PUBLISHED JANUARY 2021



Exporting Censorship and Internet Sovereignty

How China Uses its Economic Power, American Companies, and its Own Technology Companies to Implement its Vision for a Controlled Internet Globally

Jonathon Hauenschild, Policy Advisor

Executive Summary

The West and China have two different, competing views of the internet based on the values the two government systems promote. The West, led by America, largely values democratic rule, freedom of speech, freedom of association, religious liberty, and the ability to communicate with others free from unreasonable, unwarranted government surveillance. Because of its communist government, China eschews those freedoms, placing the ethereal terms "state security" and "social stability" as some of its principle values.

The Chinese government promotes a theory of "internet sovereignty," meaning that each nation should have control of the information available to, and flowing through, the internet. That is, the internet should stop at each country's borders before proceeding.

Internet sovereignty is antithetical both to the nature of the internet and values Americans hold dear. The internet was not designed with national borders in mind, but as a way to maximize communications between individuals.

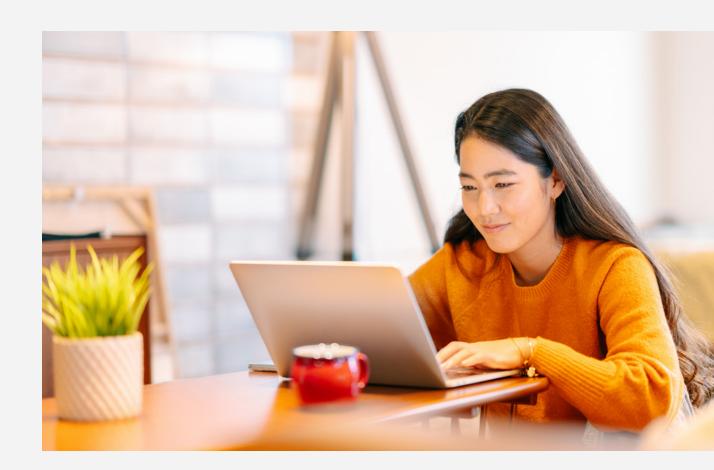
To implement its vision of internet sovereignty, China built—with the help of American companies—a Great Firewall and Golden Shield. The Great Firewall helps China control what websites its citizens can access, while the Golden Shield helps the country censor content internally, controlling dissidents and journalists critical of the Communist regime, along with any other content the Party deems inappropriate.

Just as China used American companies to help build the Great Firewall, it is using them to export its vision of internet sovereignty, along with other values, to the United States. In return for access to the potentially lucrative Chinese market, United States technology companies must agree to aid the government's censorship and share intellectual property with a local company, which is ultimately controlled by the Communist party. Increasingly, China is pressuring American companies to censor content created by Americans if those companies want continued access to its market.

China is not content to rely on American companies to export its concept of internet sovereignty and cultural values. As Chinese technology companies and social media platforms grow in popularity, they help by censoring content, providing access to telecommunications systems, and more.

2





Introduction

The internet defies national borders. It is not designed to be segmented, with one nation enjoying a different experience than another. Despite this, nation-states have devised ways to control their citizens' access to information. Nations like Saudi Arabia and China believe the internet's wealth of information is dangerous and that people cannot be trusted either with unfettered access to the internet or the ability to post information without censorship.

Of the nations that restrict their citizen's access to the internet, only one— China—actively seeks to export its values to other countries. The internet values China espouses are antithetical both to the nature of the internet and to the principles Western nations hold dear. China has the economic might and global technological reach to influence foreign nations and private companies, compelling them to adopt its values in exchange for access to its lucrative economic market. The Chinese communist government controls its citizens' online behavior in two ways: by limiting what information from the outside world is available and by censoring content posted within its borders. At least one author refers to this as the Great Firewall and Golden Shield.¹ Restricting citizen's access to information otherwise broadly available means that there are functionally two different internets: the internet as originally designed and implemented and that which is behind the Great Firewall of China.

With two different internets—one unlimited and the other limited—conflict between the two is inevitable. Each will fight for dominance, seeking to set both technological and ethical standards for other countries. The vision that wins will be able to control the internet's future, including the free circulation of information.

The unlimited internet has strategic advantages. It was first. It grows exponentially day-by-day, year-by-year. The limited, or censored, internet must react to the free internet. Above all, the free internet enjoys a broad economic, market-based support system. Many of the world's largest companies, headquartered in the United States, developed because of the unlimited internet and they have vested interests in keeping the online ecosystem as broadly accessible as possible.

The dominance of American technology companies must not be presumed, though. The West's, and specifically the United States', innovation and technological leadership is at risk. Adopting something of a neo-Marxist bent, the West has decided that large innovators are essentially evil, having abandoned some ethereal moral obligation to protect the public against propaganda, disinformation, and radicalization. Often, claims that technology companies have abandoned moral obligations go together with allegations that technology companies are profiting obscenely by gathering and processing information about consumers. Without really identifying concrete harms, the proposed solutions attempt to regulate the free flow of information in the form of so-called privacy legislation, antitrust, and other data governance restrictions.

These proposals both threaten the West's internet technology dominance. They threaten to balkanize the internet, with people in the U.S. enjoying a vastly different experience than those in Europe. And state efforts in the U.S.—during the 2018 legislative session, legislators in nearly 30 states introduced some form of

4

¹ See generally, James Griffiths, The Great Firewall of China, London: Zed Books, 2019. As discussed later, the Great Firewall controls international internet traffic into China. The Golden Shield is a model of censorship focusing primarily on intra-country services.



privacy proposal—threaten domestic balkanization. Legislation and restrictions represent significant hurdles companies and innovators must overcome before offering services. The legislation and restrictions come with huge compliance costs, with Forbes estimating that U.S.-based Fortune 500 companies spent nearly \$8 billion complying with General Data Protection Regulation (GDPR) and the California Attorney General estimates that California businesses will spend over \$55 billion initially complying with California Consumer Privacy Act (CCPA).

Even worse for the state of United States leadership in innovation is that these privacy proposals represent an open door for China. Over the past decade, Chinese technology companies have grown immensely. A decade ago, companies like Huawei, Tencent, Baidu, and Alibaba, were virtually unknown entities. Today, a number of those companies are some of the most successful, global technology stocks. There is a danger that these companies born in the world of strict government control and censorship will be unable either to break the ties that bind them to the Communist government or become vessels willingly exporting the Chinese vision of the internet to the West. While those companies face restrictions unfamiliar to the West, they remain relatively unaffected by the West's proposals to regulate the technology sector.



The Internet's Nature, American Values, and a Great Firewall

"The internet is borderless. Data moves wherever pathways exist, without regard to legal boundaries or rules."² Those who designed the internet thought more about moving data than jurisdictional boundaries. Because of this, the internet works by breaking data into different packages, for lack of a better term. It sends these packages on their way, with a specific destination in mind, but without regard for the route they take. Even a simple email may be broken into hundreds, or thousands, of different packages and sent across the country or globe before it reaches its ultimate destination, even if that destination is down the street.³

The internet reflects fundamentally American values, such as freedom of speech, freedom of expression, freedom of association, freedom of religion, and broadly an ability to communicate with anyone else free of government surveillance. Many of these values are expressed in the Constitution, particularly the First Amendment.

6

² Michael Chertoff, *Exploding Data*, New York, NY: Grove Press, 2016, p. 28.

³ See, e.g., ibid at p. 30 (explaining the internet layer of network communications—the internet layer itself is the third of five network communications layers, but the most relevant for the current discussion).

The Constitution limits the government. The First Amendment prohibits Congress from making any law that restricts the freedom of speech, of the press, respecting an establishment of religion, or prohibiting the free exercise thereof, and more. Similarly, the Fourth Amendment provides that "the right of the people to be secure in the persons, houses, papers and effects against unreasonable searches and seizures shall not be violated and no warrant shall issue but upon probable cause…" Applied to the internet, the Fourth Amendment means that government actors, in the form of law enforcement agencies, must secure warrants before intercepting emails,⁴ wiretapping phone calls (including mobile phone), tracking cell phone location data,⁵ accessing information stored on cell phones,⁶ and so on.

The pioneers of cyberspace went beyond the concepts expressed in the Constitution though, declaring the then nascent technology to have "no elected government, nor... likely to have one." Continuing in the Declaration of the Independence of Cyberspace, John Perry Barlow proclaimed "the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear."⁷

Over time, countries such as China have found ways to impose their tyrannies on cyberspace. The Communist government of China does not place the same value on speech, expression, and association that the West does, instead greatly fearing the "free circulation of information."⁸ The dangers to an authoritarian regime represented by an unencumbered internet necessitates both tight control and contortions of logic to justify that control. Thus, in Orwellian fashion,⁹ the Chinese government claims that "freedom and order are twin sisters and they must live together."¹⁰

As in the United States, the internet was first introduced in China as a way for academics to communicate with each other and the outside world. As more Chinese citizens gained access, they started sharing information previously suppressed by government censors—with one major source of censored news being what today would be referred to as spam. Between the dissident spam

⁴ The Stored Communications Act, though, allows law enforcement to access emails stored more than 6 months without a warrant. 18 U.S.C. § 2703(a).

⁵ See, e.g., Carpenter v. United States, 585 U.S. ____, 138 S.Ct. 2206 (2018).

⁶ Riley v. California, 573 U.S. ____, 134 S.Ct. 2473 (2014).

⁷ John Perry Barlow, 'A declaration of the independence of cyberspace,' Electronic Frontier Foundation, February 8, 1996, https://www. eff.org/cyberspace-independence.

⁸ Brian Crozier, *The Rise and Fall of the Soviet Empire*, Rocklin, CA: 1999, 491.

^{9 &}quot;War is peace. Freedom is slavery. Ignorance is strength." George Orwell, 1984, 4.

¹⁰ Juxtapose efforts by the United States to promote an open internet to Chinese officials' statements criticizing those efforts. China views American advocacy for global online free speech as "naked political scheming." Segal, Adam, *The Hacked World Order*, New York, NY: PublicAffairs, 2016, 31.





messages and the growing popularity of Google,¹¹ the government realized it was necessary to control the flow of online information.¹²

In place of a free and open internet, China talks about the need for "protecting national sovereignty in cyberspace."¹³ Internet sovereignty, as a policy, means that each country should have the right to control content and access to its domestic markets. Behind the policy is the theory that "the web is not a unique technology, transcending borders and international controls, but is like everything else, and should be regulated accordingly."¹⁴

Beyond just controlling access, China places a high value on protecting national security. Chinese conceptions of national security, though, might be foreign to someone from the West. Chinese law broadly defines national security and encompasses the "economy, financial system, indigenous technology innovation, and *social stability*."¹⁵ Within the communist system, social stability includes maintaining a tight control on dissent, preventing criticism of the government, the rise of non-communist political parties, religious movements not approved by the state, and so on.

China's vision of internet sovereignty requires a censored version of the internet for its citizens. Initially, this sounds difficult because of the nature of the internet—a borderless network that enables mass communication—but with the help of American companies, China's desire for a censored internet experience, became a reality.

¹¹ As of 2002, Google "controlled about 25 percent of the Chinese market" and which government officials "never fully blocked." James Griffiths, *The Great Firewall of China*, London: Zed Books, Ltd., 2019, 62.

¹² The free circulation of information made officials "feel [as if] they've got their backs against the wall." Geremie R. Barme and Sang Ye, "The Great Firewall of China," Wired, June 19, 1997. <u>https://www.wired.com/1997/06/china-3/</u>.

¹³ See Samm Sacks, "Apple in China, Part 1: What does Beijing Actually Ask of Technology Companies," Lawfare, February 22, 2016. https://www.lawfareblog.com/apple-china-part-i-what-does-beijing-actually-ask-technology-companies.

¹⁴ Griffiths, *The Great Firewall of China*, 8.

¹⁵ Sacks, "Apple in China, Part 1," above. (Emphasis added.)

EXPORTING CENSORSHIP AND INTERNET SOVEREIGNTY | JANUARY 2021

In the early 2000s, Yahoo, for instance, was designing an "internet guide" for use in China. This "internet guide" both linked to party-sanctioned news sources and agreed to censor content offensive to the government. Yahoo's efforts to cooperate with the government were so pervasive that when a "Public Pledge on Self-Discipline for the Chinese Internet Industry" was announced, it was the only American company to sign the pledge. The pledge, among other things, required companies to "refrain from 'producing, posting or disseminating pernicious information that may jeopardize state security and disrupt *social stability*, contravene laws and regulations and spread superstition and obscenity" and to "monitor the information publicized by users on websites… and remove the harmful information promptly."¹⁶

Yahoo, though, was not alone in helping the Chinese government build a censored internet. Cisco helped provide the hardware necessary for China to deploy the Great Firewall and Golden Shield. According to James Griffiths, the company principally known for its routers and networking products "began supplying filtering and surveillance equipment to Chinese censors in the early 1990s."¹⁷ Sprint, under a contract with ChinaTelecom, was responsible for the infrastructure that essentially connected the Chinese people to the internet.

Worth noting is that many U.S. companies involved in building China's internet infrastructure could argue that it was impossible to foresee the pervasive censorship that exists today. With history as a guide and the well-known nature of communist regimes censoring news, though, one can assert that the Great Firewall and Golden Shield were completely foreseeable outcomes.¹⁸

China's conceptions of internet sovereignty have been around since, at least, 2010. In 2014, China started promoting it internationally, with calls for countries to "establish a multilateral, democratic, and transparent international internet governance system."¹⁹ With hardly any support for its vision of a censored internet, China decided to continue promoting the concept and working behind the scenes at bodies like the Internet Corporation for Assigned Names and Numbers (ICANN) to export its values, including the concepts of internet sovereignty and social stability, and to utilizing its greatest asset: its economic markets.

¹⁶ Ibid at 64. (Emphasis added.)

¹⁷ Griffiths, The Great Firewall of China at 29-30.

¹⁸ As recounted by James Griffiths, as early as 2004, Yahoo was acting as "Chinese police auxiliary", providing information that would help government authorities arrest a journalist. See, The Great Firewall at 64-65.

¹⁹ Segal, The Hacked World Order, at 32.





China Exports its Values by Controlling Access to its Market

Access to a market can be a powerful motivator. The promise of access to a massive economic market can be even more powerful. China partially realized the gravity of its economic power when developing the Great Firewall and Golden Shield. Initially, much of the censorship was "outsourced" to companies participating in the internet space, both service providers and edge services.²⁰ The government, though, has taken an increasingly greater role in managing content.

China has realized its ability to export its vision of a censored internet by tapping into its economic power. China enjoys economic power in two different ways: T by granting foreign companies access to its market and through creating strong, global technology and communications firms.

²⁰ The term "edge" denotes any entity that provides services through a website, web service or application, or hosts user-generated content. Examples of edge services in the United States include Microsoft, Amazon, Facebook, and Oracle.

Access to the Chinese economic market is a powerful tool for China. Technology companies, such as Google, Microsoft, Apple and others have long wanted access to China's billion residents and their money. As of several years ago, for example, China accounted for a significant percentage of Apple's revenue—\$16 billion compared to \$74.6 billion in quarterly revenue.²¹ While exact figures are not provided, overseas revenue accounts for most technology companies' profits. In 2014, Google (now Alphabet) "earned 58 percent of its revenue from outside the United States; Facebook 55 percent…"²²

China flexes this type of economic power in several different ways. If a western technology company wants access to the Chinese market, the company must adopt China's vision of a censored internet, at least for products distributed in China.²³ Apple, as an illustration, promotes the security and privacy features of its products in the United States, but for devices sold in China, it removes apps from the AppStore upon request from the Chinese government. Some of these apps allowed users to circumvent the Great Firewall while others helped protestors track police movements. The company also acceded to demands that it store data generated by Chinese residents to servers operated by China Telecom, the state-owned telecommunications network.

The second way China flexes economic power is through corporate governance. Major companies that want access to the Chinese market must create a joint venture with a local Chinese company. While this may sound somewhat innocuous, the devil is in the details. There is no such thing as a private company in China, at least as the West understands the term "private."

The government significantly influences, if not controls most or all the private businesses in China, and the Communist Party runs the government. There is no separation between the party and the government. The Chinese Communist Party boasts that "68 percent of China's private companies had party bodies by 2016 and 70 percent of foreign enterprises."²⁴ The party's goal is to have organs in 95 percent of the companies. The presence is not merely salutary, as it is

24 Richard McGregor, "How the state runs the business in China," The Guardian, July 25, 2019. <u>https://www.theguardian.com/</u> world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei.

²¹ Segal, Adam, The Hacked World Order, New York, NY: PublicAffairs, 2016, 20.

²² Ibid.

²³ The government requires that "foreign companies wanting" to do business in the country open joint ventures if they fall into one of 35 categories. The categories roughly align with the government's economic priorities, which include nearly all categories of technology, including artificial intelligence, autonomous vehicles, 5G, robotics, and so on. See generally, U.S.-China Economic and Security Review Commission, How Chinese Companies Facilitate Technology Transfer from the United States, by Sean O'Connor (Washington, D.C., May 6, 2019), https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20 Facilitate%20Tech%20Tec



instrumental in corporate decisions.25

The Communist Party exerts control over foreign businesses, whether or not those businesses are technology companies. Giants like Walmart, Disney, and others have party apparatuses active in their Chinese operations. The party presence may force corporations to engage in conduct, such as allowing workers to "unionize" where such actions may be frowned upon in the United States. When company workers are unionized in China, the party also controls those unions.

Party presence and control of joint ventures causes several problems. China requires companies to censor content domestically, transfer intellectual property, and leads to viewpoint censorship internationally for continued access to the Chinese market.

The Great Firewall and Golden Shield are enforced both by government censors and through private sector cooperation. In return for access to the Chinese market, China demanded that Google, Facebook, and Twitter censor material

^{25 &}quot;In the past, Chinese state-owned listed companies had customarily filed misleading prospectuses ahead of their stock exchange listings, omitting the party's pivotal role in the hiring and firing of senior executives. Similarly, company boards had long been legally and theoretically independent of the party, but not in practice. 'The same individual who is chairing a party committee meeting on a Monday might well be chairing a board meeting later in the week,' notes a 2018 report on Chinese corporate governance." Ibid.

deemed inappropriate by the party and government. The technology companies refused and, consequently, were banned in China. Similarly, as previously mentioned, China demanded that Apple move data about Chinese users to government-controlled servers. Yahoo, for continued access, acquiesced to government demands both to censor content and cooperate with the government identifying dissidents.

When a foreign technology company wants access to the Chinese economic market, it must create a joint venture with a local Chinese company. Through the newly created joint venture, the local Chinese company obtains access to the foreign technology company's intellectual property. Because the local party is controlled by the government *vis-à-vis* the communist party, the government secures the foreign intellectual property. Rather than respect the foreign company's intellectual property, the government seeks to replicate the technology illegally, provide a Chinese company with the stolen property, and then undercut the foreign company, flooding the market with products artificially low due to subsidization. This is a model that has worked well, for example, for the telecommunications giant Huawei.

Not content to implement its domestic vision of the internet and steal foreign intellectual property, China is starting to realize the ability to export its cultural views and vision of the internet through American companies. In late 2019, both Activision and the National Basketball Association (NBA) have either removed foreign content China deemed inappropriate or apologized for such content.

In the case of Activision, it owns a game developer known as Blizzard, which in turn created a game called Hearthstone. Hearthstone is an online game, which provides users not only a platform for playing with each other, but also for communicating with each other. After a Hearthstone match, a player from Hong Kong promoted a pro-democracy message supportive of protests occurring in his home country. Several other players expressed support for Hong Kong during the interaction. As a result, Blizzard announced a lengthy ban for all involved, and especially for the user who started the discussion.

As a company, Blizzard enjoys a fanbase in China, access to an esports market some estimate at \$3 billion, and the Chinese technology company Tencent owns a 5 percent stake in the company. Blizzard's actions censoring content and punishing users who dared express a pro-democracy message appear to be nothing more than pandering to the Chinese Communist government in exchange for continued access to a market.





Similarly, Houston Rockets general manager Daryl Morey tweeted support for the pro-democracy movement in Hong Kong. Immediately China objected, and several Communist Party controlled companies, such as Tencent and Luckin Coffee, threatened to cut ties with the NBA. To maintain the lucrative contracts and access to the Chinese market, NBA Commissioner Adam Silver apologized for the statements. Even NBA superstar LeBron James trumpeted what could have been Communist Party talking points, stating he believed that Morey was "either misinformed or not really educated on the situation."

Through access to the market, China exported its values and vision of the internet to the United States. As when the Great Firewall was created, China relied on private companies to enforce its restrictive standards. By relying on private companies, such asBlizzard and the NBA, China effectively superseded the values represented in the American Constitution, while both the NBA and Blizzard were willing participants in this effort.

The second way China enjoys economic power is through strong technology companies of its own. Of the top ten global technology companies in 2019, two were Chinese (Alibaba and Tencent). That number of top global companies increases to five for the top twenty firms (Meituan Dianping, JD.com, and Baidu). More importantly, Chinese firms are among the fastest growing technology firms. The enormous growth of Chinese companies is evident when comparing size and revenue both over the past few years. In 2014, Tencent had a market cap value of \$132 billion, Baidu a value of \$59 billion, and JD.com a value of \$29 billion. For the same year, the top American companies included Apple, with a value of \$529 billion, Google with a value of \$377 billion, Facebook with a value of \$157 billion, and Amazon rounding out the top 4 with a value of \$144 billion. In 2019, Alibaba, which did not make the list of the most valuable global technology companies in 2014, had a market cap value of \$402 billion; Tencent, \$398 billion; JD.com, \$39 billion; and Baidu, \$38 billion. Microsoft led American companies, claiming the number 1 spot with a value of just over \$1 trillion, with Amazon and Apple rounding out the top three with values of \$888 billion and \$875 billion, respectively.

Chinese social media companies are some of the most popular global platforms. As of early 2020, Tencent's WeChat boasted more than 1 billion users, which places it just behind Facebook Messenger and WhatsApp. Sina Weibo, partially owned by Alibaba, claimed to have more than 430 million active monthly users (compare with Twitter's estimated 326 monthly users). TikTok, owned by Chinese Company ByteDance, had nearly 1.5 billion users globally and still enjoys significant growth in the United States.

Because all the platforms are Chinese, they must comply with China's internet governance standards, which means censoring content at the government's request. For some companies, such as WeChat or Weibo, the impact of this censorship falls primarily in China. For other companies, though, such as TikTok, this mandated censorship means that Americans are finding some posts removed from the platform. This censored content includes posts promoting the prodemocracy protests in Hong Kong and others critical of the Communist government.²⁶

Chinese telecommunications firms, similarly, enjoy widespread popularity. The popularity is due, in large part, to low product prices. The low product prices, in turn, are created through both intellectual property theft and government subsidization. The two companies principally benefitting from this arrangement are Huawei and ZTE. Huawei, in its due turn, deserves a bit of attention.

²⁶ If the censorship were occurring at the behest of the United States' government, users would have recourse through the court system, as the Constitution's First Amendment would bar the government from engaging in viewpoint discrimination. Since the Constitution, though, only regulates government conduct, private companies are free to remove content based on viewpoint, if they wish. Additionally, the Constitution only applies to the United States' government and, in some instances, to state and local governments. Given the relationship between the Communist Party and the government of China, some interesting questions are raised when the Chinese government directs the censorship of content posted by Americans. In this case, the answer is likely increased transparency, so that American users understand that the Chinese government does not share their values, rather than any form of government manipulation of the market.



Before that, though, it is worth noting that telecommunications firms represent unique vulnerabilities both to national security and for exporting China's internet governance standards. More than social media platforms or other technology companies, telecommunications firms represent the backbone of the internet. The internet is a hybrid technology, part telephonic services and part computers, with the two services becoming increasingly integrated. The next generation of mobile services, 5G or small cell technology, is as much a cloud service as it is a telecommunications service.

Because of the integration between computers and telecommunications service, a savvy telecommunications product provider could use its technology both to listen in to calls and to censor traffic. Now, there is little evidence that Huawei or ZTE are engaging in such nefarious services, but that does not mean they could not. A recent study by Britain's GCHQ, for example, found no evidence that Huawei's firmware and software included backdoors the Chinese government could access. It also found, though, that the coding was incredibly complex and full of bugs. The code complexity and bugs would require Huawei to push updates to the products. Between the need constantly to update software and Chinese laws requiring companies to aid the government in an emergency if so demanded, the potential exists both for massive surveillance and for the forced adoption of Chinese internet values.



Conclusion

China's vision of the internet and the values it promotes are vastly different from the vision and values espoused by the internet's creators. The internet's creators programmed western, and particularly American, values into the internet. These values include freedom of speech, freedom of expression, a desire to be free of unwarranted government surveillance, and the ability to communicate globally with anyone at any time.

China values an internet based on national "internet sovereignty" and eschews the free circulation of information—which is the single greatest threat to an authoritarian government. Its vision has led to the creation of a heavily censored internet. By promising, granting, or threatening to close access to its market, China has started to export its cultural values and vision of the internet beyond its national borders. Both Chinese and American companies are starting to censor messages the Chinese Communist Party deems inappropriate. If this trend continues, Americans and American companies will be complicit in allowing China's standards to dominate the globe, replacing the very values Americans hold dear.

Barme, Geremie R. and Sang Ye. "The Great Firewall of China." Wired. June 1, 1997. https://www.wired.com/1997/06/china-3/.

Bristow, Michael. "China defends internet censorship." BBC News. June 8, 2010. http://news.bbc.co.uk/2/hi/8727647.stm.

California. Department of Justice. *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations*. Sacramento, CA: California Dept. of Justice, Office of Attorney General, August 2019. http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_

Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

Chen, Laurie. "NBA in damage-control mode as more Chinese partners cut ties in Hong Kong protest tweet storm." South China Morning Post. October 9, 2019. <u>https://www.scmp.com/news/china/society/article/3032164/nba-damage-</u> <u>control-mode-adam-silver-lands-china-hong-kong</u>.

China Digital Times. "Cybersecurity Law: Reactions and Recent Enforcement." June 20, 2017.

https://chinadigitaltimes.net/2017/06/chinas-new-cybersecurity-law-reactionsrecent-enforcement/.

Clark, Peter Allen. "What to Know about Blizzard, Hong Kong and the Controversy Over Politics in Esports." Time. October 21, 2019.

https://time.com/5702971/blizzard-esports-hearthstone-hong-kong-protestsbacklash-blitzchung/.

Cockerell, Isobel. "TikTok—Yes, TikTok—Is the Latest Window Into China's Police State." Wired. September 25, 2019.

https://www.wired.com/story/tiktok-is-the-latest-window-into-chinas-policestate/.

Economy, Elizabeth C. "The great firewall of China: Xi Jinping's internet showdown." The Guardian. June 29, 2018.

https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown.

Getlen, Larry. "China's secret plan to topple the US as the world's superpower." New York Post. February 8, 2015.

https://nypost.com/2015/02/08/chinas-secret-plan-to-topple-the-us-as-theworlds-superpower/.

Glaser, April. "Is a Tech Company Ever Neutral?" Slate. October 11, 2019. <u>https://slate.com/technology/2019/10/apple-chinese-government-microsoft-amazon-ice.html</u>.

Harwell, Drew and Tony Romm. "TikTok's Bejing roots fuel censorship suspicion as it builds for a huge U.S. audience." The Washington Post. September 15, 2019. <u>https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-</u> <u>fuel-censorship-suspicion-it-builds-huge-us-audience/</u>.

Hern, Alex. "Revealed: how TikTok censors videos that do not please Bejing." The Guardian. September 25, 2019. https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-

censors-videos-that-do-not-please-beijing.

Kharpal, Arjun. "Everything you need to know about WeChat – China's billion-user messaging app." CNBC. February 3, 2019.

https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messagingapp.html.

Layton, Roslyn. "Trump Should Ignore Chinese Manufacturers' Phony Promises." Forbes. February 20, 2019.

https://www.forbes.com/sites/roslynlayton/2019/02/20/trump-should-ignorechinese-manufacturers-phony-promises/#715790b50ec8.

Maags, Christina. "The Great Firewall of China." Fair Observer. September 23, 2019. https://www.fairobserver.com/region/asia_pacific/great-firewall-chinacensorship-chinese-news-today-vpn-china-38018/.

McGregor, Richard. "How the state runs business in China." The Guardian (UK). July 25, 2019.

https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinpingcommunist-party-state-private-enterprise-huawei.

Meeker, Mary. "Internet Trends 2014." Kleiner Perkins, May 28, 2014. https://www.bondcap.com/report/itr19/#view/12.

Meeker, Mary. "Internet Trends 2019." Bond Capital. June 11, 2019. https://www.bondcap.com/report/itr19/#view/.

Meeker, Mary, "Internet Trends 2009." Morgan Stanley. October 20, 2009. <u>https://www.slideshare.net/Devcorporate/mary-meeker-morgan-stanley-internet-trends-october-2009</u>.

O'Brien, Danny. "China's Global Reach: Surveillance and Censorship Beyond the Great Firewall." Electronic Frontier Foundation. October 10, 2019. <u>https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-</u> <u>censorship-beyond-great-firewall</u>.

Pierson, David. "While it defies the U.S. government, Apple abides by China's orders and reaps big rewards." Los Angeles Times, February 26, 2016. <u>https://www.latimes.com/business/technology/la-fi-apple-china-20160226-story.</u> <u>html</u>.

Ren, Yuan. "Know Your Chinese Social Media." The New York Times. November 19, 2018.

https://www.nytimes.com/2018/11/19/fashion/china-social-media-weibo-wechat. html.

Robertson, Matthew. "Lenovo, Chinese Computer Giant, Sued for Patent Infringement." The Epoch Times. March 29, 2011.

https://www.theepochtimes.com/lenovo-chinese-computer-giant-sued-forpatent-infringement_1499997.html.

Sacks, Samm. "China's Cybersecurity Law Takes Effect: What to Expect." Lawfare. June 1, 2017.

https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect.

Segal, Adam. The Hacked World Order. New York, NY: PublicAffairs, 2016.

Silverman, Robert. "What did LeBron James say about China that almost everyone else in the NBA hasn't said, too? NBC News. October 20, 2019. <u>https://www.nbcnews.com/think/opinion/what-did-lebron-james-say-aboutchina-nearly-everyone-else-ncna1069131</u>.

Smith, Noah. "Trump Should Take Aim at China's Joint-Venture Rule." Bloomberg Opinion. March 3, 2019.

https://www.bloomberg.com/opinion/articles/2019-03-03/trump-shouldpressure-china-to-drop-its-joint-venture-rule#skip-to-main-content.

Smith, Oliver. "The GDPR Racket: Who's Making Money From This \$9bn Business Shakedown." Forbes. May 2, 2018.

https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whosmaking-money-from-this-9bn-business-shakedown/#7a17d38134a2.

Statt, Nick. "TikTok's global social media takeover is starting to slow down." The Verge. November 4, 2019.

https://www.theverge.com/2019/11/4/20948731/tiktok-bytedance-china-socialmedia-growth-users-decline-first-time.

Turak, Natasha. "China's response to NBA Hong Kong tweet was a 'violation of US sovereignty,' Condoleezza Rice says." CNBC. November 11, 2019. <u>https://www.cnbc.com/2019/11/11/china-response-to-nba-hong-kong-tweet-was-</u>violation-of-us-sovereignty-rice.html.

U.S.-China Economic and Security Review Commission. *How Chinese Companies Facilitate Technology Transfer from the United States*, by Sean O'Connor. Washington, DC, May 6, 2019.

https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20 Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf.

Wei, Lingling and Bob Davis. "How China Systematically Pries Technology From U.S. Companies." The Wall Street Journal. September 26, 2018. https://www.wsj.com/articles/how-china-systematically-pries-technology-from-

<u>u-s-companies-1537972066</u>.



317 A Street SE Washington, DC 20003 (202) 350-1689 info@raineycenter.org raineycenter.org