The Journal of Asian Studies Vol. 77, No. 4 (November) 2018: 923–933.
 doi:10.1017/S0021911818002541

Platform Patrol: China, the United States, and the Global Battle for Data Security

AYNNE KOKAS

Keywords: China, Committee on Foreign Investment in the United States, cybersecurity, cybersovereignty, data security, Made in China 2025, platforms, United States, World Internet Conference

Introduction

In Apple CEO Tim Cook's keynote speech at the Chinese government's 2017 World Internet Conference, he extolled the values of "Privacy. Security. Decency" (Apple Newsroom 2017). The last two terms, "security" and "decency," have long been closely associated with Chinese government efforts to control the Internet. Indeed, in 2017 Apple agreed to turn over user data to Chinese government servers and start a Chinese provincial government-run data storage center. Yet in 2015, Apple refused to turn over the passcode for one user in the United States during the FBI investigation following the San Bernardino terrorist attacks. The company's different policies in the United States and China relate directly back to Apple's concern for market share and access.

China creates digital borders that push US technology firms to allow Chinese regulators access to private corporate and individual user data, even though Chinese firms would not make similar agreements with regulators in the United States, nor would US firms make those same concessions in the United States. China takes a broad view of its national sovereignty by looking not merely at physical oversight over airspace or terrestrial or marine borders, but also at the digital infrastructure and activity that constitute the country's sphere of authority. The Chinese government defines its control over the country's digital spaces (as well as outside access to those spaces) as "cybersovereignty."

China articulated its policy of cybersovereignty early on:

> The Internet sovereignty of China should be respected and protected.… China maintains that all countries have equal rights in participating in the administration of the fundamental international resources of the Internet and a multilateral and transparent allocation system should be established on the basis of the current management mode, so as to allocate those international resources of the Internet, and a multilateral and transparent allocation system should be established on the basis of the current management mode, so as to allocate those resources in a rational way and to promote the balanced development of the global Internet industry. (Information Office of the State Council of the People's Republic of China 2010)

Aynne Kokas (aynnekokas@gmail.com) is Assistant Professor at the Woodrow Wilson Center at the University of Virginia.

In this statement, the Chinese government clearly identifies the importance of sovereignty in the control of digital resources as coming before participation in multi-stakeholder oversight through international organizations. The statement further articulates the importance of managing "the balanced development of the global Internet industry," a rationale for protecting the development of China's Internet industries from more developed competitors.

China has continued to build on these principles through its laws and regulations. Most notably, in 2017, China implemented a new cybersecurity law that required any information deemed critical, broadly defined, to be stored on local, government-owned servers in order to protect its sovereignty (Quanguo Renmin Daibiao Dahui 2016). The centrality of sovereignty and "global balance" in China's Internet governance doctrine facilitates the extension of Chinese cybersovereignty into US corporate governance. For the purposes of scholars of the media industries examining Sino-US trade, this suggests the need to move our research into a new domain: security.

Understanding the repercussions of China's technology and Internet policy is important because media platforms like the App Store operated by Apple already depend on their sales in China. Other firms like Netflix, Cisco, and Amazon have made significant compromises with Chinese corporate partners and Chinese government regulators to enter the market (Kokas 2018; Russell 2017). In the United States, Silicon Valley corporate interests have taken the lead in making technology policy, ensuring access to large troves of personal consumer data with scant responsibility for protecting it, as demonstrated by the hacks of Equifax, Anthem Healthcare, Target, and Facebook. In combination, the lack of consumer protections in the United States and the increasing global influence of Chinese national technology policy pose a potent long-term risk. Specifically, because of its failure to regulate US tech companies' operations, the US government is forgoing oversight over a precious resource: user data generated by commercial media platforms.

User data—the type gathered by social media sites, online video portals, "smart" appliances, payment apps, and the other platforms that shape our digital lives—is highly valuable as a tool both for creating reliable commercial algorithms and for surveillance. In this case of platforms operating in the United States and China, this resource is currently caught in limbo between internal corporate servers (both US and Chinese), Chinese government efforts to nationalize data storage, and international government surveillance efforts. The result of this situation is that US consumer platforms that seek to operate in China are simultaneously unaccountable to the US government and in debt to the Chinese government. The asymmetry in technology policy between the United States and China—a laissez-faire attitude on the part of US regulators contrasting with China's national interest–driven restrictions—means that the United States is effectively ceding authority over vast amounts of data, one of the most under-regulated resources of the twenty-first century, to China.

The US strategy of deferring to Silicon Valley in technology policymaking—supporting disruption while limiting regulation—may spur domestic innovation in the United States. However, it has left both US companies and global consumers vulnerable to Chinese government efforts to control global data. China, in other words, is shaping the global circulation and security of commercial data by taking advantage of the limitations in US regulations.

US Data Regulations

Though the United States played an active role in the development of the Internet, it has taken a laissez-faire approach to regulating companies and the data they generate. US firms have the freedom not only to gather consumer data, but to evade punishment if they fail to secure the data or the consumer platforms on which it is generated. For example, in Target's 2013 massive data breach, the company had to pay a financial settlement to consumers and to Visa, but faced no charges from the Securities and Exchange Commission. Further, the case demonstrated that even when there are laws requiring companies to notify consumers of their data breaches, the consumers still have little recourse (Peters 2014). Even in the wake of the Equifax breach, the US Congress still has yet to pass substantive consumer data protection laws (DiGrazia 2018).

US state laws have historically provided consumers the limited protection that they have from data breaches. The New York State Department of Financial Services was the first to incorporate comprehensive legislation for minimum security standards. Forty-eight states and most territories require notification to consumers if their data is breached, but until recently, that has been interpreted as applying to unencrypted data (DiGrazia 2018). US domestic consumer data security practices pertaining to government and commercial platforms are limited.

It is not surprising, then, that Chinese technology companies encounter a comparatively open digital environment in the United States. Chinese firms can raise capital by selling shares and listing initial public stock offerings on US capital markets (Kokas 2014). Chinese social media, video, and payment platforms are accessible in the United States, due to the openness of US markets. While such policies are the result of decisions in both countries at the national level, they have both global consequences for the international tech industry and local impacts on individual consumers.

In response to Chinese technology investment in the United States, the US government is attempting to control Chinese investment in US firms through a national security–oriented committee in the Department of the Treasury, the Committee on Foreign Investment in the United States (CFIUS). CFIUS, however, has serious limitations. It has jurisdiction over forthcoming full acquisitions, but little to no oversight over acquisitions that have already been approved. The CFIUS process has blocked only a few Chinese technology acquisitions, and does not apply at all to a wide range of transactions. With limited oversight over foreign investment in US tech platforms, the United States is now finding itself having to oversee not just data security risks from foreign entities, but also data security risks related to companies based in the United States.

The US executive and legislative branches are attempting to update this approach. In August 2018, President Donald Trump signed the National Defense Authorization Act for Fiscal Year 2019 into law (Garamone 2018). The act included the congressional consensus version of the Foreign Investment Risk Review Modernization Act, a bipartisan effort to modernize CFIUS. With respect to Chinese technology investment in the United States, the act allows for increased scrutiny of acquisitions by specific countries that are technological competitors, takes into consideration overall market share held by foreign stakeholders before approving acquisitions, and requires increased scrutiny over acquisition activity for firms which could present high levels of cybersecurity risk or access to the data of US citizens, broadly defined. While this is an important step forward, the United States still faces

a long time horizon of enactment of some of its provisions in a rapidly changing technology landscape. The act does not contend with the role that control over existing assets plays, nor have the impacts of the new process been extensively vetted. Thus, despite efforts to shore up oversight over technology acquisitions, significant challenges remain.

Increasing Chinese government access to commercial data presents significant challenges. Chinese government data servers have been rated by researchers as having poor privacy protections (Reddick and Zheng 2018). Thus, government access to corporate servers presents potential increases in the likelihood of data breaches for both US and Chinese firms. The United States Trade Representative has expressed concerns that such measures "could restrict the use of foreign information and communication technology (ICT) products and services in a wide range of commercial sectors." (Office of the United States Trade Representative 2016). Finally, scholars have hypothesized that rather than just providing a strategy for enhancing domestic cybersecurity, China's data localization laws actually increase China's advantage in signals intelligence capability through access to additional data from both local and foreign sources (Selby 2017).

The risks to US user data produced by the minimal US regulatory oversight are compounded by Chinese technology policy, specifically through acquisitions, China's 2017 cybersecurity law, and the role played by US capital markets in financing technology firms. Through these three means, Chinese technology policy demands trade-offs from US companies, often in ways consumers and regulators might find objectionable if they had full knowledge of them.

Sino-US joint ventures make the picture even more complicated. Information sharing in joint ventures is treated as an internal corporate matter. Therefore, intellectual property or data privacy violations that would previously have been forbidden under the US-China Cyber Agreement (2015), a landmark agreement against hacking foreign corporate interests between the US and Chinese governments, become internal Chinese corporate matters, which then removes them from the oversight of the US-China Cyber Agreement. The move to require foreign firms to participate in joint ventures to access the market shapes data management practices in such a way that international data falls under the internal regulation of Chinese companies, thus giving Chinese regulators the power to oversee it.

The US-China Cyber Agreement, in which both governments agreed to "refrain from conducting or knowingly supporting cyber-enabled theft of [corporate] intellectual property" (Congressional Research Service 2015), was designed to mitigate Chinese government interference in US corporations and vice versa. The agreement, however, leaves significant challenges unaddressed. For example, the definitions of intellectual property it uses typically cover the structure of databases, but not necessarily the privacy of the user-generated data within those databases.

Most significantly, the US-China Cyber Agreement applies only to foreign corporations. Partially owned companies or joint ventures present a challenge to the protections inscribed in the agreement. First, in the realm of partial acquisitions or joint ventures, who owns intellectual property within the firm becomes a much muddier question than in cases in which one firm takes the intellectual property of another separate firm. Ultimately, increased Chinese acquisitions and partial acquisitions of US firms render much of the agreement moot by shifting the ownership structure of firms so that they are no longer protected as US companies.

Second, China's cybersecurity law requires all critical information (broadly defined) to be stored on Chinese-owned servers. As a result, any foreign companies dealing with critical information must establish a domestic joint venture partnership (Yue et al. 2017). By increasing the amount and type of data stored in Chinese-owned data centers, China has structured its laws in such a way that it has increased the amount of data stored under Chinese government jurisdiction, as well as the type of firms included. This creates an increased cybersecurity risk for US technology companies with a significant presence in China.

While data security has long been an issue percolating domestically in the United States, as the Chinese and US digital economies become more entwined, it has taken on an increased urgency. Now, rather than just being concerned about the conflicts of interests entrenched in relationships between US policymakers and US companies, it becomes necessary to consider the same issues between a wide range of constituencies—Chinese policymakers and US companies, private Chinese companies and US companies, Chinese state-owned enterprises and US companies, Chinese policymakers and US policymakers, Chinese private companies and US policymakers, Chinese companies and US capital markets, etc. The complex layers of relationships dwarf the complexity of the current system and are rife with possibilities for abuse.

US capital markets further complicate the relationship between the American and Chinese technology industries. Major Chinese Internet firms like Alibaba, Tencent, and Baidu have historically listed their stocks on American, rather than Chinese, stock exchanges. By listing stocks on US capital markets, Chinese firms are leveraging foreign resources to expand their business operations (Kokas 2014). This strategy has allowed Chinese firms to grow into significant global competitors benefiting from stricter listing requirements, more intensive regulatory monitoring, a wider shareholder base, foreign expertise, and access to additional capital (Zhang and King 2010).

This may change as the Chinese government is takes additional steps to localize technology investment. Early Chinese listings on US capital markets were done through the Variable Interest Entity (VIE) structure. VIEs, rather than allowing direct foreign investment in Chinese firms, are a contractual arrangement designed as a workaround to transfer capital (Schindelheim 2012). In a VIE structure, US firms purchase shares in an offshore (typically a shell) company (Shi 2014). The ability to invest in Chinese firms through the VIE structure emerged as a result of an incompleteness in China's investment laws. Once the loophole was closed, those investments became illegal. Chinese firms then shifted to being listed on US exchanges as American depository receipts, shares in foreign stocks that are traded on a US exchange. In March 2018, the Chinese government urged technology firms to move their listings back to Chinese capital markets (Chen 2018). However, on October 2, 2018, Chinese firm Tencent Music Entertainment Group filed for an initial public offering (IPO) in the United States. Financial industry analysts have hailed the IPO as one of the biggest in the technology industry to date (Farrell and Steele 2018).

US capital markets enable the strict regulation of Chinese market entry by continuing to support Chinese firms seeking to raise capital outside China, despite a lack of reciprocity for foreign direct investment in media and technology in China. This is particularly important in the case of platforms that handle consumer data because of the relative vulnerability of consumers when compared with corporations and

governments. With the existence of these Chinese firms predicated on Chinese government access to their corporate decision-making apparatus, their expansion extends Chinese soft power to a degree unattainable by other forms of media. The intersection of the Chinese government and Chinese corporate decision-making is shifting the balance toward greater Chinese influence in the global technology industry with the support of American capital markets (Kokas 2018).

The interplay of financing, regulatory oversight, and technological development in the financing of Chinese technology firms offers valuable insight into the leverage that the Chinese government and US capital markets have in the growth of the Chinese technology industry. At present, Chinese firms are drawing capital from and producing profits for US-based financial institutions. This benefits the US financial industry, but provides Chinese firms with preferential access to US consumers in a way that is not reciprocated in China. Historically, firms have leveraged the potential gains from these investments to continue their growth in international markets (Kokas 2014).

Cybersovereignty and *Made in China 2025*

Similarly, within the context of innovation localization and financing, China has outlined goals for technology innovation through its *Made in China 2025* industrial masterplan, an outline of its national strategic technology innovation goals. The larger goal of *Made in China 2025* is to drive domestic growth in the media and technology industries through import substitution and domestic development (Guowuyuan 2015). By favoring domestic players, the larger effect is to further shift the balance of market power to Chinese firms. This ultimately creates a strategic landscape that is increasingly difficult to navigate for foreign competitors. Ultimately, the strategic direction of *Made in China 2025* implies a bright future of innovation for the Chinese domestic market, while also suggesting challenges that market entrants from other countries will face in the years to come.

Made in China 2025 and China's cybersecurity law create the structure and the rationale for China's digital borders. *Made in China 2025* provides the resources to develop local competitors to provide key technologies. China's cybersecurity law provides a national security rationale for using those local competitors rather than international providers. Together, the two frameworks both spur the development of local industry and prevent the expansion of international investment in the Chinese technology market.

China asserted the importance of cybersovereignty in its 2010 policy, but this was merely the beginning of a framework that has since been fleshed out with both incentives and penalties. The *Made in China 2025* plan offers an outline of the parts of the technology industry that are national priorities. China's cybersecurity law ensures that the key data that undergird those technologies are state-controlled.

US Firms in China

As China outlines its long-term technology development goals, US CEOs have demonstrated repeatedly that they are willing to provide Chinese government officials with

access to their platforms in exchange for market access. For example, Mark Zuckerberg took multiple meetings with China's former Internet Czar Lu Wei. US CEOs have demonstrated no appetite for pushing back against the demands of the Chinese government if such pushback would affect their potential to operate in the market (Arsène 2016).

We are now at an inflection point. Platforms are gathering huge amounts of consumer data (and other forms of data) to build smarter algorithms, which will displace more workers. With open access to the US market and virtually no foreign competitors at home, Chinese firms are getting access to vast quantities of this data, largely because there is such limited protection of consumer data in the United States and many other countries around the world. Consumers (and their data) are being sold out. Just as with the automotive industry, failure to get ahead of developments in the market may lead to a dramatic loss of American competitiveness in a key industrial sector.

The US-China technology policy relationship has already proven problematic for consumers seeking to navigate their digital lives. For example, immediately following the implementation of China's 2017 Cybersecurity Law requiring the key data generated in the PRC to be stored in the PRC, Apple agreed to be the minority partner in a cloud computing joint venture with a majority stake held by Guizhou Yunshang, a company funded by the Chinese provincial government of Guizhou. In January 2018, Apple moved the data of China-based users whose data had previously been stored on Apple servers to Guizhou Yunshang–controlled servers. Some users with US-based Apple IDs reported receiving notifications that their data was also being moved (Russell 2018). Unlike governments and corporations, consumers typically do not develop or control their own proprietary platforms, and are thus subject to the decisions of more powerful stakeholders. Consumers around the world are caught within a web of Sino-US institutional data gathering, sharing, and distributing.

In 2017, Apple was one of the first firms to build a new joint venture data center in China in order to comply with China's cybersecurity law. The law, as mentioned above, requires all firms that maintain "critical information infrastructure" to store their data on a Chinese-owned server. Apple, like many foreign firms operating in China, relies heavily on data centers to operate within the Chinese market. However, for Apple, as for many other firms in areas ranging from engineering services to enterprise computing, the decision to open a data center held with major ownership by a Chinese firm transforms the politics of power and access to data within the company and in its relations with consumers. China's cybersecurity law and the related technology regulatory framework will fundamentally transform both the ownership and the circulation of data not only within China, but for all global companies that operate in China. By regulating the security issues presented by global corporate data investments, China is establishing new global standards for the data trade. The laissez-faire policies of the United States protect neither consumers nor national competitiveness.

Consumer Risk, National Risk

By failing to closely oversee commercial data security, the US government is not just putting consumers and national competitiveness at risk, but also providing vulnerable targets for Chinese military exploits. In 2014, soldiers from the People's Liberation

Army allegedly hacked US companies for the benefit of Chinese companies (Schmidt and Sanger 2014; Wortzel 2014). The intersection of the military and the commercial in the landscape of technology development created strategic risks not just for Chinese and US companies, but also for the Chinese and US militaries, particularly with regard to the question of appropriate responses to military attacks on consumer technologies.

Trade, national security, and consumer data are all tied up together. China, for example, maintains a policy of "comprehensive national power," a strategy for incorporating consumer and military risks into its overall national security policy. Through its comprehensive national power framework, China recognizes cybersecurity as a central tenet not merely in military combat, but in the functioning of the country. The Cybersecurity Administration of China has comprehensive authority over military and consumer cybersecurity. That comprehensive approach allows China to more effectively build and police national borders in cyberspace.

The United States, by contrast, lacks a centralized cybersecurity agency. Instead, the country balkanizes data regulation into the departments of Homeland Security and Defense, the Federal Trade Commission, the Federal Communication Commission, and numerous others. The lack of comprehensive policymaking with regard to data creates gaps in oversight—gaps that are easy for countries with a more comprehensive policymaking framework to exploit.

New Chinese Institutions, New Chinese Policies

The Chinese government, leveraging strategies the United States used to export its aviation industry standards, is expanding its oversight over global consumer platforms through a combination of Chinese-led standards-building, participation in international organizations, and overseas direct investment. Standards-making events like the annual Internet Governance Forum and China's World Internet Conference are helping to expand the influence of China's standards. The Chinese government is using the growing influence of Chinese platforms to shape global trade, and more significantly, to export standards of Internet governance as Chinese platforms like Alipay, Didi Chuxing, and WeChat become global players.

Indeed, the behavior of US tech giants reveals the increasingly prominent role that Chinese government regulations are playing. Consider the example of the 2017 Wuzhen World Internet Conference, a global conference organized by the Chinese government to discuss Internet products and policy. Governments and corporations from around the world send representatives there—if they can get in. In 2017, US government representatives were invited and chose not to attend. Like US decisions to step back from the Trans-Pacific Partnership, skipping China's World Internet Conference signals that the United States is stepping back from participation in global technical governance organizations, even as participation is becoming more important for the future of the United States politically, economically, and militarily. Executives from major US corporations, by contrast, waited for approval from Chinese organizers to attend, and could not just buy tickets.

Compounding the decision to step back from regional governance organizations is the US government's decision to step back from technical leadership in areas ranging

from cybersecurity to data localization to digital sovereignty. The United States has taken an increasingly siloed approach to Internet governance, relying heavily on private corporations to secure their own data and the military to handle military cybersecurity, while doing little to bridge the gap between civilian and military data security or infrastructure regulation. By contrast, as we have seen, China is establishing clear new frameworks for data storage and security that impact private corporations, Chinese state-owned enterprises, and government agencies operating in China and globally.

The United States has not always been so passive in technology policymaking. For many years, it was criticized for being overly dominant in the field of Internet governance. The Internet Corporation for Assigned Names and Numbers (ICANN) relied on US government resources to assign domain name servers to global Internet infrastructure. The US Defense Advanced Research Projects Agency (DARPA) was a driving factor behind the development of the Internet in the first place. However, in the intervening years following the Omnibus Trade and Competitiveness Act of 1988, the United States began following a strategy focused on encouraging private investment, limiting public investment, and opening emerging markets (Hughes 2005). China, in contrast, has taken a far more active role in shaping the direction of Chinese technology policy. *Made in China 2025* offers a template for Chinese corporations and government entities to drive national development goals.

The intersection of US corporate and Chinese corporate and governmental interests is shaping the direction of the global media and technology industries. With the emergence of China's ever-growing market and bureaucratic framework, we are seeing increased patrolling by Chinese regulators of platforms, as well as the increasing global influence of China's data storage and circulation practices. As shown by the case of Apple's maneuvers in the context of China's new Internet governance frameworks, the patrolling of platforms around the world is becoming the domain of powerful corporations and authoritarian governance.

Chinese Internet standards and data security practices are shaping the Chinese domestic Internet landscape. However, through the power of China's market, they are also creating norms for US firms seeking to enter China's market. By examining the ways in which US media and technology firms interact with Chinese regulations, as well as with Chinese corporate partners as a means to navigate those regulations, it becomes possible to better understand how Chinese national security concerns are shaping the development of the technology industry not only in China, but in the United States as well.

List of References

Apple Newsroom. 2017. "Tim Cook's Remarks at the 4th World Internet Conference." December 4. https://www.apple.com/cn/newsroom/2017/12/tim-cooks-remarks-at-the-4th-world-internet-conference-in-english/ (accessed September 28, 2018).

Arsène, Séverine. 2016. "Global Internet Governance in Chinese Academic Literature: Rebalancing a Hegemonic World Order?" *China Perspectives* 2:25–35.

Chen, Wenhong. 2018. "Big Data, Big Dream, and Big Brother: The Emergence and Growth of Chinese Big Data." International Communication Association Preconference on Data and Publics, Prague, Czech Republic.

Congressional Research Service. 2015. *US-China Cyber Agreement*. Washington, D. C.: Congressional Research Service.

DiGrazia, Kevin. 2018. "Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach." *Journal of Business & Technology Law* 13(2):255–77.

Farrell, Maureen, and Anne Steele. 2018. "Tencent Music Files for U.S. IPO." *Wall Street Journal*, October 2. https://www.wsj.com/articles/tencent-music-files-for-u-s-ipo-1538496869 (accessed October 4, 2018).

Garamone, Jim. 2018. "President Signs Fiscal 2019 Defense Authorization Act at Fort Drum Ceremony." US Department of Defense. https://dod.defense.gov/News/Article/Article/1601016/president-signs-fiscal-2019-defense-authorization-act-at-fort-drum-ceremony/ (accessed October 7, 2018).

Guowuyuan 国务院 [State Council of the People's Republic of China] 2015. *Zhongguo Zhizao 2025* 中国制造 2025 [Made in China 2025]. Beijing: Guowuyuan.

Hughes, Kent H. 2005. *Building the Next American Century: The Past and Future of American Economic Competitiveness*. Washington, D.C.: Woodrow Wilson Center Press.

Information Office of the State Council of the People's Republic of China. 2010. *The Internet in China*. White paper. Beijing: Information Office of the State Council of the People's Republic of China.

Kokas, Aynne. 2014. *Building a Transparent Web in China*. Baker Institute Policy Report. Houston, Tex.: Baker Institute for Public Policy.

——. 2018. "Chilling Netflix: Financialization, and the Influence of the Chinese Market on the American Entertainment Industry." *Information, Communication & Society*. doi:10.1080/1369118X.2018.1510534.

Office of the United States Trade Representative, ed. 2016. *U.S. Fact Sheet for the 27th U.S.-China Joint Commission on Commerce and Trade*. Washington, D.C.: Office of the United States Trade Representative.

Peters, Rachael M. 2014. "So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws." *Arizona Law Review* 56(4):1171–1202.

Quanguo Renmin Daibiao Dahui 全国人民代表大会 [National People's Congress of the People's Republic of China]. 2016. *Zhongguo Renmin Gongheguo Wangluo Anquanfa* 中华人民共和国网络安全法 [People's Republic of China Cybersecurity Law]. November 7. http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (accessed October 11, 2018).

Reddick, Christopher G., and Yueping Zheng. 2018. "Online Privacy Protection in Chinese City Governments: An Analysis of Privacy Statements." In *International E-Government Development: Policy, Implementation and Best Practice*, eds. Laura Alcaide Muñoz and Manuel Pedro Rodriguez Bolivar, 99–120. Cham, Switzerland: Palgrave Macmillan.

Russell, Jon. 2017. "AWS Isn't Exiting China, but Amazon Did Sell Physical Assets to Comply with Chinese Law." *TechCrunch*. https://techcrunch.com/2017/11/13/aws-exits-china/ (accessed September 28, 2018).

——. 2018. "Apple's China iCloud Data Migration Sweeps Up International User Accounts." *TechCrunch*. https://techcrunch.com/2018/01/11/apple-china-icloud-international-users/ (accessed April 14, 2018).

Schindelheim, David. 2012. "Variable Interest Entity Structures in the People's Republic of China: Is Uncertainty for Foreign Investors Part of China's Economic Development Plan?" *Cardozo Journal of International and Comparative Law* 21:196–234.

Schmidt, Michael S., and David E. Sanger. 2014. "5 in China Army Face U.S. Charges in Cyberattacks." *New York Times*, May 19. https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html (accessed September 27, 2018).

Selby, John. 2017. "Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?" *International Journal of Law and Information Technology* 25(3):213–32. doi:10.1093/ijlit/eax010.

Shi, Serena Y. 2014. "Dragon's House of Cards: Perils of Investing in Variable Interest Entities Domiciled in the People's Republic of China and Listed in the United States." *Fordham International Law Journal* 37:1265–1308.

Wortzel, Larry M. 2014. *The Chinese People's Liberation Army and Information Warfare*. Carlisle Barracks, Pa.: United States Army War College Press.

Yue, Clarice, Sven-Michael Werner, Michelle Chan, and John Shi. 2017. "China Cybersecurity Law Update: Critical Information Infrastructure in China—Any Clarification?" Bird & Bird, February 6. https://www.twobirds.com/en/news/articles/2017/china/cyber-security-law-update-critical-information-infrastructure-in-china-any-clarification (accessed September 29, 2018).

Zhang, Cinder Xinde, and Tao-Hsien Dolly King. 2010. "The Decision to List Abroad: The Case of ADRs and Foreign IPOs by Chinese Companies." *Journal of Multinational Financial Management* 20(1):71–92. doi:10.1016/j.mulfin.2010.04.001.