fully prohibit foreign firms and their digital products from accessing multiple sectors of the Chinese market. Chinese protectionism in these sectors has already inflicted significant costs on U.S. trade and firms, and the threat will only grow with the continued proliferation and acceptance of these practices. While censorship is far from China's only (digital) protectionist tool, it is a key one that has led to a generation of Chinese consumers unaware of the vast differences between their Internet consumption and the rest of the world's.

China's Direct Blocking and Throttling of U.S. Firms

The impact of China's censorship and blocking of U.S. firms 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. China has gradually been ratcheting up the restrictions so that it is more often at the restrictive end of the spectrum. 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.¹¹³ 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).¹¹⁴

In a similar way, China has "throttled" access to foreign websites to make them so slow as to be unusable. Throttling is often a precursor to being blocked completely. For example, before Google was fully blocked, 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. Furthermore, in 2007, China temporarily re-directed all China-based requests for Google, Yahoo, and Microsoft to Baidu.¹¹⁵ The case of Microsoft's Bing is typical. When it was blocked in January 2019, Bing was the only major foreign search engine left in China. News reports quote anonymous sources that stated that China Unicom, one of China's major state-owned telecom companies, had received an order from the government to block Bing for "illegal content."¹¹⁶ Attempts to access cn.bing.com from China resulted in a (nameserver) connection error. As of December 2018, Bing held a 2 percent market share in China (far behind Chinese industry leader Baidu, with 70 percent), but it enjoyed a niche market for English-language searches.¹¹⁷

Most of the foreign online services, apps, or intermediaries that China blocks are rarely revised and lifted. 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; 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.

The status of a range of key U.S. and foreign firms and services blocked or throttled in China:

- Amazon
 - Twitch (a live video streaming service) has been blocked since September 2018.¹¹⁸
 - Local marketplace Amazon.cn shut down in 2019, due to a small market share (not due to being blocked). Amazon focuses on “cross-border commerce.”¹¹⁹ China is among the small number of countries where Amazon Prime Video is not available.¹²⁰
- Box.com
 - There appears to be a soft block on Box's cloud and sync services. Users who have Box pre-installed (e.g., travelers) can generally use the service, or through a China-specific link. Box appears to work best for those who are visiting rather than long-term residents.¹²¹
- Dropbox
 - First blocked in May 2010.¹²² Temporarily restored in February 2014, but then blocked again in June 2014.¹²³
- Facebook (further details below).
 - Main Facebook website was blocked in 2009. Instagram was blocked in September 2014. WhatsApp was blocked in September 2017.¹²⁴
 - Operates an online advertising unit for Chinese customers to target foreign markets. In 2018, China was the second-largest source of foreign revenue for ad spend on Facebook.¹²⁵
- Google (further details below).
 - Temporarily blocked in 2002, but was later re-opened. However, Google decided to withdraw its search engine from China in 2010 and direct all traffic to google.com.hk (which is blocked in China).¹²⁶ Google also operates an online advertising unit in China.
 - YouTube was blocked on-and-off in the late 2000s before being permanently blocked in March 2009.
 - Also blocked: Gmail, Google Drive, Google Docs, Google Play, Google Translate, Google Calendar, Google Picasa, Google Groups, Google Keep, Google Voice, Google Wallet, Google Earth, Google Earth, Google Chrome homepage, Google Code, Google Blogspot, and Google Feedburner.¹²⁷

- Microsoft (further details below).
 - Microsoft OneDrive was blocked in 2014.¹²⁸
 - Bing was the last major U.S. search engine blocked in China in January 2019.¹²⁹
- News services
 - *The Washington Post, The Guardian, Bloomberg, The New York Times, Reuters, The Wall Street Journal, BBC Chinese, Chosun Chinese, and Google News* are all blocked in China.¹³⁰
- Other search engines:
 - DuckDuckGo, Baidu Japan, Baidu Brazil, Yahoo Hong Kong, and Yahoo Taiwan are all blocked in China.¹³¹
- Pinterest
 - Blocked in 2017.¹³²
- Reddit
 - Blocked in August 2018.¹³³
- Slack
 - Access has been inconsistent for years, despite not being completely blocked.¹³⁴
 - China, along with a number of countries have recently blocked certain online services, including AWS, which hosts Slack, making it very difficult for such services to access those markets.¹³⁵
- Snapchat
 - Unclear when first blocked, but Snap has a small research office in China despite the block.¹³⁶
- Twitter
 - Blocked in June 2009.¹³⁷

Google has been one of the major casualties of China’s approach to censorship and digital protectionism. It entered China in 2006 with a local search engine, under an arrangement with the government that required it to purge search results on banned topics.¹³⁸ In a first for Chinese users, Google placed a notice that content had been removed when users searched for it, but this apparently wasn’t popular with regulators.¹³⁹ From 2006 to 2010, Google China fought skirmishes with the Chinese government over content restrictions.¹⁴⁰ Google struggled to comply with ever-tightening censorship requirements and a far-reaching hacking attack (known as Operation Aurora) that targeted everything from Google’s intellectual property to the Gmail accounts of Chinese human rights activists.¹⁴¹ So, in 2010, Google shut down its search engine. China’s state-controlled media quoted a State Council Information Office official saying that “Google has violated its written promise it made when entering the Chinese market by stopping filtering its search service and blaming China in insinuation for alleged hacker attacks.”¹⁴²

At this time, Google trailed its main Chinese rival, Baidu.com, with 33 percent market share to Baidu's 63 percent.¹⁴³ China has since blocked the full suite of Google services (as listed above). In August 2018, media reports suggested that Google was working on a secret prototype of a new, censored Chinese search engine, called Project Dragonfly.¹⁴⁴ In mid-December 2018, Google suspended its development efforts, in part due to political opposition in the United States.¹⁴⁵ China has gone so far as to block Google Scholar, a benign search engine for academic literature that many researchers rely upon. Lack of access to this service clearly inhibits China's broader innovation goals.¹⁴⁶ Media reports stated that Google Scholar was on a priority list to be allowed back through the Great Firewall, but this hasn't happened.¹⁴⁷

Since 2010, Google has maintained only limited connections and entry points into China. It has an active business distributing online ads for desktop computers and mobile applications, and Chinese makers of smartphones use its Android mobile device software. Google has setup a research center that focuses on AI, but the focus will be on developing AI for global products.¹⁴⁸ In 2018, Google's revenue in Greater China (which includes mainland China as well as Hong Kong, Macau, and Taiwan) grew more than 60 percent to more than \$3 billion.¹⁴⁹ In 2018, Google indirectly accessed China via a \$550 million investment in prominent Chinese online retailer JD.com. As part of this, Google and JD.com formed a strategic partnership where the latter connects its supply chain and logistics expertise with the Google Shopping platform.¹⁵⁰ JD.com also setup a Google Express site in March, 2019.¹⁵¹ Together, the partners aim to compete with Amazon and Alibaba, especially in fast-growing south east Asian markets.¹⁵² However, the Google Shopping portal is blocked in China.

Facebook's main social network site was blocked in 2009, followed by Instagram in 2014, and Whatsapp in 2017. But this has not stopped Facebook from repeated attempts to access the market.¹⁵³ In 2016, Facebook started developing software tools for third parties to use to abide by censorship laws as it relates to stories and topics that may appear on the social network.¹⁵⁴ In 2017, Facebook developed a photo-sharing app called "Colorful Balloons" that was released through a separate local company (without providing the firm's name).¹⁵⁵ In 2018, there were media reports that Facebook had gained approval to open a subsidiary in the Chinese province of Zhejiang, which Facebook said it would use for research. But then the registration disappeared and references to the subsidiary were partly censored in Chinese media. Media reports state that the approval was rescinded after a disagreement between officials in Zhejiang and the Cyberspace Administration of China, claiming the latter had not been consulted more closely.¹⁵⁶ This incident underscores how much of a challenge it is for Facebook—a global social network—to get into China in any meaningful way. It also highlights how U.S. firms seeking to enter the market must navigate multiple, often opaque rules and laws within a system in which cities, provinces, and national government agencies all vie for influence and can make key decisions.

Facebook is now limited in how it can operate in China. Facebook has setup an experience center through a Chinese advertising partner (Meet Social), where potential customers learn how to advertise on Facebook to access customers elsewhere around the world. In 2019, Meet Social reportedly expected \$1 billion to \$2 billion in ad sales on Facebook and Instagram.¹⁵⁷ In total, Facebook's revenue from Chinese-based advertisers reached an estimated \$5 billion in 2018, or about 10 percent of its total sales.¹⁵⁸

Apple has major operations in China. In the 2019 financial year, Apple earned \$44bn in revenue in Greater China, mostly from selling iPhones.¹⁵⁹ However, to do so it had to agree to store Chinese user data in the country and to remove offensive apps, such as news and VPN apps, from its app store. Apple removed 805 apps in China from 2018 to 2019.¹⁶⁰ Most recently, Apple removed the app game “Plague” following the coronavirus outbreak.¹⁶¹

While standard iPhone services like iMessage work in China, many paid offerings that help Apple generate revenue from services related to its devices aren’t available in China. Only six months after launching in China, Apple closed the iTunes Store (Apple Books, Apple TV, Apple News, and iTunes Movies) in April of 2016.¹⁶² While the Chinese government initially approved Apple’s introduction of the services, a few months later the State Administration of Press, Publication, Radio, Film and Television demanded it be closed.¹⁶³ China’s blocking extends to newer services like Apple TV+ video streaming, the Apple Card, Apple Arcade, and the News+ subscription.¹⁶⁴ While China is a huge market for Apple and its smart devices, the company’s ability to earn from associated services is severely constrained. This puts a sort of cap on its current and future profitability.¹⁶⁵

China’s Cloud Market Access Restrictions

Despite U.S. firms being world leaders in cloud services, China’s discriminatory and restrictive market access and licensing regime means that there are very few U.S. cloud providers in China. For most U.S. cloud service firms, it’s essentially closed. Given U.S. cloud firms can’t provide these services on a cross-border basis (largely due to restrictive Chinese policies), the only option to access the Chinese market is to establish a contractual partnership with a Chinese partner (in order to get the necessary licenses), which includes handing over valuable technology, intellectual property, know-how, and branding.¹⁶⁶ U.S. cloud providers have no direct relationship with customers in China and no ability to independently develop their business, or those of their partners. Companies’ efforts to build business thus inevitably build up the Chinese partner, who may well become a future global competitor.

This is exactly China’s goal. As U.S. cloud firms have told USTR during Special 301 investigations, China uses a restrictive, yet ambiguous, licensing process to benefit Chinese cloud computing businesses and pressure technology transfer. China first tacitly permits foreign investors to partner with licensed Chinese cloud service providers to gain market access, and then, once key technology and know-how is injected into these partnerships, China resolves the regulatory ambiguities that necessitated these arrangements in favor of the Chinese partner, resulting in the transfer of technology to the Chinese partner.¹⁶⁷ These are just some of the reasons why U.S. firms want greater, clearer market access (and not through joint ventures).

China’s cloud market has become more restrictive over time. In 2015, China released regulations for several services it considers value-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,” it has much greater freedom to restrict market access to foreign tech firms. This is because China made commitments as part of its accession to the WTO in 2001 to provide nondiscriminatory treatment and market access to foreign firms in “computer and related services.”¹⁶⁸ This category of

Internet-based computer services includes email, voicemail, online information and database retrieval, electronic data interchange, enhanced facsimile services, code and protocol conversion, and online information and/or data processing.¹⁶⁹ 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.

China then introduced a requirement for telecom and ISPs to apply for licenses for each subcategory of VATS services, raising the potential for government agencies to discriminate against foreign firms.¹⁷⁰ For example, China's new subcategory, "Internet-based resources collaboration services," means that providers of cloud computing application services including IaaS and PaaS have to apply for multiple licenses, given some firms and services cross over into multiple categories. As SaaS is considered too close to information services, which China is extremely sensitive to for censorship reasons, it is essentially closed and considered separately as part of its service and licensing requirements.

In 2016, China made another set of significant changes to its licensing and regulatory regime that further discriminated and restricted U.S. technology firms involved in cloud computing, big data, and other information services. 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 means that U.S. firms 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. In March 2017, 50 U.S. lawmakers complained about these new rules in a letter to China's ambassador to the United States, stating that the change would force U.S. companies to essentially transfer ownership and operations of their cloud systems to Chinese partners (which is essentially what it did).¹⁷¹ USTR's 2018 broad-ranging investigation into China's acts, policies, and practices related to technology transfers, intellectual property, and innovation noted, "According to numerous submissions in this investigation, an important example of how ambiguity in China's administrative licensing process is used to pressure technology transfer arises in the field of cloud computing."¹⁷²

China's discriminatory licensing process and restrictive JV requirements keep many leading U.S. cloud firms out, and, of those few it lets in, it strictly controls how they operate. As of 2009, although there were over 20,000 local companies licensed to provide VATS in China, only 30 or so licenses were issued to foreign companies, including five U.S. companies.¹⁷³ More recent industry estimates state that only around 5 percent of VATS licenses go to foreign firms. As USTR notes, although not explicitly stated in rule or policy, China appears to apply an economic needs test to new entrants in this sector to avoid "unhealthy competition."¹⁷⁴ By that, they mean fair competition. This section analyzes the role of China's growing cloud market in the global market and the operations of some of the few U.S. cloud service providers in China.

The global nature of cloud computing and China's large and growing digital economy means that forgoing China's market is simply not a commercially viable option for U.S. cloud firms.

Furthermore, many of their multinational customers demand globally available services. This is why a few large U.S. firms have run the gauntlet and setup operations in China, all within the confines of its strict conditions. For example, Microsoft partnered with 21Vianet (in 2014), SAP with China Telecom, and IBM with a group of local companies.¹⁷⁵

China's market restrictions have forced U.S. cloud service firms to use a few different models to enter and compete in China, each with their own advantages and disadvantages (in terms of capital intensity, compliance burden, and the range of services they're able to offer). Furthermore, of the few U.S. firms that do operate in China, they essentially must develop separate local services and infrastructure to their global operations. U.S. firms operate their China data center services (such as IaaS and PaaS) separately from their global cloud services.¹⁷⁶ Either way, U.S. 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.

China has broad data localization requirements that make it illegal, or uncertain and very difficult, for U.S. cloud firms to transfer data out of China.¹⁷⁷ It also prohibits them from providing many cross-border cloud services and creates technical and operational issues for U.S. cloud firms, such as being able to seamlessly transfer data in and out as part of software updates, debugging, technical upgrades, and other cross-border services. China would need to provide broad digital market access to make it meaningful for U.S. cloud firms given the critical role of value-added services that U.S. firms deploy alongside their cloud services, whether this is consumer-facing services (such as email) or enterprise-facing (such as VPNs and data analytic services).

Generally, China's market is broken down into three components for U.S. firms to target: domestic firms, multinational companies, and Chinese firms expanding into overseas markets. Basically, U.S. cloud firms are competing to accelerate the globalization of Chinese firms, while empowering foreign multinationals in terms of their cloud needs in China. U.S. firms are more competitive in these two categories given they have larger global operations for these firms to use, but Chinese firms are rapidly expanding global operations, meaning this advantage will diminish.

In 2014, Microsoft launched its Azure cloud services in a partnership with 21Vianet, which was the first international public cloud service to become generally available in China. Microsoft plans to expand its partnership, effectively doubling its cloud computing capacity in China.¹⁷⁸ Microsoft Azure's partnership is not a JV, but a licensing agreement, with Shanghai Blue Cloud Technology Co., Ltd., which is wholly owned by 21Vianet. This licensing model is reportedly what the Chinese government prefers, as it gives the local partner even greater control over data center operations. For Microsoft, it provides a local partner to then sell and service a broad range of software (especially its Office 365 portfolio) and to compete in the otherwise excluded SaaS market. In 2018, Microsoft's Office 365 (which is a type of SaaS) became a leader in China's SaaS market.¹⁷⁹ However, since Azure is IaaS, Microsoft is limited in what it can do. 21Vianet independently operates, provides, and manages the delivery of Microsoft cloud services. It also provides subscription and billing services, as well as support.¹⁸⁰ However, indicative of China's

huge market potential, even with these restrictions, Microsoft has reported growth of over 100 percent in some quarters. Also indicative of the critical role that cloud market access plays in allowing firms to offer a broader range of services, Microsoft has over 17,000 local IT system integrators that use its services.

Amazon Web Services (AWS) has had a tortured experience in China. For example, in April 2019, Amazon closed its Chinese e-commerce marketplace.¹⁸¹ In January 2021, a Beijing court ruled that AWS cannot use its AWS logo in China as it belonged to a Chinese company.¹⁸² Furthermore, China forced Amazon to sell part of its China operations to its local partner to comply with new laws (further explained below).

However, despite very restrictive access, AWS remains engaged and is expanding services to seize as much market share as it can. AWS has data centers in Ningxia, Beijing, and Hong Kong. China is the only country outside of the United States with three AWS regions. AWS partners with Beijing Sinnet Technology Co. to operate the AWS China cloud-computing service in the Beijing region. In November 2017, AWS sold the hardware for its cloud computing operation to Sinnet for \$300 million, reportedly to meet Chinese regulations which forbid foreign companies from owning or operating certain technology for the provision of cloud services.¹⁸³ Amazon made the sale in advance of Ministry of Industry and Information Technology (MIIT) plans to force firms to apply for a new operating license by the end of 2017. Since then, AWS has also partnered with Ningxia Western Cloud Data Technology Co (NWCD) to operate data centers in Ningxia.¹⁸⁴ Similar to Microsoft, AWS provides technology, guidance, and expertise to NWCD and Sinnet, while NWCD and Sinnet operate and provide AWS Cloud services to local customers.¹⁸⁵

What this means is that AWS China operates apart from AWS's global regions. AWS China uses local management console and account systems for billing and support charges, which use their own authentication for access to AWS services in China. AWS customers need to access AWS services in mainland China and Hong Kong using respective portals, which are not the same as those they'd use to access AWS services elsewhere around the world. Furthermore, AWS has more than 175 fully-functional, global services for its customers to use; however, many are not available in the China region.¹⁸⁶ Even within China, some service offerings differ. While AWS services are generally available in both the Beijing and Ningxia regions, some services are only available in one of the two regions. For example, AWS IoT Analytics is limited to businesses in the Beijing region.

AWS's operations in China continue to expand and evolve to grow market share. In 2019, AWS added a new Asia-Pacific region in Hong Kong. In March 2021, AWS announced it is expanding its partnership with NWCD to provide 130 percent more cloud capacity, and that it'll open a third cloud zone as part of its Beijing-based operations.¹⁸⁷ AWS also seeks to close a gap in offering new services. For example, it launched AWS Marketplace China in 2020, with more than 200 third-party software offerings. Similarly, AWS is expanding its Partner Program (who are specialist third parties that use AWS to build solutions and services for customers) through strategic partnerships with well-known domestic and foreign IT providers such as KPMG, Capgemini, Deloitte, Digital China, Ultrapower Software, and Futong. It has also designated 43 local partners as AWS Competent, which shows they are especially adept at using AWS services.

Like other U.S. cloud firms in China, AWS is targeting Chinese firms expanding into overseas markets such as CIMC, Globalegrow, Cheetah Mobile, Midea, OnePlus, and Huya. For example, it only took AWS five days to complete the global deployment and migration of all of OnePlus's overseas shopping sites onto a global system to support its overseas businesses.¹⁸⁸ As another example, AWS only recently announced that it will provide global cloud services for Chinese tech firm Huami (a wearable computing device vendor with operations in 70 countries and regions).

In 2015, Oracle (the largest enterprise software company in the world) partnered with Tencent to provide its SaaS, PaaS, and IaaS services.¹⁸⁹ Oracle provides the technology that powers its data centers, while Tencent Cloud provides service for consumers. Oracle has operated in China for about two decades, owns 14 branches, five R&D centers, and has nearly 5,000 employees in the country. Oracle's Asia Pacific arm accounts for about 16 percent of the company's total revenues. In 2019, Oracle closed its R&D center in China.¹⁹⁰

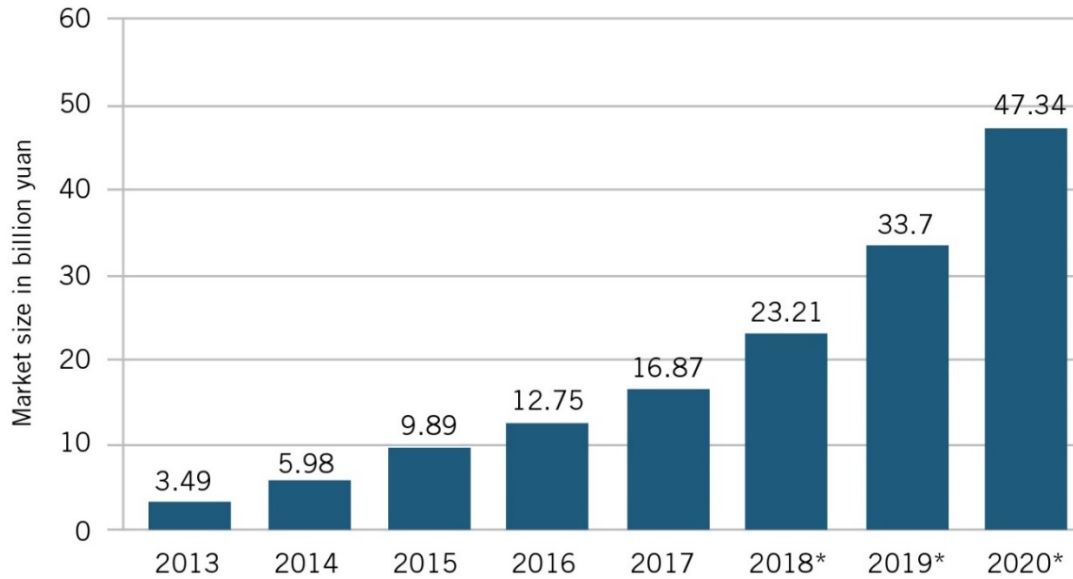
Google Cloud does not operate in mainland China. In mid-2020, Google reportedly considered a new initiative (called “isolated regions”) that would have allowed it to try and re-enter China. Google considered allowing third parties to control and manage its cloud services—such as via a locally owned company or a government agency (which it does not currently do)—in no small part due to China's market restrictions (as well as those in Europe).¹⁹¹ This follows reported talks between Google and a Chinese firm in 2017 about the potential to setup a partnership to provide cloud services in China.

China's Cloud vs. the Global Cloud

Censorship related restrictions have a direct impact in both a given market and in other markets around the world. China's restrictive approach to cloud services at home, alongside the global expansion of Chinese cloud firms, reflects this. China is the world's second-largest cloud services market. COVID-19 only accelerated its rapid growth, as China directed economic stimulus spending into supporting digital adoption.

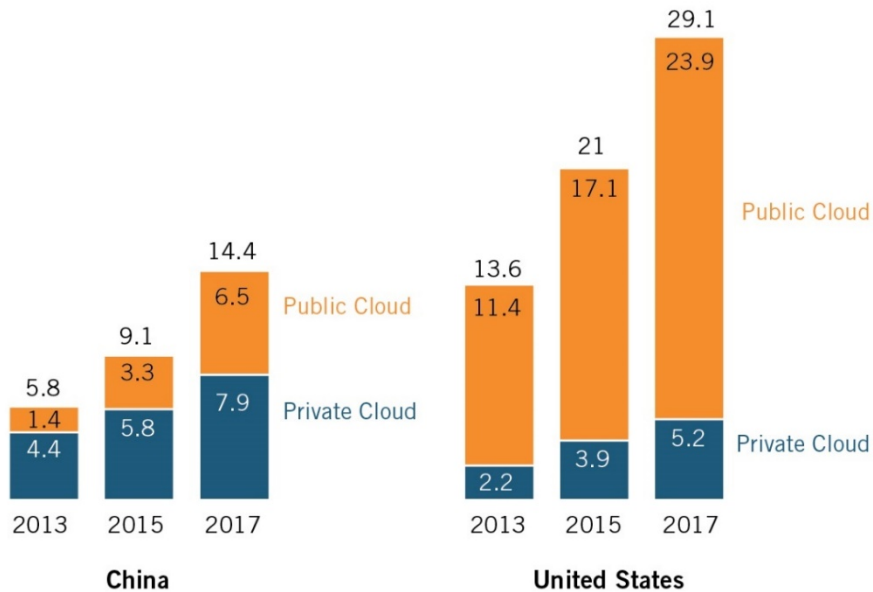
China's cloud services market is worth tens of billions of dollars and is growing rapidly.¹⁹² For example, China's SaaS market alone grew 13-fold from an estimated 3.5 billion yuan in 2013 (nearly \$500 million) to 47.3 billion yuan (nearly \$6.7 billion) in 2020 (see figure 4).¹⁹³ Total cloud spending was worth an estimated \$5 billion in the third quarter of 2020 alone.¹⁹⁴ As figure 4 below shows, China's cloud market is growing rapidly. In the first quarter of 2020, China's cloud infrastructure spending increased 67 percent year on year to \$3.9 billion, maintaining its No. 2 position behind the United States, according to data from Canalys.¹⁹⁵ China's spending accounted for 12.5 percent of the world's total (\$34.6 billion) investment on cloud infrastructure in the first quarter of 2020 compared to 10 percent in the same quarter in 2019.¹⁹⁶ In the same time period, International Data Corporation (another commercial market analysis firm) reported that China's SaaS market segment grew 57.6 percent year-over-year, while the PaaS segment expanded 64.6 percent. The sum of these two markets increased by 58.7 percent year-over-year.¹⁹⁷

Figure 4: China's software-as-a-service (SaaS) cloud market (billion yuan, 2013-2017).¹⁹⁸



China's cloud market retains enormous growth opportunities. Chinese firms spent around 14 percent of their total IT budget on cloud services in 2017—more than double the amount spent in 2013. However, even with this growth, China still lags behind global peers in terms of cloud expenditure. In the United States, for instance, cloud spending accounted for around 29 percent of the total IT budget in 2017, up from around 14 percent in 2013 (figure 5). This is indicative of the enormous growth potential that remains.

Figure 5: China vs. U.S. cloud expenditures (percent of total IT budget)¹⁹⁹



The absence of U.S. firms has allowed local Chinese firms to grow and seize the majority of China’s domestic cloud market, which is dominated by local providers, such as Alibaba Cloud, Tencent, JD Cloud, Huawei, and Baidu, as well as niche players like ChinaC, ChinaCache, ChinaNetCenter, Kingsoft Cloud, Qingcloud, Qihoo 360 Technology, Qiniu and UCloud, among others. In China, in the first half of 2020, Alibaba Cloud, Tencent Cloud, Huawei Cloud, and China Telecom together held around 44, 14, and 14 percent market share, respectively, according to Canalys. Amazon was the fifth-biggest cloud provider with around 7 percent; altogether, foreign firms make up around 20 percent of the market.²⁰⁰

Indicative of the importance of the cloud sector to Chinese tech firms, Alibaba’s revenue from cloud operations grew 50 percent during the quarter ended December 2020 to \$2.47 billion, accounting for around 7 percent of the company’s quarterly revenue. Signaling the market opportunity, Chinese firms (often supported by government policy) are investing huge amounts in new data centers. For example, in May 2020, Tencent Cloud stated it plans to invest \$70 billion in digital infrastructure to expand its cloud computing, AI, blockchain, and cybersecurity capabilities over the next five years. Similarly, in April 2020, Alibaba Cloud stated it planned to invest around \$29 billion over the next three years on cloud infrastructure.²⁰¹

The main saving grace for U.S. cloud firms is that the U.S. IaaS and PaaS market remains significantly larger than China’s, and it is also growing quickly (20+ percent a year).²⁰² The global public cloud services market grew 6.3 percent in 2020 to \$257.9 billion, up from \$242.7 billion in 2019 (figure 6).²⁰³ SaaS remains the largest market segment and is forecast to grow to \$104.7 billion in 2020 due to more firms shifting from on-premises license software to subscription-based SaaS models, in conjunction with the increased need for new software collaboration tools during COVID-19. The second-largest market segment is cloud infrastructure

as a service (IaaS), which was forecast to grow 13.4 percent to \$50.4 billion in 2020.²⁰⁴ Indicative of the pace of growth, between 2018 and 2019, global public IaaS and PaaS markets doubled in size (see figure 6).²⁰⁵ But whereas U.S. firms can obviously compete for a share of the growing demand for cloud services at home and in most other countries around the world, it can't in China, which represents a large part of the global market.

Figure 6: Worldwide public cloud service revenue and forecast (millions of U.S. dollars)²⁰⁶

	2019	2020	2021	2022
Cloud Application Infrastructure Services (PaaS)	37,512	43,498	57,337	72,022
Cloud Application Services (SaaS)	102,064	104,672	120,990	140,629
Cloud System Infrastructure Services (IaaS)	44,457	50,393	64,294	80,980

On a global basis, Amazon's worldwide market share of the public cloud has held relatively steady at around 38-40 percent, while Microsoft, Google, and Alibaba have all steadily gained market share (see figure 7).²⁰⁷ These four leading providers generally account for around 70 percent of the worldwide market for IaaS and PaaS. These leading firms are followed by Salesforce, IBM, Oracle, Tencent, and a large group of companies with minor market shares (see figure 8). The rest of the market is comprised of hosted and managed private cloud services, where IBM is the market leader alongside companies like Rackspace and OVH.²⁰⁸ (See the next section for a competitive analysis of Alibaba Cloud and Tencent Cloud).

Figure 7: Global public cloud services—market share trends (Public IaaS and PaaS).²⁰⁹

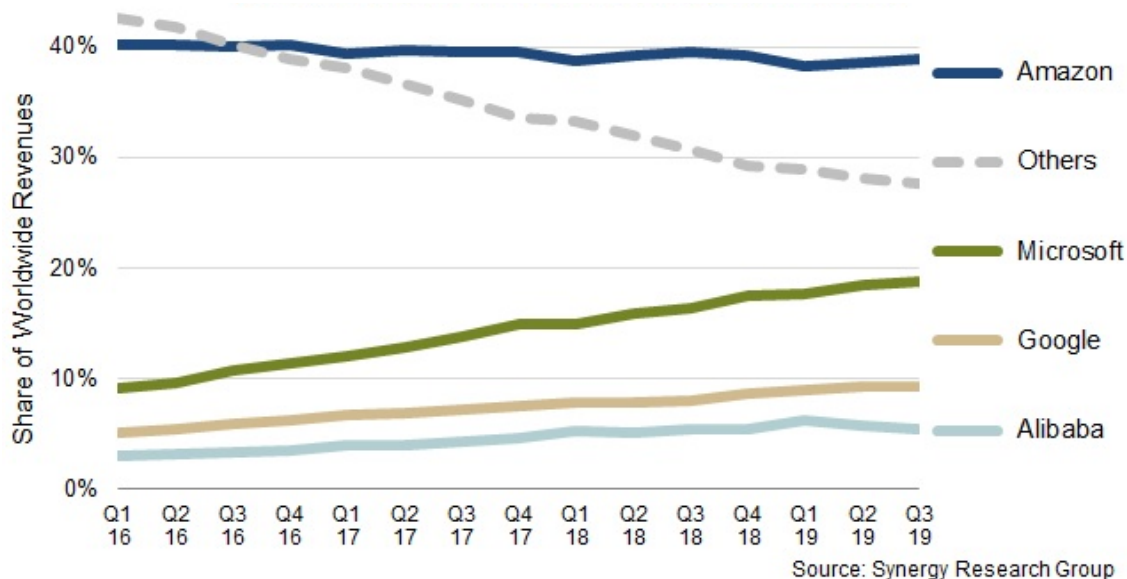
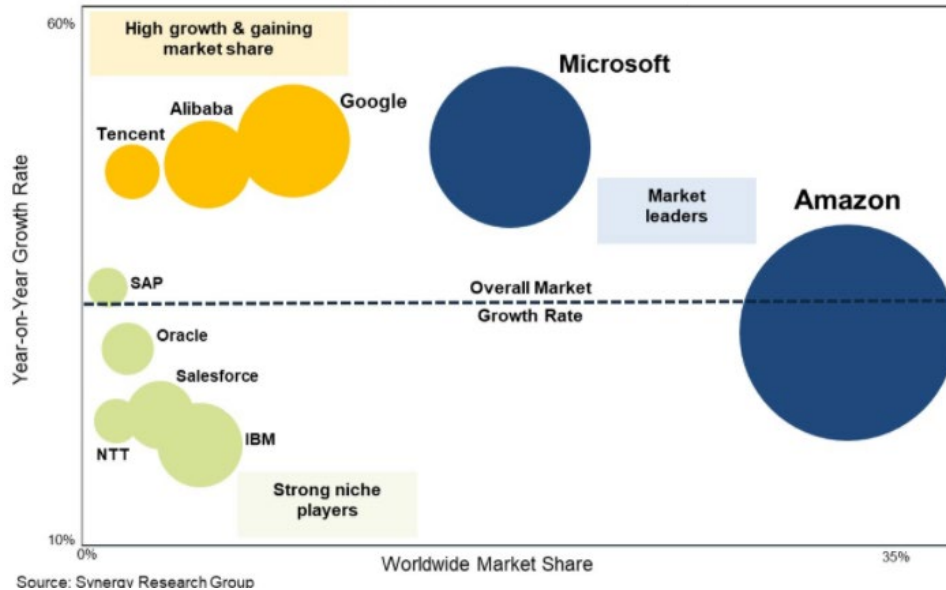


Figure 8: Global cloud provider's competitive positioning (IaaS, PaaS, hosted private cloud, third quarter, 2020)²¹⁰



Censorship Is One of Many Barriers to Trade in Cultural Content in China

China's Communist Party has centralized, strengthened, and expanded the censorship mechanisms it uses in an attempt to protect itself at home and abroad. U.S. content creators face major market access and operational issues that are directly and indirectly related to censorship. The Great Firewall and explicit censorship review process is just the tip of the iceberg in terms of market restrictions U.S. content creators face in China, which are often part of a complicated and often opaque legal, political, and bureaucratic process. Indicative of this, the International Intellectual Property Alliance reported that the ability of U.S. producers to compete in the Chinese marketplace for all audiovisual content was even more drastically curtailed during 2019, with licensing opportunities on all distribution platforms significantly hampered, through opaque regulations, obscure content review processes, and a "soft ban" on new or never released U.S. imports.²¹¹ This has effectively prevented access by U.S. content creators and distributors to one of the largest consumer markets in the world.

The impact of China's censorship and market restrictions on U.S. movie exports has grown more costly over time. Before COVID-19 hit, China was on track to overtake the United States as the world's largest movie market in 2020.²¹² While U.S. movie-ticket sales (pre-COVID) are relatively flat, China's have more than tripled since 2011.²¹³ China has become an important market delivering profits that support Hollywood's blockbuster franchise offerings. Overseas box office revenue is what often turns somewhat new and ambitious films (like *Interstellar* or *Life of Pi*) into blockbusters. The Hollywood releases that break out in China are generally the same ones that succeed globally.²¹⁴ While China cannot be counted upon to bail out big-budget movies that bomb in the United States, U.S. content producers want to (at least) be able to count on potential revenue to justify the budgets that keeps the industry growing.

The impact of China's censorship and market restrictions on U.S. video game makers is similarly clear. China's rapidly expanding video game market already accounts for 33 percent of total global revenue for PC and mobile gaming, but foreign games make up only a small minority of the games approved by censors. In 2019, of the 1,570 games approved, an overwhelming 88 percent (1,385) titles were domestic, a phenomenon not seen in other countries where titles by major U.S. and Japanese developers have a large share of the market. The justifications for blocking games can be as arbitrary and vague as "overly obscene or immoral" content and "cultural content." The lack of a clear criteria and a transparent approval and appeal process gives Chinese officials a free hand to block foreign content not just in their rapidly expanding gaming market, but also in the equally enticing Chinese movie and TV markets.

Discriminatory and Opaque Content Review Processes: Video Games, Movies, and TV Shows

The formal content review process that every video game, movie, and television show undergoes in China is based on vague and non-transparent criteria, which are applied inconsistently, creating an unpredictable and burdensome market access restriction.²¹⁵ Similarly, U.S. firms are prohibited or limited from entering multiple key sectors in China due to opaque, discriminatory, and often arbitrary content regulations and moderations.

Reviewers may require various changes, such as edits in the script, obfuscated translation, and title changes. Sometimes the censors simply don't respond, thus denying access. Furthermore, U.S. content creators must submit full seasons of television shows (rather than as episodes are developed), which also delays distribution, instead of allowing advance registration and rolling approval for content as it's finalized. U.S. films are also often locked out from prime release dates.

In a similar way, the State Administration of Press and Publication's (SAPP) opaque, unpredictable, and restrictive Chinese censorship has affected the approval and distribution of video games. In 2018, China stopped all game license reviews, which severely affected both domestic and foreign firms and game distributors (due to a restructuring of departments and new rules for video game oversight).²¹⁶ While the actual content being censored is often not political (such as intimacy, pornography, and violence), the criteria is often vague and unevenly enforced. For example, "anything that harms public ethics or China's culture and traditions" and "anything that violates China's constitution" are both prohibited in Chinese videogames. Once SAPP started reviewing game licenses again after a nine-month hiatus, it quickly approved nearly 1,000 games, which included 30 foreign games.²¹⁷

Having clear and predictable access to China's video game market is a huge issue as China overtook the United States as the world's largest video-game market in 2016.²¹⁸ As an industry, video games are now worth three times more than movies globally.²¹⁹ China's rapidly expanding video game market already accounts for 33 percent of total global revenue for PC and mobile gaming, but foreign games make up only a small minority of the games approved by the censors.²²⁰

However, the impact of Chinese restrictions are clear. In 2019, of the 1,570 games approved, an overwhelming 88.2 percent (1,385) of titles were domestic, a phenomenon not seen in other

countries where titles by major American and Japanese developers enjoy the majority of the market share.²²¹ The justifications for blocking games can be as arbitrary and vague as “overly obscene or immoral” content, “cultural content,” or even displaying any on-screen text not in simplified Chinese.²²² These rules give Chinese officials a free hand to block foreign access to the rapidly expanding and lucrative gaming market.

This isn't to say that China would be an easy market to compete in. China is a daunting market for foreign firms—93 percent of total spend on Apple's iOS mobile operating system in China is spent on Chinese games, which is more localized than any other country, including Japan or South Korea.²²³ This shows that even without restrictions, U.S. firms would have their work cut out given local preferences, complex distribution systems, and how successful Chinese game developers and platforms have been. But they (again) should have the opportunity to compete on the same terms as local developers.

China Use of Quotas and Revenue Sharing Limits to Restrict U.S. Market Access and Profitability

China uses explicit quotas to limit U.S. market access to their theatrical film sector. Since 1994, China has placed a quota (at that time it was 10) on the number of foreign films that can be shown in Chinese theatres. In 2002, the quota increased to 20. In 2009, the United States won a WTO trade dispute challenging China's restrictions on foreign films (that they only be imported through a few government-designated intermediaries) at the WTO.²²⁴ In 2012, the United States and China negotiated an increase in the quota from 20 to 34.²²⁵ The 2012 agreement also allows foreign movie makers to keep a bigger share of the box office takings, increasing from 13 percent to 25 percent, a rate that is significantly lower than in market-based economies.

This quota mainly affects the major U.S. studios, as a few dozen foreign independent films also get approved for release each year. Both sides agreed to re-negotiate the quota five years after the 2012 revision, but there hasn't been any further progress because the issue succumbed to the broader U.S.-China trade war.²²⁶ The formal quota comes on top of an unofficial policy of manipulating the market to ensure Chinese movies account for a 60 percent box office share.²²⁷ On top of all of this, studios have had problems getting paid for what they are allowed to distribute in China. For example, a Motion Pictures Association-requested audit of the Chinese box office in 2016 showed that Chinese cinemas underreported box office numbers by 9 percent, which, given the revenue sharing arrangement, meant U.S. studios were underpaid by about \$40 million.²²⁸

China's Use of Distribution Restrictions

Quotas and censorship are far from the only issues facing Hollywood. The International Intellectual Property Alliance reported that the ability of U.S. producers to compete in the Chinese marketplace was drastically curtailed during 2019, with licensing opportunities on all distribution platforms significantly hampered, through opaque regulations, obscure content review processes, regulatory delays, and a “soft ban” on new U.S. imports.²²⁹ The former State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) prohibits the cross-border supply of online video services, foreign suppliers from qualifying for a license to distribute content domestically (theatrical distribution is dominated by two state-owned firms), and the

foreign majority ownership of firms engaged in the production and publication of audiovisual content.²³⁰ China also has ‘blackout’ periods when foreign films aren’t allowed to be shown—even if they’ve been approved—such as Chinese New Year.

Investment Restrictions Keep U.S. Streaming Services and their Content Out of China

China uses investment restrictions and regulations to preclude U.S. streaming services from operating in China and from providing services on a cross-border basis. According to Mathew Alderson, a partner at Harris Bricken Attorneys & Consultants in Beijing, “The operation of a VOD [video on demand] service by Disney+, or any other foreign streamer, would require a major change to the negative list [the official set of foreign investment guidelines that precludes cross-border VODs].”²³¹ SAPPRFT and other Chinese regulatory authorities have also taken actions to prevent the cross-border supply of online video services (no doubt, they’d inevitably cite some censorship-related rationale if pressed), which may implicate China’s WTO commitments relating to video distribution.²³²

SAPPRFT also required that all video platforms be state-owned, thus preventing foreign suppliers from qualifying for a license to distribute content. At the same time, several Chinese companies (including Alibaba) appear exempt from some requirements.²³³ Furthermore, China doesn’t allow foreign firms to hold a majority share in entities engaged in the production and publication of audiovisual content.

The measures block leading U.S. streaming services from entering the Chinese market. Disney’s subsidiary Hulu, as well as its own streaming service Disney+, are unavailable in China. Ironically, the Marvel Cinematic Universe franchise (also owned by Disney) includes some of the most successful foreign films to be distributed in China.²³⁴

HBO is able to distribute some content in China, although its streaming service HBO Max is blocked. HBO partners with domestic Chinese media giant Tencent, allowing the company’s content to be streamed through Tencent’s services, but also subjecting HBO to arbitrary censorship. A recent flashpoint came when HBO’s main website was blocked by Chinese officials following a John Oliver segment criticizing Chinese President Xi Jinping.²³⁵

Netflix, the world’s largest streaming service, made a similar arrangement to allow its content to be streamed in China, but the company had to leave the market in 2017. In order to bypass the ban on cross-border VODs, Netflix partnered with iQiyi, a subsidiary of Chinese streaming giant Baidu. This partnership was not renewed in 2017, with iQiyi CEO Gong Yu citing “the verification system and users’ tastes” as the principal reason, further adding that iQiyi has “partnered more with the six traditional major studios, in the U.S. and other regions,” eliminating Netflix from the equation.²³⁶

U.S. Firms in China Show the Difficulty in Navigating China and the Value of Market Access

There are U.S. digital and tech firms that have succeeded in entering and navigating China’s market restrictions, including those directly and indirectly relating to censorship. The cases below highlight how difficult this is and why it’s important that U.S. policy fight for greater, clearer market access given the revenue it provides these firms. Also, it provides potential

datapoints and case studies to use to estimate the cost of censorship for select firms and sectors. These cases (and others like them) show that foreign firms can successfully compete against Chinese competitors even when there are local requirements related to data and content that are significantly different to other major markets. They've found an equilibrium between the laws of their home market and Chinese laws, while still being successful. These experiences provide a blueprint, and perhaps a cautionary lesson, for other foreign tech firms wanting to enter China, as well as policymakers regarding what approach is most effective for both trade and human rights.²³⁷

Airbnb

While Airbnb is not directly involved in censorship related activities and content, it's indirect involvement and compliance and cooperation with local laws and government agencies has contributed to its success in China. It's among the few clear examples where a foreign technology firm can be successful when given the opportunity to compete on fair terms. For Airbnb, China is a critical source of both outbound customers (Chinese tourists travelling overseas) and local hosts for domestic and foreign tourists. As of October 2016, more than 3.5 million Chinese travelers used Airbnb listings around the world.²³⁸ Airbnb faces stiff competition from Chinese rivals, such as Tujia.com and Xiaozhu.com, forced to comply with the same requirements. Airbnb used these outbound Chinese tourists and its global network (which its local competitors don't have) to build up its domestic operations in China. In 2018, Airbnb reported that 91 percent of total nights booked within China were booked by locals.²³⁹ The company has also introduced premium services and expanded into many second and third-tier cities.

Airbnb setup local operations to both abide by local laws and to ensure its services were tailored to the market. In 2016, the company 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).²⁴⁰ In March 2018, Airbnb stated that it would comply in sending customer details to Chinese government authorities, in order to abide by local regulations that require foreigners to register their accommodation with police (hotels have done this for a long time).²⁴¹ Listings and foreign 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 success in China. It has changed its local name (to Aibiyang in Chinese) and doubled its staff (to 500) in Beijing, in part to build a customized version of its platform to better suit local preferences, including the use of WeChat Pay and Alipay.²⁴² Airbnb wants to find a home in the notoriously difficult and cloistered market, and thus far, it has done a pretty good job of doing so.²⁴³

GitHub

GitHub—the largest public code repository in the world that allows developers to collaborate on projects—presents an interesting case as to the potential limits of censorship given how it affects China's broader digital development goals. GitHub (owned by Microsoft) is a U.S.-based global company that provides hosting for software development. It's known as a critical repository for open-source code, providing the vital digital infrastructure on which much of the multibillion-dollar software business depends. While Microsoft does not publish GitHub's financial

information, if the number of developers is a guide, China is its second-most-important market after America, and one of the fastest growing.²⁴⁴

On January 21, 2013, GitHub was blocked in China due to DNS hijacking. The blocking of GitHub gained greater attention in the country after the former head of Google's China operations, Kai-Fu Lee, posted about it on Sina Weibo (China's version of Twitter), where it was re-tweeted over 80,000 times.²⁴⁵ He made the case that “blocking GitHub is unjustifiable, and will only derail the nation's programmers from the world, while bringing about a loss in competitiveness and insight.”²⁴⁶ The block was lifted on January 23, 2013. However, access to GitHub from China can still be slow and unreliable. More recently, Chinese programmers have used GitHub to complain about working conditions in China's tech sector.²⁴⁷ It also remains a popular platform for creating and sharing anti-censorship software tools within China.²⁴⁸ However, in this case, China did not block GitHub. This placed Microsoft, which has extensive operations in China, in a potentially difficult situation, given it has introduced a tailored version of Microsoft Office for Chinese government use. GitHub has already received notices from China's government to remove content. In 2019 it received five notices from China's Ministry of Public Security to take down content related to Falun Gong (a religious group).²⁴⁹

In December 2019, media reports stated that GitHub was moving to setup an office in China.²⁵⁰ In response to a question about China, GitHub CEO Nat Friedman reportedly said that “on net,” the company's approach “is that we want to lean towards more access to GitHub for every developer, even in countries that aren't democratic, even in teams that are doing things that we might disagree with.”²⁵¹ While a GitHub subsidiary in China will make censoring easier for individual projects, such as Great Fire products, it will likely also provide greater regulatory and market certainty for the firm.

LinkedIn

LinkedIn, another Microsoft unit, is among the few prominent foreign tech platforms that are legally allowed in China and that have been successful in the market.²⁵² In 2014, LinkedIn agreed to censor content when it decided to enter China.²⁵³ In 2019, LinkedIn's transparency report showed it received two requests for member data from China's government (this contrasts with 663 for the United States in the same time period) and 17 requests for content removal (of which it took action on 14).²⁵⁴ Part of LinkedIn's success is that it formed a partnership with two influential Chinese venture capital investment funds—who built a good relationship and communication channel with the Chinese government—to create a separate China-based operation.²⁵⁵ The company also focused on the specific characteristics of the Chinese market. It hired local staff who, in part, created a stand-alone app to bring LinkedIn, a service built around email and computers, to China's smartphone-dependent population.²⁵⁶ But even here, it has to adapt to the fact that Chinese users rely more on messaging apps than email, thereby pitching it against WeChat and other larger social networks. LinkedIn isn't trying to compete against the “super apps” like WeChat, but to grow as a career development platform.²⁵⁷ Despite all these challenges, it has found a market with tens of millions of users (reported at 47 million in 2019).²⁵⁸ While its success may be modest, it is indicative of what should be possible for other U.S. firms if given the chance to enter and compete in China.

Steam

An anomaly in China's restrictive approach to video game censorship is Steam (owned by Valve, an American video game developer), which remains accessible (without a VPN) to Chinese users. With Steam, only community features like forums and adult games on the platform are blocked.²⁵⁹ Indicative of the opportunity for foreign firms if they're able to abide by Chinese law and operate in these censored sectors, the Chinese market is incredibly valuable for Steam: it has an estimated 40 million Chinese players and hundreds of game developers. Many local games have been very successful, as well, indicating how local Chinese developers can benefit from working with global platforms like Steam.²⁶⁰ In 2018, Valve announced its intent to partner with a local firm and develop a China-specific Steam platform.²⁶¹

Zoom

Zoom—the video-chat service that operates in more than 80 countries—recently tripped two major landmines that demonstrate how U.S. companies need to establish clear boundaries between operations involving China and other markets, given how censorship requests in the former can quickly spillover to the later. No doubt, Zoom has made mistakes, but it has admitted and addressed many of these in an effort to operate by local laws in China and elsewhere.²⁶² It made these challenging adjustments while expanding from 10 million meetings a day in December 2019 to 200 million meetings a day in March 2020.²⁶³ The company's experience provides useful lessons for other U.S. firms and policymakers.

Zoom is headquartered in San Jose, California and is listed on the NASDAQ. It has over 2,500 employees, about 1,400 of which are in the United States with the remainder overseas, including about 700 at subsidiaries in China (doing R&D work).²⁶⁴ While not every mid-sized U.S. technology company uses China-based R&D, hundreds of multinational firms have R&D centers in China.²⁶⁵ The main Zoom website (zoom.us) and international app appear blocked in China, but there are reportedly several third-party services that allow access in China (e.g., zoom.cn, zoomvip.cn, zoomcloud.cn).²⁶⁶ Zoom's local service and app (<https://zoom.com.cn>) has reportedly been (generally) reliable and popular for users in calls between China and the outside world, including in reaction to COVID-19.²⁶⁷

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).²⁶⁸ Zoom's CEO responded, stating that the firm added server capacity in China as part of its efforts to rapidly scale capacity in response to COVID-19-related demand, during which it failed to fully implement geo-fencing best practices.²⁶⁹ As a result, certain non-China related meetings may have been routed through these servers in China, when they otherwise would not have been. Zoom has removed 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 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).²⁷⁰ Zoom services generally store data in the United States, though it

stores data locally where required or when customers choose to have their data stored outside of the U.S (in their geographic vicinity).²⁷¹

Zoom encountered another major issue when it briefly blocked, and then restored, 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 incident.²⁷² 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, reportedly mid-event.²⁷³ U.S.-based staff reviewed meeting metadata (such as IP addresses) to determine which meetings had China-based participants. Zoom terminated the meetings as (at that time) it did not have the ability to remove specific participants from a meeting or block participants from a certain country from joining a meeting. The company states it did not provide any user information or meeting content to the Chinese government.²⁷⁴

While reactive and incomplete, Zoom's response and approach is the right one in that it wants to manage operations so that they abide by laws in each jurisdiction. This approach is comparable to every other multinational firm in the world—just because a firm is foreign owned does not make it immune from local laws, even if those laws are ones that most Americans would disagree with. 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 significant. Firms are enacting administrative and technical firewalls between China and non-China operations. This is the case for U.S. and other foreign firms in China, but also Chinese firms that operate overseas. For example, Chinese tech firm Bytedance separates its two key services (Douyin inside of China and TikTok outside of China) to minimize cross-border interaction on either platform. It recently implemented restrictions on China-based employees from accessing the code bases for overseas products.²⁷⁵ Zoom rightly committed to “not allow requests from the Chinese government to impact anyone outside of mainland China.”²⁷⁶ It developed technology to remove or block participants based on their country, allowing 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.

Zoom has also committed to release a transparency report that details information related to requests for data, records, or content.²⁷⁷ Naturally, given the need to follow local laws, U.S. technology companies frequently turn over private information requested by home and foreign governments, including those in the United States. Businesses other than Zoom routinely submit to Chinese government censorship demands in China, though there have been few public, high-profile cases involving cross-border issues like this one (besides Yahoo in 2005).²⁷⁸

The onus should be on the United States government and likeminded countries that value and advocate for human rights—not firms like Zoom—in China, whether by engagement, negotiation, or confrontation. As Zoom stated: “It is not in Zoom's power to change the laws of governments opposed to free speech. However, Zoom is committed to modifying its processes to further protect its users from those who wish to stifle their communications.”²⁷⁹ The time has long since

passed, if it ever existed, where an individual U.S. firm could change Chinese government policy through such a public challenge or withdrawal.

For those policymakers and advocates who want Zoom to leave China or cut off services on moral grounds, they also need to recognize that there are clear negative tradeoffs: Zoom is currently a rare channel of relatively low-friction communication through the Great Firewall and the myriad barriers to in-person meetings. The company, and everyone else, should weigh the importance of that connectivity in deciding how to best deal with the underlying challenge that is China's approach to human rights.²⁸⁰

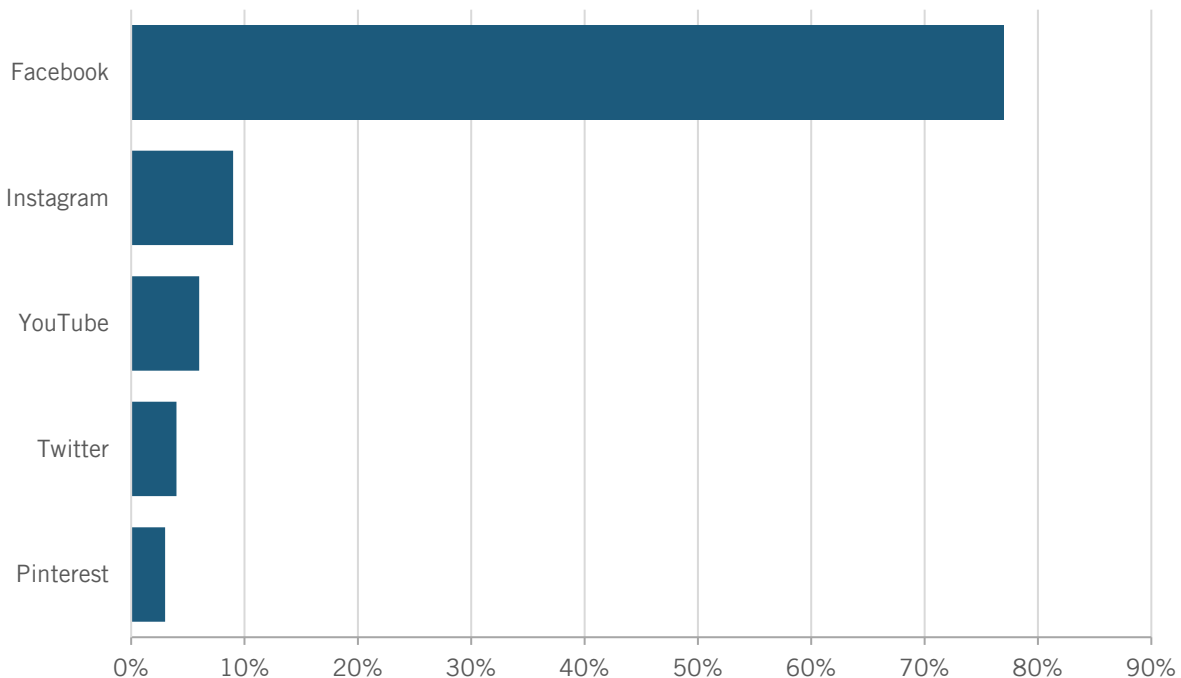
OTHER TROUBLING CASES: INDIA, INDONESIA, NIGERIA, AND TURKEY

China is a world leader, but it's far from alone in using censorship as an NTB. It acts a model for other countries to follow. Below are some other country cases.

India

India has enacted or is considering a broad range of policies related to content moderation that also touch on elements of censorship. U.S. firms are increasingly caught between complying with increasingly strict and arbitrary Indian law and defending free speech in what could eventually be one of their biggest foreign markets, given India is a tech-savvy country with nearly 1.4 billion people (see figure 9).²⁸¹

Figure 9: Leading Social Media Sites in India, May 2021.²⁸²



The Indian constitution includes the right to freedom of speech, but it also bans expression or publication of anything that risks India's security, public order or "decency." India's Information Technology Act (2000) allows the government to issue emergency blocking orders against tech platforms.²⁸³ Indian Prime Minister Narendra Modi—whose Hindu nationalist government is particularly touchy about criticism—went further and introduced new IT rules (the Intermediary Guidelines and Digital Media Ethics Code) that go beyond this, requiring social media platforms to warn users not to post anything that's defamatory, obscene, invasive of someone else's privacy, encouraging of gambling, harmful to a child, or "patently false or misleading." If the government orders it, platforms are required to take down such material. The new law was released in February 2021 without a formal review process and came into force in May 2021.

The rules are very broad and vague and lend themselves to arbitrary, politically-motivated action. For example, in May 2021, police raided Twitter's office in India trying to deliver a notice alerting Twitter to misinformation allegedly tweeted by an opposition politician.²⁸⁴ In addition, in February 2021, the Indian government ordered Twitter to block more than 500 accounts before reversing course when it realized many belonged to journalists, opposition politicians, and activists.²⁸⁵ In a clear move to favor Twitter's local rival "Koo," India's government began shifting its accounts and followers from the former to the latter. An anonymous government official was quoted in the media stating it clearly: "The idea is to create an alternative to Twitter."²⁸⁶

Beyond its use for political purposes and censorship, India's new intermediary liability framework is problematic for several other reasons. The government requires large online intermediaries to designate a chief compliance officer who would be personally liable for any failure to comply with the law. Not only is it unlikely that companies would be willing to find individuals willing to personally take on this type of risk, but, even if they could, this would create a significant amount of pressure on companies to restrict more content than is legally required to avoid any potential legal exposure. The result would be to diminish free speech online.

The law has strict timelines for compliance, such as a 72-hour obligation to respond to a government order, which would impose substantial administrative burdens on businesses. The rules are vague and ambiguous, making compliance difficult. For example, it is not clear exactly how these timelines work, such as whether the clock stops if companies receive an incomplete request for content removal. Moreover, the timeline is unreasonable to obtain data from abroad using existing international legal frameworks, such as mutual legal assistance treaties (MLATs). As a result, this obligation, if enforced, would create a de facto data localization requirement for online intermediaries.

The goal of online intermediary liability laws should be to strike a balance between protecting users, fostering free speech, and allowing online innovation. While many countries are moving to impose more obligations on online intermediaries to protect users, they should be careful not to impose obligations that would undermine these other worthwhile goals.²⁸⁷

India is a large and fast-growing market, so these censorship-related restrictions will have significant short- and long-term impact on U.S. trade. For example, Facebook India's revenues

grew by 43 percent year-on-year to about \$171 million in 2019-20, while its net profit more than doubled to \$18.1 million. During the same time, Google's revenues increased 34.8 percent to about \$726 million, with the company's net profit increasing by about 23.9 percent to \$78.9 million.²⁸⁸ Meanwhile, in 2019, Twitter reported its net profit increased 108 percent to \$780,000, and its revenue climbed to \$7.6 million.²⁸⁹

India and PUBG

The case of Korean firm Krafton, which makes the massively popular "PUBG" video game, is indicative of the scenario faced by U.S. content creators. India is the world's second-largest digital economy, so the implications for all foreign firms and digital content are huge.

In September 2020, India banned PUBG mobile and over 100 other Chinese apps, citing cybersecurity concerns as geopolitical tensions escalated at the two neighboring nations' disputed border. PUBG is published and distributed in India by Chinese firm Tencent. It is by far the most popular title among the banned apps (It had 40 million monthly active users in July 2020 in India). India's IT Ministry banned the apps as they were "prejudicial to sovereignty and integrity of India, defence of India, security of state and public order," indicating the move will help "safeguard the interests of crores (tens of millions) of Indian mobile and internet users. This decision is a targeted move to ensure safety, security, and sovereignty of Indian cyberspace."²⁹⁰

Besides PUBG, search engine Baidu, business collaboration suite WeChat Work, cloud storage service Tencent Weiyun, Rise of Kingdoms game, utility service APUS Launcher, a VPN for TikTok, e-commerce service Mobile Taobao, video hosting service Youku, and news outlet Sina News were all banned. However, the ban was of specific apps, not the firms, so several other Tencent and Alibaba apps remained available in India.

In June, 2021, Krafton was able to make PUBG mobile (rebranded as Battlegrounds Mobile India) available again in India, but it's unclear whether it is considered a new game, the Indian government approved the game, or Krafton had to make any particular changes to address concerns about data privacy and cybersecurity.²⁹¹ Krafton cut ties with Tencent in 2020 due to India's targeting of Chinese firms and apps. Krafton also committed to investing \$100 million in India.²⁹²

The scenario in India holds many important lessons for U.S. firms and policymakers. The U.S. has many firms providing exactly these services that could just as easily be banned with arbitrary and broad restrictions. The threat of firms and specific apps and services being arbitrarily banned during periods of geopolitical tension seems to only grow as more countries realize how much is at stake in the global digital economy, especially if they can use broad, vague concerns about data privacy, cybersecurity, and national security.

Indonesia and Netflix

Netflix's experience in Indonesia is also indicative of the challenge that U.S. firms face in navigating content moderation and censorship concerns that often mix with protectionist interest. Since it entered the country in 2016, Netflix has experienced a challenging regulatory and political landscape in Indonesia, which has progressed from a bumpy entry to being banned and

unbanned by a state-owned telecommunications firm and a million-dollar deal with a government ministry.

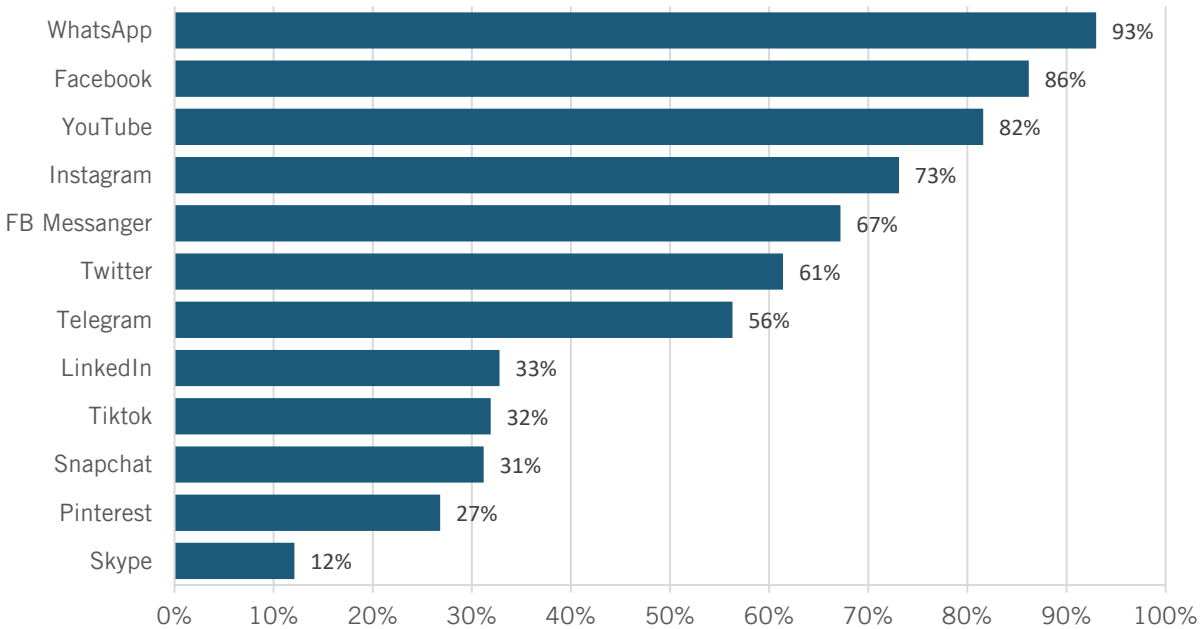
When Netflix became available in Indonesia in January 2016, the streaming service was quickly blocked by state-owned telecommunications company Telkom Group, supposedly because it did not have the right license and due to concerns about unfiltered content, including some displaying violence and adult situations.²⁹³ Indonesia's then-communications and information minister said Telkom's move did not represent the government's stance, calling it a "purely corporate decision," despite Telkom being a state-owned enterprise. However, the minister also stated that the streaming service's presence might affect the country's entertainment industry and other online businesses. Following this, Telkom Indonesia found a foreign company willing to abide by Indonesia's strict entry requirements to launch a (now defunct) video-streaming service, Singapore-based Hooq.²⁹⁴ Then in June 2020, Telkom announced it would allow Netflix on its platforms. It stated that it made this decision after Netflix committed not to air "prohibited content that includes child pornography and terrorism" and agreed to respond to customer complaints within 24 hours.²⁹⁵

Nigeria and Twitter

Nigeria is a major and fast-growing market for U.S. social media services (figure 10). Yet, the Nigerian government's recent decision to ban Twitter shows how suddenly market access can be cut off. In June 2021, Nigeria indefinitely suspended Twitter's service in the country, two days after the social media giant removed a post from President Muhammadu Buhari that threatened to punish regional secessionists. Nigeria's Ministry of Information and Culture announced the ban on Twitter.²⁹⁶ Twitter stated that Buhari's post threatening to punish groups blamed for attacks on government buildings had violated Twitter's "abusive behaviour" policy.²⁹⁷

Social media in Nigeria isn't just about political expression. Many people use it to promote their business, sell their wares, express personal social or religious opinions, and read and share the news, including news often not covered by mainstream media.²⁹⁸ Scores of small and medium-sized businesses across Nigeria are reeling from the indefinite suspension of the social media site. One survey (by NOI Polls) estimates that 39.6 million Nigerians use Twitter, and that 20 percent of them use it for business advertisement while 18 percent use it to look for employment.²⁹⁹

Figure 10: Most used social media platforms in Nigeria (3rd quarter of 2020).³⁰⁰



Turkey and Social Media

Turkey's new social media law (Law No. 7253) requires social media companies with over 1 million Turkish users to open offices, hire representatives, and store Turkish user data on servers locally, or face heavy fines, advertising bans, throttling, or blocking. The law has also streamlined the way courts can order news reports to be blocked or removed from websites without a hearing and increased penalties for non-compliance.³⁰¹ Turkey's courts can issue censorship orders via the Access Providers Association, a member-funded group of ISPs founded in 2014 to streamline the process to enforce censorship orders. The new law specifies that blocking "and/or removal" orders from the association should be fulfilled within 48 hours (or to provide legitimate grounds for challenging such order). The company would be held liable for damages if the content is not removed or blocked within 24 hours.

The law will have a substantial impact on Turkey's economy and society. More than a third of Turks use Twitter and Facebook as their primary source of information.³⁰² Advertising on Turkish social media is expected to fetch companies \$236 million in revenue this year.³⁰³

Indicative of the trade impact, in January 2021, Turkey enacted advertising bans on Twitter, Pinterest, and Periscope over their non-compliance with a controversial new law. Facebook avoided the advertising ban after it announced earlier that it had begun the process of assigning a legal entity in Turkey, joining LinkedIn, YouTube, and TikTok.³⁰⁴ At the same time, Turkey's government is experimenting with its own versions of apps and wants to create "domestic and national" equivalents of Facebook, Google, and other U.S. firms.³⁰⁵

Vietnam and Facebook

Vietnam is a good example of the challenge that U.S. firms face in navigating strict, opaque, and changing regulatory requirements related to censorship that amount to a significant barrier to trade. In April 2020, Facebook's servers in Vietnam were taken offline as the government deemed the company had not complied with censorship demands. Vietnam threatened to do it again later in 2020, as it still believed Facebook was not doing enough to censor more local political content.

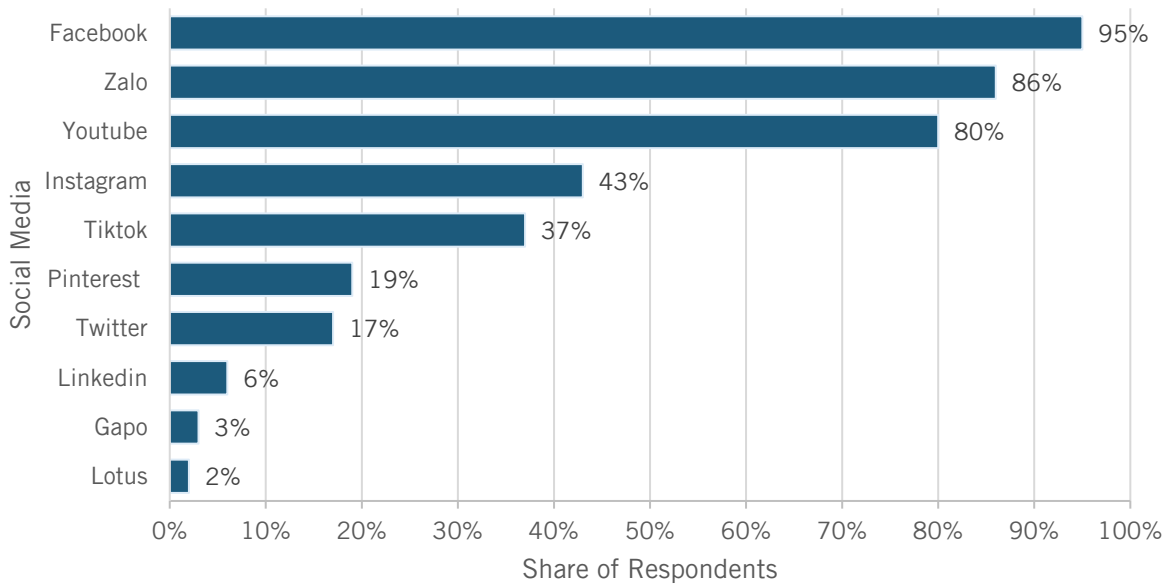
Media reports stated Facebook complied with government requests in April to increase its censorship of "anti-state" posts but was asked to do even more in August. Facebook officials stated they made good faith efforts to comply.³⁰⁶ Indicative of the difficulty U.S. firms face in navigating broad and opaque censorship frameworks, the Vietnamese government stated Facebook should abide by local laws and cease "spreading information that violates traditional Vietnamese customs and infringes upon state interests." Facebook has been subject to a negative media campaign in state-controlled Vietnamese press.

The data shows that Facebook has obviously been trying to meet local censorship requirements. Facebook's transparency report states that from July-December 2019 it restricted access to 77 items in Vietnam in response to reports from the Ministry of Information and Communications Authority of Broadcasting and Electronic Information (ABEI) and the Ministry of Public Security (MPS). This increased to 834 items in January to June 2020, and even further in July-December 2020 when Facebook restricted access to 2,205 items. Facebook consistently states that it removed this content for violating Decree No. 72/2013/ND-CP, including content opposing the Communist Party and the Government of Vietnam. Pursuant to the same law, Facebook also restricted access to 21 pieces of content for regulated goods violations and two pieces of content for COVID-19 related misinformation. Facebook also reviews its decisions and, in select cases, removes restrictions if it was made in error.³⁰⁷

Vietnam is a major market for Facebook, with around 60 million users (see figure 11). There are also an estimated 62 million Google accounts.³⁰⁸ Vietnam's market is worth nearly \$1 billion to Facebook.³⁰⁹ Other data points estimates differ somewhat, but still show the market is significant. For example, market research company ANTS forecast that the turnover of the local advertising market in 2019 would reach \$648 million, including \$275 million made by Facebook, \$174.9 million by Google, and the remaining \$180.9 million shared among the rest of the market.³¹⁰

Vietnam's targeting of Facebook needs to be put in the broader context as it's not just about censorship, but trade. Vietnam has tried to launch home-grown social media networks to replace Facebook and other U.S. tech services (a digital attempt at import substitution). For example, at the September 2019 launch of Lotus (a new social media service) Vietnam's Minister of Information and Communication (MIC), Nguyen Manh Hung, urged Vietnamese companies to create viable domestic alternatives to foreign social media platforms which are more difficult for the government to control.³¹¹ However, despite ongoing government support, the local alternatives are struggling to compete.³¹²

Figure 11: Leading active social media platforms among internet users in Vietnam (1st quarter, 2021).³¹³



CONCLUSION

U.S. policy must recognize the harm caused by these barriers and seek to mitigate their impact on global digital market access. Because China (and other countries) rely on a range of otherwise legitimate public policy goals to provide a justification for their approach to censorship—such as public safety, morals, and national security—the United States and other governments have been reluctant to challenge Chinese practices. This needs to change.

If the United States fails to act against China and other countries' use of censorship as an NTB, it will undermine the U.S.'s leading role in the global digital economy. Failure to act will also further legitimize the concept of "digital sovereignty" where governments intervene directly and extensively in the digital economy to censor online data flows and digital content without limits. The United States must develop and employ a stronger strategy to push back against the trade impact of Chinese censorship as an NTB and to prevent this protectionist model from spreading to more markets.

ENDNOTES

1. Tim Wu, “The World Trade Law of Internet Filtering,” Columbia University Law School, May 3, 2006, <http://dx.doi.org/10.2139/ssrn.882459>.
2. “DS363: China – Measures affecting trading rights and distribution services for certain publications and audiovisual entertainment products,” World Trade Organization website, https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds363_e.htm.
3. Ibid; “Testimony: Commercial Espionage and Barriers to Digital Trade in China,” Matt Schruers, Computer & Communications Industry Association, June 15, 2015, <https://www.uscc.gov/sites/default/files/Schruers%20Testimony.pdf>.
4. Fredrik Erixon, Brian Hindley, and Hosuk Lee-Makiyama, “Protectionism Online: Internet Censorship and International Trade Law” (The European Center for International Political Economy, 2009), <https://ecipe.org/wp-content/uploads/2014/12/protectionism-online-internet-censorship-and-international-trade-law.pdf>.
5. Ibid.
6. Ibid.
7. See e.g. Appellate Body Report, EC – Seal Products, para. 5.169; Columbia – Textiles (AB), para. 5.74. (“As we have noted, in most cases, a panel must then compare the challenged measure and possible alternative measures that achieve the same level of protection while being less trade restrictive. The Appellate Body has explained that an alternative measure may be found not to be ‘reasonably available’ where ‘it is merely theoretical in nature, for instance, where the responding Member is not capable of taking it, or where the measure imposes an undue burden on that Member, such as prohibitive costs or substantial technical difficulties’”). “WTO Analytical Index: Jurisprudence: Article XX,” World Trade Organization, https://www.wto.org/english/res_e/publications_e/ai17_e/gatt1994_art20_jur.pdf.
8. Erixon, Hindley, and Lee-Makiyama, “Protectionism Online: Internet Censorship and International Trade Law.”
9. Asbestos and audiovisuals cases: “WTO Analytical Index: Jurisprudence: Article XX,” World Trade Organization, https://www.wto.org/english/res_e/publications_e/ai17_e/gatt1994_art20_jur.pdf.
10. Erixon, Hindley, and Lee-Makiyama, “Protectionism Online: Internet Censorship and International Trade Law.”
11. Christopher Painter, Daniel Sepulveda, and Uzra Zeya, “Internet Freedom for All,” *DipNote*, U.S. Department of State, August 13, 2013, <http://blogs.state.gov/stories/2013/08/13/internet-freedom-all>; “Say No To Online Censorship,” Electronic Frontier Foundation, accessed July 8, 2014, <https://www.eff.org/pages/say-no-to-online-censorship>; Daniel Castro and Robert Atkinson, “Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy” (ITIF, September 2014), <http://www2.itif.org/2014-crossborder-internet-policy.pdf>.
12. Doug Brake, “Open Internet Oral Argument—Still Need a Bill” (Information Technology and Innovation Foundation, February 1, 2019), <https://itif.org/publications/2019/02/01/open-internet-oral-argument-still-need-bill>.
13. Daniel Castro and Robert Atkinson, “Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy.”

-
14. "Germany: Dozens of Raids Over Online Hate Speech," *Deutsche Welle*, accessed November 21, 2019; <https://www.dw.com/en/germany-dozens-of-raids-over-online-hate-speech/a-49080109>.
 15. Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy."
 16. "Banned: Complete List of 857 Porn Websites Blocked in India," *Deccan Chronicle*, updated January 10, 2016, <http://www.deccanchronicle.com/150803/nation-current-affairs/article/porn-ban-complete-list-857-porn-websites-blocked-india>.
 17. Javier C. Hernández, "Why China Silenced a Clickbait Queen in Its Battle for Information Control," *The New York Times*, March 16, 2019, <https://www.nytimes.com/2019/03/16/world/asia/china-bloggers-internet.html>.
 18. "Lese-Majeste Explained: How Thailand Forbids Insult of Its Royalty," *BBC*, October 6, 2017, <https://www.bbc.com/news/world-asia-29628191>.
 19. The Motion Picture Association – Canada, "Before the Radio-Television and Telecommunications Commission," (March 29, 2018), <https://torrentfreak.com/images/mpa-can.pdf>
 20. Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet,'" (ITIF: August, 2016), https://www2.itif.org/2016-website-blocking.pdf?_ga=2.205709203.149744602.1626532887-1768637206.1619446332
 21. Clifford J. Levy, "Russia Uses Microsoft to Suppress Dissent," *The New York Times*, September 11, 2010, <http://www.nytimes.com/2010/09/12/world/europe/12raids.html>.
 22. Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," *The New York Times*, September 2, 2019, <https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html>
 23. Ina Fried, Sara Fischer, "Facebook says government internet shutdowns are on the rise," *Axios*, May 20, 2021, https://www.axios.com/facebook-government-internet-shutdowns-censorship-a1c1c181-dc01-4450-9945-e1465f5139e8.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioslogin&steam=top
 24. Christopher Giles, "Africa Internet: How do Governments Shut It Down?" *BBC*, March 31, 2019, <https://www.bbc.com/news/world-africa-47734843>.
 25. Jon Henley, "Algeria Blocks Internet to Prevent Students Cheating During Exams," *The Guardian*, June 22, 2018, <https://www.theguardian.com/world/2018/jun/21/algeria-shuts-internet-prevent-cheating-school-exams>.
 26. Yarno Ritzen, "Cameroon Internet Shutdowns Cost Anglophones Millions," *Al Jazeera*, January 26, 2018, <https://www.aljazeera.com/news/2018/01/cameroon-internet-shutdowns-cost-anglophones-millions-180123202824701.html>.
 27. Jan Rydzak, "*Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India*" (working paper, *Global Digital Policy Incubator, Stanford University, February 7, 2019*), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413.
 28. *Rahul Bhatia, "Growing Unease as India Curbs the net to Keep the Peace," LiveMint, September 18, 2017, https://www.livemint.com/Politics/t13L9GsLYgMHzoXZNj7L6J/Growing-unease-as-India-curbs-the-net-to-keep-the-peace.html; Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India."*

-
29. Gopal Kateshiya, "Mobile Internet Services Banned in Rajkot as Patidar Threat Looms," *The Indian Express*, October 18, 2019, <http://indianexpress.com/article/india/india-news-india/mobile-internet-services-banned-in-rajkot-as-patidar-threat-looms/>.
 30. Rae Hodge, "75% of Iraq's Internet Shut Down Amid Mass Protests," *CNet*, October 3, 2019, <https://www.cnet.com/news/75-of-iraqs-internet-shut-down-amid-mass-protests/>.
 31. "Jat Reservation Protest in Haryana: Mobile Internet Services Blocked in Rohtak," *India Today*, February 19, 2016, <https://www.indiatoday.in/india/story/jat-reservation-protest-in-haryana-mobile-internet-services-blocked-in-rohtak-309472-2016-02-18>.
 32. Darrell M. West, "Internet Shutdowns Cost Countries \$2.4 Billion Last Year." (Center for Technology Innovation at Brookings: October 2016), <https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf>
 33. Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India," *Stanford Global Digital Policy Incubator* (February 7, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413
 34. *Ibid.*
 35. "After WhatsApp, Facebook Messenger Gets banned in Saudi Arabia," *Deccan Chronicle*, May 17, 2016, <https://www.deccanchronicle.com/technology/mobiles-and-tabs/170516/after-whatsapp-facebook-messenger-gets-banned-in-saudi-arabia.html>; Jan Rydzak, "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India," *Stanford Global Digital Policy Incubator* (February 7, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413
 36. "Middle East Telecommunications & VOIP Challenges," Istizada, accessed November 1, 2019, <http://istizada.com/blog/telecommunication-voip-challenges-in-the-middle-east/>
 37. Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," *The New York Times*, September 2, 2019, <https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html>; "Policy Brief: Internet Shutdowns," *Internet Society*, November 13, 2017, https://www.internetsociety.org/policybriefs/internet-shutdowns#_edn20.
 38. Patrick Kingsley, "Life in an Internet Shutdown: Crossing Borders for Email and Contraband SIM Cards," *The New York Times*, September 2, 2019, <https://www.nytimes.com/2019/09/02/world/africa/internet-shutdown-economy.html>
 39. *Ibid.*
 40. Saad Guerraoui, "Morocco Banned Skype, Viber, WhatsApp and Facebook Messenger. It Didn't Go Down Well"; "You Can Make Skype Calls in Morocco Again," *Fortune*, November 4, 2019, <https://fortune.com/2016/11/04/morocco-skype-ban/>.
 41. Darrell M. West, "Internet Shutdowns Cost Countries \$2.4 Billion Last Year." (Center for Technology Innovation at Brookings: October 2016), <https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf>.
 42. "The Economic Impact of Disruption to Internet Connectivity" (*Deloitte*, October 2016), <https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html>.
 43. Darrell M. West, "Internet Shutdowns Cost Countries \$2.4 Billion Last Year." (Center for Technology Innovation at Brookings: October 2016), <https://www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf>; Rajat Kathuria et al., "The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India"; "The Economic Impact of Internet Disruptions in Sub-Saharan

-
- Africa*" (Collaboration on International ICT Policy in East and Southern Africa, September 2017), https://cipesa.org/?wpfb_dl=252
44. Ibid.
 45. Darrell M. West, "Internet Shutdowns Cost Countries \$2.4 Billion Last Year." (Center for Technology Innovation at Brookings: October 2016), <https://www.brookings.edu/wp-content/uploads/2016/10/internet-shutdowns-v-3.pdf>.
 46. Rajat Kathuria et al., "The Anatomy of an Internet Blackout: Measuring the Economic Impact of Internet Shutdowns in India," (Indian Council for Research on International Economic Relations, April 2018), http://icrier.org/pdf/Anatomy_of_an_Internet_Blackout.pdf
 47. "A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa" (Collaboration on International ICT Policy in East and Southern Africa, September 2017), https://cipesa.org/?wpfb_dl=252
 48. Paul Mozur, "Apple Removes Apps From China Store That Help Internet Users Evade Censorship," *New York Times*, July 30, 2017, <https://www.nytimes.com/2017/07/29/technology/china-apple-censorship.html>; "@Star_VPN: We just received notice that @Apple removing all the @VPN apps from the @China app store," *Twitter*, July 29, 2017, https://twitter.com/star_vpn/status/891191888547651584; Paul Mozur, "Joining Apple, Amazon's China Cloud Service Bows to Censors," *New York Times*, August 1, 2017, <https://www.nytimes.com/2017/08/01/business/amazon-china-internet-censors-apple.html>.
 49. United States Trade Representative (USTR), 2018 Report to Congress On China's WTO Compliance, <https://ustr.gov/sites/default/files/2018-USTR-Report-to-Congress-on-China's-WTO-Compliance.pdf>
 50. Yuan Yang and Lucy Hornby, "China disrupts global companies' web access as censorship bites," *FT*, January 16, 2018, <https://www.ft.com/content/80e50a6c-fa8a-11e7-9b32-d7d59aace167>; Linda Musthaler, "An SD-WAN service that gets around the Great Firewall of China legally," *Network World*, November 3, 2019, <https://www.networkworld.com/article/3451384/a-vpn-service-that-gets-around-the-great-firewall-of-china-legally.html>; (English translation) "Notice of the Ministry of Industry and Information Technology on Cleaning Up and Regulating the Internet Network Access Service Market," *Ministry of Industry and Information Technology of the People's Republic of China*, January 22, 2017, accessed via the Wayback Machine Internet Archive, <https://web.archive.org/web/20190203073845/http://www.miit.gov.cn/n1146290/n4388791/c5471946/content.html>.
 51. "Notice on Invitation to Membership and Overseas Observers of China Cross-border Data Telecommunications Industry Alliance," China Academy of Information and Communication Technology. http://www.caict.ac.cn/english/news/201809/t20180920_271372.html
 52. Yang and Hornby, "China disrupts global companies' web access as censorship bites," *FT*, January 16, 2018, <https://www.ft.com/content/80e50a6c-fa8a-11e7-9b32-d7d59aace167>
 53. Ibid.
 54. Musthaler, "An SD-WAN service that gets around the Great Firewall of China legally," (Southborough: Linda Network World, Nov 3, 2019), <https://www.proquest.com/docview/2311779485>
 55. "Annex 1 (Word Document) of Notice on Invitation to Membership and Overseas Observers of China Cross-border Data Telecommunications Industry Alliance," China Academy of Information and Communication Technology, <http://www.caict.ac.cn/english/news/201809/P020180920452814498554.doc>
 56. Ibid.
 57. Ibid.

-
58. Ibid.; Musthaler, “An SD-WAN service that gets around the Great Firewall of China legally,” (Southborough: Linda Network World, Nov 3, 2019), <https://www.proquest.com/docview/2311779485>; Teridion, “Teridion Introduces Industry’s First Compliant Cloud-Based Global SD-WAN Service to Mainland China Delivering High-Performance and Cost-Effective Access,” news release, October 24, 2019, <https://www.businesswire.com/news/home/20191024005256/en/Teridion-Introduces-Industry%E2%80%99s-Compliant-Cloud-Based-Global-SD-WAN>.
 59. “Annex 1 (Word Document) of Notice on Invitation to Membership and Overseas Observers of China Cross-border Data Telecommunications Industry Alliance,” China Academy of Information and Communication Technology, <http://www.caict.ac.cn/english/news/201809/P020180920452814498554.doc>
 60. Ibid.
 61. Kuwar Singh, “A Time of How Things Went Downhill For TikTok In India,” Quartz, April 17, 2019; <https://qz.com/india/1598153/heres-why-tiktok-is-getting-banned-in-india/>
 62. Rishi Iyengar, “India’s Two-Week Ban Cost TikTok 15 Million Users,” CNN, May 2, 2019, <https://www.cnn.com/2019/05/02/tech/tiktok-ban-india-users/index.html>
 63. “TikTok: Apple and Google Block Video Sharing App in India,” *BBC*, April 17, 2019, <https://www.bbc.com/news/business-47957684>.
 64. Aria Thaker, “An Indian Court Lifts the Ban on Downloading TikTok,” *Quartz*, April 24, 2019, <https://qz.com/india/1602417/tiktok-download-ban-lifted-by-indias-madras-high-court/>.
 65. Pango provided ITIF data on the number of their daily connected users for the VPN from April 1–April 24, 2019.
 66. Pango provided ITIF data on the number of their daily connected users for the VPN from April 1–April 24, 2019.
 67. Ibid.
 68. TikTok was offering users who downloaded the app a chance to win \$1,400, which may have helped cause the surge in downloads. Aria Thaker, “TikTok is Regaining Its Position in India by Paying Indians to Download the App,” <https://qz.com/india/1610408/downloads-surge-as-tiktok-logo-returns-to-google-apple-in-india/>
 69. Erica Fraser, “Data Localisation and the Balkanisation of the Internet,” *SCRIPTed*, 2016, Vol. 13, p. 359, <https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/>.
 70. Murray Scot Tanner, “Beijing’s New National Intelligence Law: From Defense to Offense,” Lawfare blog post, July 20, 2017, <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense>; Samm Sacks, Qiheng Chen, and Graham Webster, “Five Important Takeaways From China’s Draft Data Security Law,” DigiChina Project blog post, July 9, 2020, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law/>.
 71. Bill Bishop, “One country, one Internet?; TikTok; Gaokao; Floods in China; US FBI head on China,” Sinocism newsletter, July 7, 2020, <https://sinocism.com/p/one-country-one-internet-tiktok-gaokao>.
 72. For example, Russia stated that its personal data localization requirement (enacted in 2015) was to “provide extra protection for Russian citizens both from misuse of their personal data by foreign companies and surveillance of foreign governments;” Alexander Savelyev, “Russia’s new personal data localization regulations: A step forward or a self-imposed sanction?” *Computer Law & Security Review*, 32 (2016) 128–145, <https://doi.org/10.1016/j.clsr.2015.12.003>; “Russia’s security service tells internet firms to hand over user data: The Bell,” *Reuters*, February 12, 2020, <https://www.reuters.com/article/us-russia-internet/russias-security-service-tells-internet-firms-to-hand-over-user-data-the-bell-idUSKBN2060UV>.

-
73. Daniel Castro, "India's Intermediary Liability Law Out of Step With Global Norms," (ITIF: May 11, 2021), <https://itif.org/publications/2021/05/11/indias-intermediary-liability-law-out-step-global-norms>
 74. Article 26.3: "Domestic and foreign enterprises providing services on telecommunication networks or the internet or value-added services in cyberspace in Vietnam with activities of collecting, exploiting, analyzing, and processing personal information data, data on the relationships of service users, or data generated by service users in Vietnam must store such data in Vietnam for the period prescribed by the government. Foreign enterprises mentioned in this clause must open branches or representative offices in Vietnam."
 75. Tilleke & Gibbins, "Update on the Implementation of Vietnam's New Cybersecurity Law and Status of Implementing Decrees," *Lexology*, December 18, 2019, <https://www.lexology.com/library/detail.aspx?g=8833627c-e189-4d60-a472-6ee742cc38fd>
 76. The Decree took effect on 15 April 2018. It updated Decree 72/2013/ND-CP (dated July 15, 2013). <https://www.lexology.com/library/detail.aspx?g=bec72ba6-167d-468e-938c-391199d8579c>
 77. Ibid.
 78. Human Rights Watch (HRW), "Vietnam: Withdraw Problematic Cyber Security Law," (HRW: June 7, 2018), <https://www.hrw.org/news/2018/06/07/vietnam-withdraw-problematic-cyber-security-law>
 79. Facebook Transparency, "Vietnamese Government Requests for User Data," July-December 2020, <https://transparency.facebook.com/government-data-requests/country/VN>
 80. Recently notified rules under Section 37 of Prevention of Electronic Crimes Act 2016 (PECA) hold that online dissemination of any information that intimidates or harms the reputation of Federal or Provincial Government or any person holding public office or attempting to "excite disaffection towards" the government would be seen as threat to 'integrity, security and defense of Pakistan' and would be removed or blocked. The Rules also allow PTA to remove content that is seen to be against decency and morality as defined in the Pakistan Penal Code. <https://www.digitalrightsmonitor.pk/pta-empowered-to-block-online-speech-critical-of-government-gets-power-to-block-entire-online-systems/>
 81. The initial draft was called the Citizen's Protection (Against Online Harms) Rules 2020
 82. Digital Rights Monitor, "Govt begins consultation on online harm rules," June 3, 2020, <https://www.digitalrightsmonitor.pk/govt-begins-consultation-on-online-harm-rules/>
 83. Sadaf Khan et al., "The Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2020," *Media Matters for Democracy*, 2020, <https://www.digitalrightsmonitor.pk/wp-content/uploads/2021/01/Social-Media-Rules-2020-Legal-Analysis.pdf>
 84. Media Matters for Democracy, "analysis of the new social media rules and their potential impact on digital rights and economy in Pakistan," November 23, 2020, <https://mediamatters.pk/media-matters-for-democracy-conducts-an-initial-analysis-of-the-new-social-media-rules-and-their-potential-impact-on-digital-rights-and-economy-in-pakistan/>
 85. Sadaf Khan et al., "The Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2020," *Media Matters for Democracy*, 2020, <https://www.digitalrightsmonitor.pk/wp-content/uploads/2021/01/Social-Media-Rules-2020-Legal-Analysis.pdf>
 86. Chris Rasmussen, "Jobs Supported by Exports 2016: An Update," (Office of Trade and Economic Analysis, August 2, 2017), https://legacy.trade.gov/mas/ian/build/groups/public/@tg_ian/documents/webcontent/tg_ian_005543.pdf
 87. Chris Rasmussen, "Jobs Supported by Exports Methodology," (Department of Commerce, 2017), <https://www.trade.gov/sites/default/files/2020-12/Jobs%20Supported%20by%20Exports%20Methodology.pdf>

-
88. Internet Association, "A Look At American Digital Exports," January 23, 2019, <https://internetassociation.org/publications/a-look-at-american-digital-exports/>
 89. "Estimating the relationship between exports and the labour market in the UK," Department for International Trade, March 10, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/966549/Estimating-the-relationship-between-exports-and-the-labour-market-in-the-UK.pdf.
 90. Motion Picture Association, "The American Motion Picture and Television Industry: Creating Jobs, Trading Around the World," research report, February 25, 2020, <https://www.motionpictures.org/research-docs/the-american-motion-picture-and-television-industry-creating-jobs-trading-around-the-world/>
 91. Erich Schwartzel, "Covid-19 Derails China's Push to Be Biggest Movie Market," *The Wall Street Journal*, July 6, 2020, <https://www.wsj.com/articles/covid-19-derails-chinas-push-to-be-biggest-movie-market-11594035600>
 92. Erich Schwartzel, "Hollywood's New Script: You Can't Make Movies Without China," *The Wall Street Journal*, April 18, 2017, https://www.wsj.com/articles/hollywoods-new-script-you-cant-make-movies-without-china-1492525636?mod=article_inline
 93. Scott Mendelson, "Box Office: 'Wolf Warrior 2's \$600M+ Success Should Terrify Hollywood,'" *Forbes*, August 10, 2017, <https://www.forbes.com/sites/scottmendelson/2017/08/10/as-wolf-warrior-2-tops-600m-what-chinas-box-office-blockbuster-means-to-hollywood/#375fa5b21f61>
 94. Dean Takahashi, "ESA: Games Directly Contributed \$40.9 Billion to US Economy," *Gamesbeat*, December 3, 2020, <https://venturebeat.com/2020/12/03/esa-games-directly-contributed-40-9-billion-to-u-s-economy-and-employed-143045-people-in-2019/>
 95. Entertainment Software Association, "Impact of the Video Game Industry (Interactive Map)," <https://www.theesa.com/video-game-impact-map/>
 96. Entertainment Software Association, "Trade Policy," <https://www.theesa.com/policy/trade-policy/>
 97. Executive Office of the President National Science and Technology Council Advanced Manufacturing National Program Office, "National Network for Manufacturing Innovation Program: Annual Report" (Executive Office of the President, February 2016), <https://www.manufacturing.gov/files/2016/02/2015- NNMI-Annual-Report.pdf>
 98. For a review of studies, see Michelle A. Wein and Stephen J. Ezell, "How to Craft an Innovation Maximizing T-TIP Agreement" (ITIF, October 2013), <http://www2.itif.org/2013-innovation-maximizing-ttip-agreement.pdf>.
 99. Laura DiDio, "The Critical Role of High-Tech R&D in the COVID-19 Era," *Tech News World*, January 12, 2021, <https://www.technewsworld.com/story/86977.html>.
 100. Sundar Pichai, "Investing in America in 2021," Google blog post, March 18, 2021, <https://blog.google/inside-google/company-announcements/investing-america-2021/>.
 101. "Google Economic Impact," *Google*, <https://economicimpact.google.com/>.
 102. DiDio, "The Critical Role of High-Tech R&D in the COVID-19 Era."
 103. "China issues 2020 list of top 500 enterprises," *China Daily*, September 28, 2020, <https://www.chinadaily.com.cn/a/202009/28/WS5f71991ea31024ad0ba7c659.html>.
 104. DiDio, "The Critical Role of High-Tech R&D in the COVID-19 Era."

-
105. "Recent patent trends in cloud computing," IPlytics blog post, November 22, 2018, <https://www.iplytics.com/general/recent-patent-trends-cloud-computing/>.
 106. Louis Columbus, "The Most Innovative Tech Companies Based On Patent Analytics," Blog post, A Passion for Research, December 22, 2019, <https://softwarestrategiesblog.com/2019/12/22/the-most-innovative-tech-companies-based-on-patent-analytics/>.
 107. Matthew Wilson, "Cloud computing patents a major part of another record-breaking year for IBM," IBM, blog post, January 8, 2019, <https://www.ibm.com/blogs/cloud-computing/2019/01/08/cloud-patents-ibm-2018/>.
 108. "Recent patent trends in cloud computing," IPlytics blog post.
 109. Roxanne Heston and Remco Zwetsloot, "Mapping U.S. Multinationals' Global AI R&D Activity" (CSET, December, 2020), <https://cset.georgetown.edu/research/mapping-u-s-multinationals-global-ai-rd-activity/>.
 110. Ibid.
 111. Ibid.
 112. Robert D. Atkinson, "Limiting L-1 Visas: How to Harm America's Business Climate and Kill Jobs," Innovation Files blog post, June 18, 2020, <https://itif.org/publications/2020/06/18/limiting-l-1-visas-how-harm-americas-business-climate-and-kill-jobs>; Adams Nager, "Worried About Foreign H-1B Hirers? Award More Visas!," Innovation Files blog post, March 31, 2016, <https://itif.org/publications/2016/03/31/worried-about-foreign-h-1b-hirers-award-more-visas>.
 113. United States Trade Representative (USTR), *2018 Report to Congress On China's WTO Compliance*.
 114. Ibid.
 115. Victoria Ho, "China accused of rerouting search traffic to Baidu," CNET, October 22, 2007, <https://www.cnet.com/news/china-accused-of-rerouting-search-traffic-to-baidu/>.
 116. Yuan Yang, "China blocks Bing access in curb on last foreign search engine," *FT*, January 24, 2019, <https://www.ft.com/content/714ac466-1f64-11e9-b126-46fc3ad87c65>
 117. Ibid.
 118. Shannon Liao, "Twitch is now blocked in China," *The Verge*, September 20, 2018, <https://www.theverge.com/2018/9/20/17883736/twitch-china-block-app-store>.
 119. Arjun Kharpal, "Amazon is shutting down its China marketplace business. Here's why it has struggled," *CNBC*, April 18, 2019, <https://www.cnbc.com/2019/04/18/amazon-china-marketplace-closing-down-heres-why.html>.
 120. Patrick Frater, "Why China Is Absent From Amazon Prime Video's Global Rollout," *Variety*, December 14, 2016, <https://variety.com/2016/digital/asia/why-china-is-absent-from-amazon-prime-videos-global-rollout-1201941851/>.
 121. "Accessing Box from China," Box Community website, May 18, 2018, <https://community.box.com/t5/Archive-Forum/Accessing-Box-from-China/td-p/56552>.
 122. Matthew Humpries, "China has blocked Dropbox," *Geek.com*, May 11, 2010, <https://www.geek.com/news/china-has-blocked-dropbox-1235291/>.
 123. Catherine Shu, "Dropbox Now Accessible For The First Time In China Since 2010," *TechCrunch*, February 17, 2014, <https://techcrunch.com/2014/02/17/dropbox-now-accessible-for-the-first-time-in-china-since->

-
- 2010; Michael Kan, "China cuts access to Dropbox," *PC World*, June 19, 2014, <https://www.pcworld.com/article/2365540/china-cuts-access-to-dropbox.html>.
124. Hannah Kuchler, "WhatsApp blocked in China ahead of Communist Party Congress in Oct," *FT*, September 25, 2017, <https://www.ft.com/content/685b02c6-4f37-3d69-97f1-38bf7eafeb9d>.
125. George P. Slefo, "Report: China, despite ban, is Facebook's second-largest ad market," *AdAge*, May 15, 2018, <https://adage.com/article/digital/china-facebook-s-largest-market/313524>.
126. <https://www.google.com.hk> is 100% blocked in China, GreatFire.org website, <https://en.greatfire.org/https/www.google.com.hk>.
127. "Google disrupted prior to Tiananmen Anniversary; Mirror sites enable uncensored access to information," GreatFire.org website, June 2, 2014, <https://en.greatfire.org/blog/2014/jun/google-disrupted-prior-tiananmen-anniversary-mirror-sites-enable-uncensored-access>.
128. Kaylene Hong, "Little trouble in big China: Flickr, OneDrive, Line and Kakao Talk suffer accessibility issues," *TheNextWeb*, July 4, 2014, https://thenextweb.com/asia/2014/07/04/little-trouble-in-big-china-flickr-onedrive-line-and-kakao-suffer-downtime/#.tnw_FFQ06QZk.
129. Yuan Yang, "China blocks Bing access in curb on last foreign search engine," *FT*, January 24, 2019, <https://www.ft.com/content/714ac466-1f64-11e9-b126-46fc3ad87c65>.
130. For example: Shih, "China adds Washington Post, Guardian to 'Great Firewall' blacklist," *The Washington Post*, https://www.washingtonpost.com/world/china-adds-washington-post-guardian-to-great-firewall-blacklist/2019/06/08/5ae4fb76-8a56-11e9-b1a8-716c9f3332ce_story.html
131. Paige Leskin, "Here are all the major US tech companies blocked behind China's 'Great Firewall'," *Business Insider*, October 10, 2019, <https://www.businessinsider.com/major-us-tech-companies-blocked-from-operating-in-china-2019-5#duckduckgo-18>.
132. Sherisse Pham, "China adds Pinterest to list of banned sites," *CNN Business*, March 17, 2017, <https://money.cnn.com/2017/03/17/technology/pinterest-banned-china/>.
133. Alice Truong, "Users in China found Reddit blocked over the weekend," *Quartz*, August 13, 2018, <https://qz.com/1354441/china-blocked-reddit-but-access-is-returning-for-some-users/>
134. "@SlackHQ: While we do not block Slack in China from our end, we do know that our content delivery network is very often blocked in China, and so accessing Slack there is somewhat inconsistent," Twitter, February 27, 2018, <https://twitter.com/slackhq/status/968526959213936640?lang=en>.
135. "Slack Technologies filing to the United States Securities and Exchange Commission (SEC)," WEC website, May 31, 2019, <https://www.sec.gov/Archives/edgar/data/1764925/000162828019007428/slacks-1a3.htm>
136. Leskin, "Here are all the major US tech companies blocked behind China's 'Great Firewall'"; Sherisse Pham, "Why Snapchat's owner is hiring in China," *CNN Business*, December 21, 2016, <https://money.cnn.com/2016/12/21/technology/snapchat-china-spectacles-shenzhen-office/>.
137. Paul Mozur, "Twitter Users in China Face Detention and Threats in New Beijing Crackdown," *New York Times*, January 10, 2019, <https://www.nytimes.com/2019/01/10/business/china-twitter-censorship-online.html>.
138. Miguel Helft and David Barboza, "Google Shuts China Site in Dispute Over Censorship," *New York Times*, March 22, 2010, <https://www.nytimes.com/2010/03/23/technology/23google.html>.
139. Matt Sheehan, "How Google took on China—and lost," *Technology Review*, December 19, 2018, <https://www.technologyreview.com/s/612601/how-google-took-on-china-and-lost/>.

-
140. Ibid.
141. Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010, <https://www.wired.com/2010/01/operation-aurora/>.
142. Helft and Barboza, "Google Shuts China Site in Dispute Over Censorship," *The New York Times*, <https://www.nytimes.com/2010/03/23/technology/23google.html>
143. Ibid.
144. Ryan Gallagher, "Google's Secret China Project "Effectively Ended" After Internal Confrontation," *The Intercept*, December 17, 2018, <https://theintercept.com/2018/12/17/google-china-censored-search-engine-2/>.
145. Ibid.
146. Dennis Normile, "Science suffers as China's internet censors plug holes in Great Firewall," *Science*, August 30, 2017, <https://www.sciencemag.org/news/2017/08/science-suffers-china-s-internet-censors-plug-holes-great-firewall>.
147. Nectar Gan, "Is Google another step closer to being unblocked in China?," *South China Morning Post*, March 12, 2017, <https://www.scmp.com/news/china/policies-politics/article/2078173/google-another-step-closer-being-unblocked-china>.
148. Carlos Tejada, "Google, Looking to Tiptoe Back Into China, Announces A.I. Center," *New York Times*, December 13, 2017, <https://www.nytimes.com/2017/12/13/business/google-ai-china.html>.
149. Yunan Zhang and Juro Osawa, "Google's Ad Sales From China Are Booming," *The Information*, February 27, 2019, <https://www.theinformation.com/articles/googles-ad-sales-from-china-are-booming>.
150. Karim Tamsamani, "A strategic partnership with JD.com," Google in Asia Blogpost, June 18, 2018, <https://www.blog.google/topics/google-asia/partnering-jdcom/>.
151. Josh Horwitz, "Chinese e-commerce company JD.Com launches store on Google shopping site," *Reuters*, March 5, 2019, <https://www.reuters.com/article/us-jd-com-google/chinese-e-commerce-company-jd-com-launches-store-on-google-shopping-site-idUSKCN1QM13Y>.
152. Krystal Hu. "How Google is revamping its e-commerce business with JD.com's help," *Yahoo Finance*, August 9, 2019, <https://finance.yahoo.com/news/how-google-is-revamping-its-ecommerce-business-with-j-dcoms-help-183825490.html>.
153. Paul Mozur, "In China, Facebook Tests the Waters With a Stealth App," *New York Times*, August 11, 2017, <https://www.nytimes.com/2017/08/11/technology/facebook-china-moments-colorful-balloons.html>.
154. Mike Isaac, "Facebook Said to Create Censorship Tool to Get Back Into China," *New York Times*, November 22, 2016, <https://www.nytimes.com/2016/11/22/technology/facebook-censorship-tool-china.html>.
155. Mozur, "In China, Facebook Tests the Waters With a Stealth App," *New York Times*, <https://www.nytimes.com/2017/08/11/technology/facebook-china-moments-colorful-balloons.html>
156. Paul Mozur, "China Said to Quickly Withdraw Approval for New Facebook Venture," *New York Times*, July 25, 2018, <https://www.nytimes.com/2018/07/25/business/facebook-china.html>.
157. Paul Mozur and Lin Qiqing, "How Facebook's Tiny China Sales Floor Helps Generate Big Ad Money," *New York Times*, February 7, 2019, <https://www.nytimes.com/2019/02/07/technology/facebook-china-internet.html>.

-
158. Ibid.
159. “Apple’s Chinese troubles,” *The Economist*, February 20, 2020, <https://www.economist.com/business/2020/02/20/apples-chinese-troubles>.
160. 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>.
161. Jay Peters, “Plague Inc. pulled from the App Store in China amid coronavirus outbreak,” *The Verge*, February 27, 2020, <https://www.theverge.com/2020/2/27/21156162/plague-inc-pulled-china-ios-app-store-coronavirus>.
162. Paul Mozur and Jane Perlez, “Apple no longer immune to China’s scrutiny of US tech firms,” *The New York Times*, April 22, 2016, <https://www.cnbc.com/2016/04/22/apple-itunes-movies-ibooks-store-shut-down-in-china.html>.
163. Ibid.
164. Yoni Heisler, “Some of Apple’s most ambitious services still aren’t available in China,” *BGR*, November 7, 2019, <https://bgr.com/2019/11/07/apple-services-china-apple-tv-plus-arcade-not-available/>
165. Ibid; Mark Gurman, “iPhones Are Big in China, But Apple’s Services Play Gets Mired in Censorship,” *Bloomberg*, November 7, 2019, <https://www.bloomberg.com/news/articles/2019-11-07/apple-tv-apple-arcade-other-apple-services-blocked-in-china>.
166. For example, in 2017, China’s regulator issued a circular, entitled “On Cleaning up and Regulating Internet Access Services Market”, which prohibits Chinese telecommunication operators from offering consumers leased lines or virtual private network (VPN) connections reaching overseas data centers, which could restrict a key access mechanism companies use to connect to foreign cloud computing service suppliers and related resources.
167. United States Trade Representative (USTR), *China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974* (Washington, DC: USTR, March 22, 2018), <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>
168. World Trade Organization Council for Trade in Services, “Computer and Related Services Background Note by the Secretariat S/C/W/45” (Geneva: World Trade Organization, July 14, 1998), https://www.wto.org/english/tratop_e/serv_e/w45.doc.
169. Stephen J. Ezell and Robert D. Atkinson, “False Promises: The Yawning Gap between China’s WTO Commitments and Practices” (Information Technology and Innovation Foundation, September 2015), <http://www2.itif.org/2015-false-promises-china.pdf>.
170. For example: Telecommunications Regulations of the People’s Republic of China, art. 7 and the Telecommunications Services Catalogue, attached as the Annex (State Council Order No. 291, issued Sept. 25, 2000 and amended on July 29, 2014 and Feb. 6, 2016), which lists IDC under the VATS operator license.
171. William Mauldin, “U.S. Lawmakers Complain About China’s Cloud Computing Restrictions,” *Wall Street Journal*, March 23, 2017, <https://www.wsj.com/articles/BL-WB-67850>.
172. USTR, *China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*.

-
173. United States Trade Representative, *2013 National Trade Estimate China* (Washington, DC: United States Trade Representative, 2014), <https://ustr.gov/sites/default/files/2013%20NTE%20China%20Final.pdf>; Hogan Lovells, "Third Party Payment Licenses in China - Are They Within the Grasp of Foreign Investors?" (London: Hogan Lovells, June 2014), http://www.hoganlovells.com/files/Uploads/Documents/14.06_Corporate_China_Alert_-_Third_Party_Payment_Licences_in_China_-_Are_They_within_The_Grasp_of_Foreign_Investors_SHALIB01_1093411.pdf.
 174. USTR, *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*.
 175. IBM, "Made in IBM Labs: IBM to Build First Cloud Computing Center in China," news release, February 1, 2008, <http://www-03.ibm.com/press/us/en/pressrelease/23426.wss>; Rebecca Blumenstein, "Microsoft's Partner Strategy in China," *The Wall Street Journal*, June 8, 2016, <http://www.wsj.com/articles/microsofts-partner-strategy-in-china-1465421401>; SAP, "SAP and China Telecom Expand Strategic Partnership to Provide SAP Cloud Portfolio in China," news release, November 20, 2013, <http://news.sap.com/sap-and-china-telecom-expand-strategic-partnership-to-provide-sap-cloud-portfolio-in-china/>; "Azure China Data Centers," Microsoft website, July 20, 2020, <https://docs.microsoft.com/en-us/azure/china/overview-datacenter>.
 176. "Cross-border connectivity and interoperability," Microsoft website, July 20, 2020, <https://docs.microsoft.com/en-us/azure/china/overview-connectivity-and-interoperability>.
 177. Nigel Cory, "Why China Should Be Disqualified From Participating in WTO Negotiations on Digital Trade Rules" (ITIF, May 9, 2019), <https://itif.org/publications/2019/05/09/why-china-should-be-disqualified-participating-wto-negotiations-digital>; Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (ITIF, May 1, 2017), <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>.
 178. Omar Khan, "New Azure region coming to China in 2022," Microsoft blog post, March 4, 2021, <https://azure.microsoft.com/en-us/blog/new-azure-region-coming-to-china-in-2022/>.
 179. "Microsoft and 21Vianet reinforce long-term cooperation on cloud services in China," Microsoft blog post, March 14, 2018, <https://azure.microsoft.com/en-au/blog/microsoft-and-21vianet-reinforce-long-term-cooperation-on-cloud-services-in-china/>.
 180. "Apply to sell in Microsoft national clouds as part of the CSP program," Microsoft website, May 5, 2020, <https://docs.microsoft.com/en-us/partner-center/csp-national-clouds-overview>.
 181. "Amazon to close Chinese domestic marketplace business in major e-commerce setback," *South China Morning Post*, April 18, 2019, <https://www.scmp.com/news/world/united-states-canada/article/3006643/amazon-close-chinese-online-store-major-e-commerce>.
 182. Yang Jie, "Amazon Banned From Using AWS Logo in China Trademark Ruling," *Wall Street Journal*, January 5, 2021, <https://www.wsj.com/articles/amazon-banned-from-using-aws-logo-in-china-trademark-ruling-11609841232>.
 183. Yang Jie and Liza Lin, "Amazon Sells Hardware to Cloud Partner in China," *Wall Street Journal*, November 14, 2017, https://www.wsj.com/articles/amazon-to-sell-its-china-cloud-computing-business-1510628802?mod=article_inline.
 184. Indicative of the restrictive licensing requirements, AWS's website of its partnership with NWCD states that it is a cloud service provider with the Internet Data Center Services license (a B1 category service in figure 1) and the Internet Resource Collaboration Services license. "Ningxia Western Cloud Data Technology Co.Ltd.," AWS website,

-
- <https://partners.amazonaws.com/partners/0010L00001rCaF1QAK/Ningxia%20Western%20Cloud%20Data%20Technology%20Co.Ltd>.
185. “Amazon Web Services (AWS) and Ningxia Western Cloud Data Technology Co. Ltd (NWCD) Announce a Second AWS Region in China, Now Available to Customers,” press release, December 11, 2017, <https://www.businesswire.com/news/home/20171211006337/en/Amazon-Web-Services-AWS-and-Ningxia-Western-Cloud-Data-Technology-Co.-Ltd-NWCD-Announce-a-Second-AWS-Region-in-China-Now-Available-to-Customers>.
 186. Agatha Poon, “AWS China hopes to benefit from China’s ‘dual circulation’ strategy” (industry report, 451 Research, February 26, 2021), https://d1.awsstatic.com/analyst-reports/451-AWS-China-dual-circulation-strategy.pdf?trk=ar_card.
 187. Zhu Shenshen, “Amazon expanding cloud services in China to meet booming demand,” *Shanghai Daily*, march 26, 2021, <https://www.shine.cn/biz/company/2103266544/>.
 188. Poon, “AWS China hopes to benefit from China’s ‘dual circulation’ strategy.”
 189. John Foley, “Oracle, Tencent Reach Agreement To Advance Cloud Services In China,” *Forbes*, November 13, 2015, <https://www.forbes.com/sites/oracle/2015/11/13/oracle-tencent-reach-agreement-to-advance-cloud-services-in-china/?sh=26513f2e138c>.
 190. Cyrus Lee, “Oracle closes China’s R&D centre and axes nearly 1,000 employees: Report,” *ZDNet*, May 8, 2019, <https://www.zdnet.com/article/oracle-said-to-close-chinas-r-d-center-axing-nearly-1000-employees/>.
 191. “Google scraps cloud initiative in China and other ‘sensitive markets’,” *South China Morning Post*, July 9, 2020, <https://www.scmp.com/news/world/united-states-canada/article/3092416/google-scraps-cloud-initiative-china-and-other>.
 192. Yoko Kubota and Lingling Wei, “China Sweetens Its Cloud-Computing Offer in U.S. Trade Talks,” *Wall Street Journal*, April 11, 2019, https://www.wsj.com/articles/china-sweetens-its-cloud-offer-in-u-s-trade-talks-11554976562?mod=article_inline.
 193. “Market size of software-as-a-service (SaaS) cloud market in China from 2013 to 2020,” Statista, <https://www.statista.com/statistics/1029285/china-software-as-a-service-market-size/>.
 194. Celia Chen, “AWS made cloud computing services mainstream, but it still hasn’t cracked China,” *South China Morning Post*, February 3, 2021, <https://sg.news.yahoo.com/aws-made-cloud-computing-services-123818013.html>.
 195. Minghe Hu, “Cloud computing adoption accelerates in China as economy recovers from coronavirus pandemic,” *South China Morning Post*, June 16, 2020, <https://www.scmp.com/tech/big-tech/article/3089225/cloud-computing-adoption-accelerates-china-economy-recovers>.
 196. Ibid.
 197. “IDC: China’s Public Cloud Service Market Tops USD 3.92 Billion,” press release, July 24, 2020, <https://equalocean.com/briefing/20200724230002731>.
 198. “Market size of software-as-a-service (SaaS) cloud market in China from 2013 to 2020,” Statista, <https://www.statista.com/statistics/1029285/china-software-as-a-service-market-size/>.
 199. Cloud computing budget spending divided by overall enterprise software, service, and IT infrastructure spending. Hari Kannan and Christopher Thomas, “Public cloud in China: Big challenges, big upside” (McKinsey & Company report, July 6, 2018), <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/public-cloud-in-china-big-challenges-big-upside>.

-
200. Yang Jie, "Amazon Banned From Using AWS Logo in China Trademark Ruling," *Wall Street Journal*, January 5, 2021, <https://www.wsj.com/articles/amazon-banned-from-using-aws-logo-in-china-trademark-ruling-11609841232>; Karen Chiu, "Huawei looks to cloud services in 2021 as US sanctions strangle smartphone business," *South China Morning Post*, January 3, 2021, <https://www.scmp.com/tech/tech-leaders-and-founders/article/3116243/huawei-looks-cloud-services-2021-us-sanctions>; Celia Chen, "AWS made cloud computing services mainstream, but it still hasn't cracked China," *South China Morning Post*, February 3, 2021, <https://sg.news.yahoo.com/aws-made-cloud-computing-services-123818013.html>.
 201. Minghe Hu, "Cloud computing adoption accelerates in China as economy recovers from coronavirus pandemic," *South China Morning Post*, June 16, 2020, <https://www.scmp.com/tech/big-tech/article/3089225/cloud-computing-adoption-accelerates-china-economy-recovers>.
 202. Jeff Zhang, "Alibaba Cloud Intelligence - Strong Growth Driven by Digital Transformation and Core Technologies" (presentation, 2020 investor day), https://alibabagroup.com/en/ir/presentations/Investor_Day_2020_AlibabaCloud.pdf.
 203. "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020," press release, July 23, 2020, <https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020>.
 204. Ibid.
 205. "Amazon, Microsoft, Google and Alibaba Strengthen their Grip on the Public Cloud Market" (Synergy Research Group Report, October 29, 2019), <https://www.srgresearch.com/articles/amazon-microsoft-google-and-alibaba-strengthen-their-grip-public-cloud-market>.
 206. "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020."
 207. "Amazon, Microsoft, Google and Alibaba Strengthen their Grip on the Public Cloud Market," (Reno, NV: Synergy Research Group, October 29, 2019), <https://www.srgresearch.com/articles/amazon-microsoft-google-and-alibaba-strengthen-their-grip-public-cloud-market>
 208. Ibid.
 209. Ibid.
 210. "Cloud Market Growth Rate Nudges Up as Amazon and Microsoft Solidify Leadership" (Synergy Research Group Report, October 29, 2019), <https://www.srgresearch.com/articles/cloud-market-growth-rate-nudges-amazon-and-microsoft-solidify-leadership>.
 211. "China: 2020 Special 301 Report on Copyright Protection and Enforcement," The International Intellectual Property Alliance, February 6, 2020, <https://www.iipa.org/files/uploads/2020/02/2020SPEC301CHINA.pdf>
 212. "Strong revenue growth continues in China's cinema market," PWC China, June 17, 2019, https://www.pwccn.com/en/press-room/press-releases/pr-170619.html?mod=article_inline.
 213. Erich Schwartzel, "Hollywood's New Script: You Can't Make Movies Without China," *Wall Street Journal*, April 18, 2017, https://www.wsj.com/articles/hollywoods-new-script-you-cant-make-movies-without-china-1492525636?mod=article_inline.
 214. Scott Mendelson, "Box Office: 'Wolf Warrior 2's \$600M+ Success Should Terrify Hollywood,'" *Forbes*, August 10, 2017, <https://www.forbes.com/sites/scottmendelson/2017/08/10/as-wolf-warrior-2-tops-600m-what-chinas-box-office-blockbuster-means-to-hollywood/#17981d101f61>.
 215. United States Trade Representative (USTR), 2018 Report to Congress On China's WTO Compliance.

-
216. Rick Lane, "China freezes all game license approvals," PC Gamer, August 15, 2018, <https://www.pcgamer.com/china-freezes-all-game-license-approvals/>; Shannon Liao, "Apple blames revenue loss on China censoring video games," The Verge, January 29, 2019, <https://www.theverge.com/2019/1/29/18202812/chinese-censorship-hurt-apples-bottom-line>.
 217. "Nearly 1,000 games have received a license since the restart of game approvals in China," Niko Partners, 2019, <https://nikopartners.com/nearly-1000-games-have-received-a-license-since-the-restart-of-game-approvals-in-china/>.
 218. "Europe Meets China – How The Games Industry Is Evolving," Atomico, June 1, 2017, <https://www.atomico.com/europe-meets-china/>.
 219. Ibid.
 220. "Tencent's Silent Pursuit of Global Gaming Domination," Niko Partners, 2021, <https://nikopartners.com/tencents-silent-pursuit-of-global-gaming-domination/>
 221. "Game Regulations in China: Everything you need to know," Niko Partners, 2020, <https://nikopartners.com/game-regulations-in-china-everything-you-need-to-know/>
 222. Ibid.
 223. Ibid.
 224. Keith Bradsher, "W.T.O. Rules Against China's Limits on Imports," *New York Times*, August 12, 2009, <https://www.nytimes.com/2009/08/13/business/global/13trade.html>.
 225. Rogier Creemers, "China increases foreign movie quota, so what does it solve?," China Copyright and Media blog, April 23, 2012, <https://chinacopyrightandmedia.wordpress.com/2012/02/20/china-increases-foreign-movie-quota-but-what-does-that-mean/>.
 226. Pei Li and Michael Martina, "Hollywood's China dreams get tangled in trade talks," Reuters, May 19, 2018, <https://www.reuters.com/article/us-usa-trade-china-movies/hollywoods-china-dreams-get-tangled-in-trade-talks-idUSKCN11KOW0>.
 227. Patrick Frater, "U.S. and China Struggle Over Film Quotas," *Variety*, February 9, 2017, <https://variety.com/2017/biz/asia/u-s-and-china-struggle-over-film-quotas-1201979720/>.
 228. Matthew Dresden, "China Box Office Audit Results Are In – Now What?," China Law Blog, October 10, 2017, <https://www.chinalawblog.com/2017/10/china-box-office-audit-results-are-in-now-what.html>.
 229. INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE (IIPA), "2020 SPECIAL 301 REPORT ON COPYRIGHT PROTECTION AND ENFORCEMENT," 2020, <https://www.iipa.org/files/uploads/2020/02/2020SPEC301CHINA.pdf>
 230. <http://chinahollywood.org/chinese-film-studios>
 231. Patrick Brzeski, "Will China Open the Door to Disney+?," *The Hollywood Reporter*, <https://www.hollywoodreporter.com/business/business-news/will-china-open-door-disney-1203847/>
 232. United States Trade Representative (USTR), 2018 Report to Congress On China's WTO Compliance.
 233. Ibid.
 234. Rebecca Davis, How the Avengers Became Such a Marvel in China, *Variety*, <https://variety.com/2018/tv/news/john-oliver-hbo-china-game-of-thrones-website-1202859077/>

-
235. Lily Kuo, China blocks HBO after John Oliver parody of Xi Jinping, *The Guardian*, <https://www.theguardian.com/world/2018/jun/25/china-blocks-hbo-after-john-oliver-parody-of-xi-jinping>
 236. Arjun Kharpal, "Netflix has a China strategy — but it doesn't involve launching there soon", *CNBC*, <https://www.cnbc.com/2019/05/10/netflix-has-a-china-strategy-it-doesnt-involve-launching-there-soon.html>
 237. Mozur and Goel, "To Reach China, LinkedIn Plays by Local Rules," *New York Times*, <https://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html>
 238. "Supporting our community in China," Airbnb website, <https://blog.airbnb.com/supporting-our-community-in-china/>.
 239. Tyler Sonnemaker, "An Airbnb cofounder explained the strategy behind its success in China, a market where most US companies have failed," *Business Insider*, June 14, 2018, <https://www.businessinsider.com/airbnb-cofounder-china-strategy-success-focused-outbound-travel-2020-2>.
 240. Pei Li and Cate Cadell, "Airbnb to start sharing Chinese host information with government," Airbnb, 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>.
 241. "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>.
 242. Sam Shead, "Airbnb China president: Localization is key if we want to be successful in the country," *CNBC*, November 19, 2019, <https://www.cnbc.com/2019/11/19/airbnb-china-president-localization-abiayang.html>.
 243. Jessi Hempel, "Airbnb Wants to Find a Home in China," *WIRED*, August 21, 2010, <https://www.wired.com/story/airbnb-china-market/>.
 244. "Microsoft's GitHub mulls expansion in China," *The Economist*, December 6, 2019, <https://www.economist.com/business/2019/12/06/microsofts-github-mulls-expansion-in-china>.
 245. Michael Kan, "GitHub unblocked in China after former Google head slams its censorship," *ComputerWorld*, January 23, 2013, <https://www.computerworld.com/article/2493478/github-unblocked-in-china-after-former-google-head-slams-its-censorship.html>.
 246. Ibid.
 247. Yuan Yang, "China tech worker protest against long working hours goes viral," *FT*, April 3, 2019, <https://www.ft.com/content/72754638-55d1-11e9-91f9-b6515a54c5b1>.
 248. Emily Feng, "GitHub Has Become A Haven For China's Censored Internet Users," *NPR*, April 10, 2019, <https://www.npr.org/2019/04/10/709490855/github-has-become-a-haven-for-chinas-censored-internet-users>.
 249. Yuan Yang, "GitHub keen to open subsidiary in China," *FT*, December 9, 2019, <https://www.ft.com/content/4c1f2d1c-1a63-11ea-97df-cc63de1d73f4>.
 250. "Microsoft's GitHub mulls expansion in China," *The Economist*, December 6, 2019, <https://www.economist.com/business/2019/12/06/microsofts-github-mulls-expansion-in-china>
 251. Colin Lecher, "GitHub CEO discussed 'evolving' position on China in private all-hands meeting," *The Verge*, October 10, 2019, <https://www.theverge.com/2019/10/10/20908713/github-ceo-china-transcript-leak-microsoft>.

-
253. Derek Shen, "Introducing LinkedIn's Simplified Chinese Beta Site," LinkedIn Official Blog, February 24, 2014, <https://blog.linkedin.com/2014/02/24/introducing-linkedins-simplified-chinese-beta-site>; Paul Mozur and Vindu Goel, "To Reach China, LinkedIn Plays by Local Rules," New York Times, October 5, 2014, <https://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html>.
254. "Government Requests Report," LinkedIn Transparency website, <https://about.linkedin.com/transparency/government-requests-report>.
255. Paul Mozur and Vindu Goel, "To Reach China, LinkedIn Plays by Local Rules," New York Times, October 5, 2014, <https://www.nytimes.com/2014/10/06/technology/to-reach-china-linkedin-plays-by-local-rules.html>.
256. Mozur and Carolyn Zhang, "Silicon Valley Giants Confront New Walls in China."
257. Zhang Erchi and David Kirton, "LinkedIn's China President Wants to Make Better Use of Career Site's Global Reach," June 24, 2019, <https://www.caixinglobal.com/2019-06-24/linkedins-china-president-wants-to-make-better-use-of-career-sites-global-reach-101430839.html>.
258. Ibid; and Mozur and Carolyn Zhang, "Silicon Valley Giants Confront New Walls in China."
259. Andy Chalk, "Steam Community access has been blocked in China," PC Gamer, December 19, 2017, <https://www.pcgamer.com/steam-community-access-has-been-blocked-in-china/>.
260. "The rise of Chinese games on Steam," *ResetEra*, January 18, 2019, <https://www.resetera.com/threads/the-rise-of-chinese-games-on-steam.94371/>.
261. Chris Tapsell, "Valve talks Steam China, curation and exclusivity," *EuroGamer*, August 21, 2019, <https://www.eurogamer.net/articles/2019-08-21-valve-talks-steam-china-curation-exclusivity>.
262. Bill Marczak and John Scott-Railton, "Move Fast and Roll Your Own Crypto A Quick Look at the Confidentiality of Zoom Meetings," The Citizen Lab, University of Toronto, April 3, 2020, <https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/>; Eric Yuan, "A Message to Our Users," Zoom blog post, April 1, 2020, <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/>.
263. Ibid.
264. "Form 10-K: Zoom Video Communications, Inc. Annual Report to the Securities and Exchange Commission (for the year ending January 31, 2020)," Zoom website, <https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa>.
265. Capucine Cogné, "Is Zoom crazy to count on Chinese R&D?," *TechNode*, April 13, 2020, <https://technode.com/2020/04/13/is-zoom-crazy-to-count-on-chinese-rd/>.
266. "[Translation] Zoom suspended in China," *Sohu*, September 9, 2019, https://www.sohu.com/a/339796981_115035
267. Karen Chu, "Why are people in China using Zoom?," *South China Morning Post*, June 18, 2020, <https://www.scmp.com/abacus/tech/article/3089667/why-are-people-china-using-zoom>; Emma Lee, "China's Zoom users switch to local version after blockage," *TechNode*, September 19, 2019, <https://technode.com/2019/09/19/chinas-zoom-users-switch-to-local-version-after-blockage/>.
268. 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/>.
269. Eric Yuan, "Response to Research From University of Toronto's Citizen Lab," Zoom blog post, April 3, 2020, <https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/>.
270. 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://www.theguardian.com/technology/2020/jun/17/zoom-encryption-free-calls;); <https://blog.zoom.us/end-to-end-encryption-update/>.
271. [Archived] "Zoom: Privacy Policy," March 29, 2020, <http://archive.fo/5gKKh#selection-2299.271-2299.426>.
272. 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>.
273. "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/>.
274. Ibid.
275. Chen Du, "Exclusive: ByteDance Cuts Domestic Engineers' Data Access to TikTok, Other Overseas Products," PingWest, June 7, 2020, <https://en.pingwest.com/a/6875>.
276. "Improving Our Policies as We Continue to Enable Global Collaboration," Zoom blog.
277. Zoom's privacy policy notes that: "In certain limited circumstances, courts, law enforcement agencies, regulatory agencies, or security authorities in those other countries may be entitled to access your personal data."
278. "Chinese journalist Shi Tao, jailed for eight years after Yahoo gave up his identity, gets early release," Reuters, September 9, 2013, <https://www.scmp.com/news/china/article/1306818/chinese-journalist-shi-tao-jailed-eight-years-after-yahoo-gave-his>.
279. Gerry Shih, "Zoom censors video talks on Hong Kong and Tiananmen, drawing criticism," Washington Post, June 11, 2020, https://www.washingtonpost.com/world/asia_pacific/zoom-censors-video-talks-on-hong-kong-and-tiananmen-drawing-criticism/2020/06/11/0197dc94-ab90-11ea-a43b-be9f6494a87d_story.html.
280. As raised by Graham Webster in: "China's Zoom Bomb: A ChinaFile Conversation," China File, June 16, 2020, <https://www.chinafile.com/conversation/chinas-zoom-bomb>.
281. Lauren Frayer and Shannon Bond, "Twitter In Standoff With India's Government Over Free Speech And Local Law," *NPR*, February 18, 2021, <https://www.npr.org/2021/02/17/968641246/twitter-in-standoff-with-indias-government-over-free-speech-and-local-law>; <https://www.npr.org/2021/02/17/968641246/twitter-in-standoff-with-indias-government-over-free-speech-and-local-law>
282. Facebook had the highest traffic at around 78 percent among social media platforms across India in May 2021. The social media company has consistently secured a high page traffic share in India since March 2019 when it was around 90 percent. Instagram and YouTube followed far behind, with traffic shares of around five percent and 3.2 percent respectively during that time period. "Leading social media sites across India in May 2021," Statista, <https://www.statista.com/statistics/1115648/india-leading-social-media-sites-by-page-traffic/>
283. India Central Government Act Section 69A in The Information Technology Act, (2000), https://indiankanoon.org/doc/10190353/?_cf_chl_jschl_tk__=83828603e1886977fc4212a3fcb8ae9ebe08e5d-1613475069-0-AZm-x5V5LniKam8j5MYqbF93_yIKHvOoEy_fkvoaaMG6_HsJ-

-
- QEI91484aCUAo8rqS7WSes7ISxCqohnV33on9eHqjxkqM5TGmepGOaqEEk6P1zqXg6ckilmF3K7df0soUtqwO
qPChVNzLpbNtN_8vcQpj3AIPxNxaZMfZ7DzAsxABOSa2RNtyzB8VSwj2KdI8_gEoVUI9WcGkdFESRZmQucxnjs
9_WfnBWvErKYu6mYHYO3uCi39EG5MooCEsgInJ07pQv2qVtYs8RSi2eJs3NGKScm4nroY_WmJN8z7GhBGzr
7huvVINJqpUkbJaBWysqZfcJjSQY_MnMnijrkdOm4C5ikiQoTACOs4dqvkEEbimfL2cUkKLezRGFOJby1w
284. Lauren Frayer and Shannon Bond, "India And Tech Companies Clash Over Censorship, Privacy And 'Digital Colonialism,'" *NPR*, June 10, 2021, <https://www.npr.org/2021/06/10/1004387255/india-and-tech-companies-clash-over-censorship-privacy-and-digital-colonialism>
285. Frayer and Bond, "Twitter In Standoff With India's Government Over Free Speech And Local Law."
286. Sankalp Phartiyal and Aditya Kalra, "In spats with Twitter, India's government begins messaging shift to rival Koo," *Reuters*, July 28, 2021, <https://www.reuters.com/world/india/spats-with-twitter-indias-government-begins-messaging-shift-rival-koo-2021-07-28/>
287. Daniel Castro, "India's Intermediary Liability Law Out of Step With Global Norms," (ITIF: May 11, 2021), <https://itif.org/publications/2021/05/11/indias-intermediary-liability-law-out-step-global-norms>
288. "FACEBOOK INDIA FY 2020 REVENUE UP 43 PERCENT AT RS 1,277 CRORE, NET PROFIT DOUBLES TO RS 135.7 CRORE," *Tech2*, December 11, 2020, <https://www.firstpost.com/tech/news-analysis/facebook-india-fy-2020-revenue-up-43-percent-at-rs-1277-crore-net-profit-doubles-to-rs-135-7-crore-9100731.html>
289. Sagar Malviya, "Twitter India profit doubles in FY19," *The Economic Times*, October 21, 2019, <https://economictimes.indiatimes.com/tech/internet/twitter-india-profit-doubles-in-fy19/articleshow/71830378.cms?from=mdr>
290. Manish Singh, "India bans PUBG Mobile, and over 100 other Chinese apps," *TechCrunch*, September 2, 2020, <https://techcrunch.com/2020/09/02/india-bans-pubg-and-over-100-additional-chinese-apps/>
291. Manish Singh, "Hit game PUBG Mobile returns to India with scores of questions," *TechCrunch*, June 17, 2021, <https://techcrunch.com/2021/06/17/battlegrounds-mobile-pubg-returns-to-india/>
292. Manish Singh, "PUBG announces India return plan with new game and \$100 million investment," *TechCrunch*, November 12, 2020, <https://techcrunch.com/2020/11/12/pubg-mobile-announces-return-to-india-new-game-100-million-investment/>
293. "Indonesia Gives Netflix One Month to Get Permit, Office," *Jakarta Globe*, January 13, 2016, <http://jakartaglobe.id/technology-features/indonesia-gives-netflix-one-month-get-permit-office/>; Resty Woro Yuniar, "Netflix Blocked by Indonesia's Top Telecom Provider," *The Wall Street Journal*, January 27, 2016, <http://www.wsj.com/articles/netflix-blocked-by-indonesias-top-telecom-provider-1453896220>.
294. "Telkom to Bring Netflix Rival to Indonesia," *The Jakarta Post*, March 28, 2016, <http://www.thejakartapost.com/news/2016/03/28/telkom-bring-netflix-rival-indonesia.html>.
295. "How Netflix went from foe to friend in Indonesia," *Business Inquirer*, August 9, 2020, <https://business.inquirer.net/304939/how-netflix-went-from-foe-to-friend-in-indonesia>
296. @FMICNigeria, "PRESS RELEASE: FG Suspends @Twitter Operations in Nigeria," Twitter.com, <https://twitter.com/FMICNigeria/status/1400843062641717249>
297. "Nigeria says it suspends Twitter days after president's post removed," *Reuters*, June 5, 2021, https://www.reuters.com/technology/nigeria-indefinitely-suspends-twitter-operations-information-minister-2021-06-04/?taid=60ba657ab4cefa000172dc37&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter

-
298. Kólá Túbòsún, "Nigeria's Twitter Ban Is Another Sign Dictatorship Is Back," *FP*, June 7, 2021, <https://foreignpolicy.com/2021/06/07/nigeria-twitter-ban-dictatorship/>.
 299. "Nigeria's Twitter ban leaves some businesses in the lurch," *Reuters*, June 14, 2021, <https://www.reuters.com/technology/nigerias-twitter-ban-leaves-some-businesses-lurch-2021-06-14/>
 300. Simona Varrella, "Leading social media platforms in Nigeria 2020," *Statista*, February 2021, <https://www.statista.com/statistics/1176101/leading-social-media-platforms-nigeria/>.
 301. Özgür Öğret, "Turkish social media law consolidates news censorship under 'right to be forgotten,'" (Committee to Protect Journalists, March 18, 2021), <https://cpj.org/2021/03/turkish-social-media-news-censorship/>.
 302. Turkuazlab, "Dimensions of Polarization in Turkey 2020 Survey," https://www.turkuazlab.org/wp-content/uploads/2020/12/Survey_Key_Findings.pdf
 303. Social Media Advertising (Turkey), *Statista*, <https://www.statista.com/outlook/dmo/digital-advertising/social-media-advertising/turkey>.
 304. Suzan Fraser, "Turkey slaps advertising ban on Twitter, Pinterest," *AP*, January 19, 2021, <https://apnews.com/article/turkey-media-social-media-censorship-laws-4e5da08d55ceb2805456e0a5bf89b415>
 305. Sinan Tartanoglu, "[translated] Presidency aims to develop domestic and national Google, Apple and Facebook," *Ankara Gazette*, February 28, 2021, <https://ankaragazetecisi.com/2021/02/28/cumhurbaskanligi-yerli-ve-milli-google-apple-ve-facebook-gelistirmeyi-hedefliyor/>.
 306. James Pearson, "Vietnam threatens to shut down Facebook over censorship requests," *Rueters*, November 19, 2020, <https://www.reuters.com/article/vietnam-facebook-shutdown/exclusive-vietnam-threatens-to-shut-down-facebook-over-censorship-requests-source-idUSKBN28007K>
 307. "Facebook content restricted on local law (Vietnam)," Facebook Transparency, accessed August 3, 2021, <https://transparency.fb.com/data/content-restrictions/country/VN>
 308. "Vietnam's social media crowd swells with new entrant to take on Facebook, Google," *Reuters*, September 17, 2019, <https://www.reuters.com/article/us-vietnam-cybersecurity/vietnams-social-media-crowd-swells-with-new-entrant-to-take-on-facebook-google-idUSKBN1W20NH>.
 309. James Pearson, "Vietnam threatens to shut down Facebook over censorship requests."
 310. Van Anh, "Local platform's work cut out to reinvent social networking," *Vietnam Investment Review*, January 26, 2020, <https://vir.com.vn/local-platforms-work-cut-out-to-reinvent-social-networking-73353.html>
 311. "Vietnam's social media crowd swells with new entrant to take on Facebook, Google," Reuters.
 312. Van Anh, "Local platform's work cut out to reinvent social networking."
 313. According to a survey among internet users conducted in Vietnam by Decision Lab in the first quarter of 2021, 95 percent of respondents stated that they used Facebook, followed by Zalo and YouTube. While Facebook and YouTube are known globally, Zalo is Vietnam's premier chatting platform that was launched in 2012. <https://www.statista.com/statistics/941843/vietnam-leading-social-media-platforms/>.