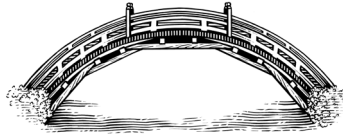


BOOK REVIEW ROUNDTABLE

Aynne Kokas's  
*Trafficking Data:  
How China Is Winning the Battle for Digital Sovereignty*  
New York: Oxford University Press, 2022  
ISBN: 9780197620502



*Emily S. Weinstein*

*Kendra Schaefer*

*Paul Triolo*

*Aynne Kokas*

## Assessing a Range of Approaches to Data Privacy and Security

Emily S. Weinstein

Comparing the U.S. and Chinese systems is always a dangerous game. For decades, scholars have tried to piece together and pick apart ways to compare and contrast the political and economic inner workings of these two countries to gain a better understanding of how they can (or perhaps cannot) work together. As a result, several assumptions have emerged that I believe have blinded U.S. policymakers from seeing shortcomings in our own system. As an example, the March 2023 congressional hearing on TikTok could have been time spent asking important questions about social media and privacy, particularly as they relate to minors; instead, it mostly devolved into an ill-informed spectacle, with policymakers asking if TikTok was listening to Americans via their home Wi-Fi. There are genuine concerns about how social media companies and other firms that have access to large swaths of data are keeping this data safe and secure, but these concerns are not isolated only to data in China.

In *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*, Aynne Kokas argues that the movement of data, particularly from the United States to China, threatens digital sovereignty around the world (p. 2). She coins this movement “data trafficking,” as it is often done without the express consent of citizens or in a fuzzy, extralegal way that the legal systems in question have yet to address. In this book, Kokas finds an effective way to show how both the United States and China are taking advantage of and failing to protect their citizens’ data. In the context of China, this is a no-brainer. The world has become intimately familiar with China’s problematic data practices thanks to coverage of TikTok and widespread surveillance tactics in Xinjiang and elsewhere, and U.S. policymakers are working frantically to address these issues. Few pay attention, however, to how similar practices may be playing out within our own borders, and Kokas does an excellent job of shedding light on this problem. Moreover, she dispels some long-standing assumptions about good and bad policy by demonstrating the strengths and weaknesses of both the Chinese and U.S. approaches to data regulation.

---

EMILY S. WEINSTEIN is a Research Fellow at Georgetown University’s Center for Security and Emerging Technology (United States). She is also a Nonresident Fellow at the Atlantic Council’s Global China Hub and at the National Bureau of Asian Research. She focuses on U.S. national competitiveness in artificial intelligence and machine-learning technology and on U.S.-China technology competition. She can be reached at <emily.weinstein@georgetown.edu> or on Twitter <@emily\_sw1>.

While reading Kokas's book, I kept returning to the question of whether allowing your government to have access to all your data is a bad thing that infringes upon personal liberties. This assumption has been prevalent across U.S. discourse for decades now, particularly in cases that Kokas highlights like the leaks by Edward Snowden (p. 17), which arguably caused more societal uproar than instances in which companies have lost or misused U.S. citizens' personal data. In contrast to countries like China, where the government asserts control over almost all public and private data, Kokas describes the fragmented and piecemeal approach that the U.S. government, at both the federal and state levels, has taken to regulating data and the fact that much of this responsibility is left to the private sector to shape as it sees fit (pp. 26–40). The decentralized U.S. approach to data regulation has not been all bad, but it has left us in a messy place. Many in the United States tend to assume that, because of what we see happening in China regarding data sovereignty and regulation, any attempts to regulate the flow or use of data will lead us down a slippery slope to authoritarianism.

In the United States, we have operated under the assumption that less political oversight will breed more innovation, and in many cases this has proved to be true. The emergence of Silicon Valley is just one of many examples of the benefits of our historically hands-off approach to technology and innovation, and Kokas asserts that the openness of the U.S. system has indeed made it a more welcoming environment for capital investment and innovation from around the world (p. 26). However, she astutely points out that this openness—often exalted as our greatest strength—brings with it several vulnerabilities that countries like China have and can continue to take advantage.

Much of *Trafficking Data* is spent comparing and contrasting the U.S. and Chinese approaches to data across different sectors, including social media, gaming, finance, healthcare, and home security. Throughout these different case studies, Kokas provides solid evidence to demonstrate how a lack of movement on the part of the United States has allowed China to take advantage of things we previously viewed as strengths. In her discussion of social media, she points out that the openness of the U.S. tech sector in permitting Chinese tech companies to operate in the United States—thereby granting them the ability to mine U.S.-based consumers' data and develop algorithms that draw on that user engagement—may provide Chinese firms with a competitive advantage over U.S. counterparts (p. 114). In the healthcare sector, openness in the context of free markets allowed the acquisition of Complete Genomics by Chinese firm BGI in 2013; here, the

lack of regulatory barriers to inbound investment likely helped kick-start BGI's eventual global dominance in genomic data sequencing (pp. 164–65). Similarly, in home appliances, China-based Haier's acquisition of GE Appliances in 2016 increased its global market dominance, which, as Kokas points out, offers several key advantages for both Haier and the Chinese government, particularly in the realm of soft power (p. 179).

In analyzing China, Kokas argues that its more proactive approach to managing consumer data may offer lessons: “Chinese laws treat data generated by companies and by users as valuable resources and rightly consider data as central to the future of economic growth, national security, and long-term autonomy” (p. 209). This is not to say that the Chinese approach to data regulation or privacy is good or better than that of the United States. On the contrary, it is clear to most policymakers and scholars outside of China that the Chinese system itself, as well as its growing influence globally, promotes illiberal digital practices. However, this does not mean that the U.S. approach is any better at protecting citizens from data trafficking. Neither system is perfect, and the evidence presented in *Trafficking Data* demonstrates this repeatedly. Countries around the world—regardless of their political systems or institutions—are grappling with how to regulate data, as the results will have massive implications for the future of economic competition, military competition, civil liberties, and beyond. As we all consider the next steps for regulating data, I believe that Kokas has provided an effective and comprehensive foundation upon which U.S. policymakers can build a better understanding of our strengths and weaknesses and eventually craft smarter policies. ♦

## An Excellent Point Lost in Execution

*Kendra Schaefer*

In *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*, Aynne Kokas does what so many books addressing China's data governance regime fail to do: she urges U.S. policymakers to “look to thine own house first.”

This book's key argument is that the failure of U.S. policymakers to pass federal, cross-sector legislation protecting the data of U.S. citizens leaves the door open for any malicious actor—state-sponsored or otherwise—to abuse and exfiltrate it. Without a federal data privacy law or a centralized, cross-agency, and cross-sector framework for oversight of data security, U.S. government bodies seeking to protect the privacy of their citizens from competing countries are left combating threats on a whack-a-mole, case-by-case basis, which is both ineffective and ultimately unsustainable. *Trafficking Data* successfully draws attention to these important issues and highlights a multitude of gaps in the current U.S. policy approach that are worthy of consideration by policymakers.

However, *Trafficking Data* is less successful in accurately describing the nuances of China's data and network policy, the mechanisms through which the Chinese state and private actors collect and employ data, and the structure and functions of the Chinese government. The result is that the specific nature of the threat presented by data trafficking may be misrepresented.

One such misrepresentation made repeatedly is that China's 2017 Cybersecurity Law requires “Chinese or foreign firms operating in China [to] legally store their data in Chinese government-run servers” (p. 4, also pp. 51 and 209). For example, the book notes:

Beyond online user content, corporations face restrictions that prevent them from privately storing the data they generate. China's 2017 Cybersecurity Law asserted that all “critical information” should be controlled by Chinese state-owned data centers, thus structuring it as part of the national security apparatus. The law required the transfer of all such data, both

---

**KENDRA SCHAEFER** is a Partner at the Beijing-based strategic advisory consultancy Trivium China and a Nonresident Fellow at the National Bureau of Asian Research (United States). Based in Beijing from 2002 to 2022, Ms. Schaefer leads Trivium's technology policy research team, keeping investors, companies, and governments briefed on Chinese technology regulation. Her team focuses on data, artificial intelligence, semiconductors, digital infrastructure, censorship, platform companies, and bleeding-edge technologies. She is also Chief Editor of the Trivium Tech Daily newsletter. She can be reached at <ks@triviumchina.com> or on Twitter <@kendraschaefer>.

government and commercial, to Chinese-government-run servers (p. 65).

However, this is a misinterpretation and simply not the case. Neither in the text of the Cybersecurity Law, nor in that of other Chinese data laws and regulations, does there exist a stipulation for companies—even those operating critical information infrastructure—to place commercial data on servers administered by the state. The Cybersecurity Law and subsequent cybersecurity acts, such as the Data Security Law and Personal Information Protection Law, do require some companies handling certain types of sensitive data to implement tight security protocols on networks, store user data collected in China within China, and submit to cybersecurity inspections by Chinese state agencies, but the servers on which that data is stored can be (and often are) privately owned.

The book further states that under the Cybersecurity Law, U.S. firm Tesla was forced to place its data on government-run servers. The articles referenced for this information indicate that Tesla established a data center in Shanghai to comply with Chinese regulations on the local storage of sensitive information (such as personal information and geographic data collected by smart cars), but they also note that there is no information available in terms of where and how that data is hosted.<sup>1</sup>

Two separate issues are likely being conflated here: First, that China's data governance regime requires certain companies collecting large amounts of personal and other information that is deemed sensitive by the state to store that data locally and to apply for licenses to export it. Second, that rules laid out by the Ministry of Industry and Information Technology essentially restrict data center providers and cloud service providers with more than 50% foreign ownership from applying for an operational permit.<sup>2</sup> The result of these rules is that foreign data center companies and cloud

<sup>1</sup> Sebastian Moss, "Tesla Opens Data Center in Shanghai, China," *Data Center Dynamics*, October 25, 2021 ~ <https://www.datacenterdynamics.com/en/news/tesla-opens-a-data-center-in-shanghai-china>; and Trefor Moss, "Tesla to Store China Data Locally in New Data Center," *Wall Street Journal*, May 26, 2021 ~ <https://www.wsj.com/articles/tesla-to-store-china-data-locally-in-new-data-center-11622015001>.

<sup>2</sup> "Gongye he xinxi hua bu guanyu qingli guifan hulanwang wangluo jie ru fuwu shichang de tongzhi" [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 (PRC), January 22, 2017 ~ [https://www.miit.gov.cn/jgsj/xgj/wjfb/art/2020/art\\_ac2095b32d054e22a03e8154c3a44d50.html](https://www.miit.gov.cn/jgsj/xgj/wjfb/art/2020/art_ac2095b32d054e22a03e8154c3a44d50.html); and "Gongye he xinxi hua bu guanyu fabu 'Dianxin Yewu Fenlei Mulu (2015 nianben)' de tonggao" [Notice of the Ministry of Industry and Information Technology on Issuing the "Catalogue of Telecommunications Business Classifications (2015 Edition)"], Ministry of Industry and Information Technology (PRC), December 28, 2015 ~ [https://www.miit.gov.cn/zwglk/zcwj/wjfb/tg/art/2020/art\\_e98406cd89844f7e92ea1bcf3b5301e0.html](https://www.miit.gov.cn/zwglk/zcwj/wjfb/tg/art/2020/art_e98406cd89844f7e92ea1bcf3b5301e0.html).

service providers must partner with a local Chinese data center to operate within China, although there are no stipulations requiring the partner data center to be state-owned. Indeed, there are many examples of foreign companies choosing privately owned Chinese data centers as a partner. Microsoft, for example, has partnered with privately held VNET/21Vianet for offering Microsoft 365 services, and Amazon Web Services partners with privately held Sinnet Technology.<sup>3</sup> Apple, however, was widely criticized for agreeing to partner with a state-owned firm to store its Chinese user data.<sup>4</sup>

*Trafficking Data* makes additional claims that misrepresent or misinterpret the source documents cited as evidence. For example, the source of the statement “The Chinese social media platform WeChat censors content according to Chinese government standards even for users outside of China” (p. 80) is a 2020 Citizen Lab report in which Citizen Lab conducted in-depth experiments on how WeChat monitors and blocks sensitive communication for users within and outside of China.<sup>5</sup> This report explicitly found that communication between users outside of China on Chinese social media platforms was not censored, but that the transfer of files, such as PDFs and images, between users outside of China was monitored and used to bolster the censorship regime for users within China. Although that is problematic for a host of reasons, it does not necessarily constitute long-arm censorship.

Many of these issues may be due to the book’s overreliance on English-language media sources. For instance, based on incorrect reports by foreign media, *Trafficking Data* indicates that China’s social credit system profiles citizens by leveraging data submitted to private-sector apps, including data from dating profiles and payment platforms (pp. 56, 61).

---

<sup>3</sup> Dan Swinhoe, “SpaceDC to Partner with Centrin Data in China,” Data Center Dynamics, March 8, 2022 [~ https://www.datacenterdynamics.com/en/news/spacedc-to-partner-with-centrin-data-in-china](https://www.datacenterdynamics.com/en/news/spacedc-to-partner-with-centrin-data-in-china); Amazon Web Services, “What’s New: Announcing a Broader Operating Relationship between Amazon Web Services and Sinnet,” August 21, 2016 [~ https://www.amazonaws.cn/en/new/2016/announcing-operating-relationship-between-aws-and-sinnet](https://www.amazonaws.cn/en/new/2016/announcing-operating-relationship-between-aws-and-sinnet); Microsoft, “Microsoft Azure Operated by 21Vianet,” August 5, 2020, <https://learn.microsoft.com/en-us/azure/china/overview-operations>; and “21Vianet Group Inc.,” Securities and Exchange Commission, Form F-1 Registration Statement, Registration no. 333, April 4, 2011 [~ https://www.sec.gov/Archives/edgar/data/1508475/000119312511088222/df1.htm](https://www.sec.gov/Archives/edgar/data/1508475/000119312511088222/df1.htm).

<sup>4</sup> Jack Nicas, Raymond Zhong, and Daisuke Wakabayashi, “Censorship, Surveillance and Profits: A Hard Bargain for Apple in China,” *New York Times*, May 17, 2021 [~ https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html](https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html).

<sup>5</sup> Jeffrey Knockel et al., “We Chat, They Watch: How International Users Unwittingly Build Up WeChat’s Chinese Censorship Apparatus,” University of Toronto, Citizen Lab, Research Report, no. 127, May 2020 [~ https://citizenlab.ca/2020/05/we-chat-they-watch](https://citizenlab.ca/2020/05/we-chat-they-watch).

This is a common misconception.<sup>6</sup> The confusion is understandable, as poor reporting on social credit abounds, and the scholarship surrounding such a complex mechanism is difficult to decipher. However, China's social credit system, while indeed an expansive data-collection effort, only currently aggregates data held by government agencies—such as tax payment history and past penalties for legal violations—and was not designed to monitor citizens' social behavior using data pulled from private apps, such as online dating matches or purchases on e-commerce platforms. The widespread misinformation on social credit has been a source of frustration for social credit scholars for half a decade, as it informs perceptions of the Chinese state as an all-seeing techno-dystopia. The truth about social credit is, fortunately, much less exciting. Similar inaccuracies abound throughout this book.


All this may sound like hair-splitting. Storing data within China certainly places that data more closely within the reach of the Chinese state. In practice, even privately owned data center companies in China over a certain size are often connected to local governments, state-owned companies, or state-backed investment vehicles. The Chinese government has, without a doubt, prioritized control over domestic data flows and has taken steps toward influencing international data flows. However, nuance matters. As *Trafficking Data* rightly notes, when it comes to assessing the risks that China's data regime poses to international data flows and infrastructure networks, "there are both concrete concerns and hyperbolic threats. Carefully sorting through the risks is essential to both the credibility of policymakers and the protection of users" (p. 84). As such, "hyperbolic 'China threat' discourse creates gridlock that makes it even more important to consider the specific mechanisms through which China is using data to enlarge its sovereign footprint" (p. 91).

---

<sup>6</sup> Kendra Schaefer, "China's Corporate Social Credit System," Trivium China, November 16, 2020 ~ [https://www.uscc.gov/sites/default/files/2020-12/Chinas\\_Corporate\\_Social\\_Credit\\_System.pdf](https://www.uscc.gov/sites/default/files/2020-12/Chinas_Corporate_Social_Credit_System.pdf); Vincent Brussee, "China's Social Credit Score—Untangling Myth from Reality," Mercator Institute for China Studies, February 11, 2022 ~ <https://merics.org/en/comment/chinas-social-credit-score-untangling-myth-reality>; Jamie Horsley, "China's Orwellian Social Credit Score Isn't Real," *Foreign Policy*, November 16, 2018 ~ <https://foreignpolicy.com/2018/11/16/chinas-orwellian-social-credit-score-isnt-real>; Zeyi Yang, "China Just Announced a New Social Credit Law. Here's What It Means," *MIT Technology Review*, November 22, 2022 ~ <https://www.technologyreview.com/2022/11/22/1063605/china-announced-a-new-social-credit-law-what-does-it-mean>; Zeyi Yang, "How China's Social Credit System Actually Works—It's Probably Not How You Think," *South China Morning Post*, January 7, 2023 ~ <https://www.scmp.com/magazines/post-magazine/long-reads/article/3205829/how-chinas-social-credit-system-actually-works-its-probably-not-how-you-think>; and Cindy Yu, "Mythbusting the Social Credit System," *Spectator*, June 13, 2022 ~ <https://www.spectator.co.uk/podcast/social-credit-system>.



Sadly, *Trafficking Data* may perhaps inadvertently contribute to just such a hyperbolic China threat discourse by glossing over the gaps between what we fear may happen and what has actually happened. This is worth considering since the book targets U.S. policymakers, many of whom are currently debating bans on Chinese technologies and are all too eager to accept such claims without fact-checking the footnotes. The answers to these questions—whether the Chinese government leverages its censorship apparatus beyond its own borders, whether and how the state accesses and uses private-sector data, and whether (and to what extent) the state leverages data collection and aggregation to control its citizens—will impact geopolitical relations and foreign policy for years to come. Although there is widespread suspicion among U.S. policymakers that China intends to (or already has) maliciously leveraged digital tools in such ways, there is thus far only a small body of concrete, credible evidence to undergird such fears, making it difficult for policymakers to develop a sober assessment of the state of play.

These issues are unfortunate, as they distract from the fact that Kokas is making an argument that very much needs to be made: that is, the United States has thus far failed to formulate robust data protections for its citizens, act as a global leader on data policy issues, write rules that govern the collection of data by firms inside the United States, and participate strategically in international forums. All these shortcomings create national security risks for U.S. citizens and may, in the end, unnecessarily cede a strategic advantage to China. While I applaud *Trafficking Data* for tackling this complex and critical topic, the book would have benefited from greater nuance and review of these complicated issues. 

## Trafficking in Assertions on Data in China Lacks Explanatory Power

*Paul Triolo*

The issue of China and data, including Chinese government access to data, has become one of the most discussed topics in U.S.-China relations. News on this issue seems to emerge on a daily basis—whether it is the Montana governor banning TikTok, claims that Chinese drones are sending data back to Beijing, or headlines claiming that China is blocking outbound data flows due to national security concerns.

In her new book *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*, Aynne Kokas offers a sweeping view of the data landscape and its nexus with China, from TikTok to WeChat to the Digital Silk Road. There is much to say about the evolution of China’s data governance, which has progressed substantially since its Cybersecurity Law was enacted in 2016 and implemented in 2017, as well as about successful Chinese apps such as TikTok and WeChat. While well-researched in places, the book, like many articles on China and data, makes initial assumptions, and then builds theories of risks on top of a largely unexamined set of theses about the Chinese government, its ability and intention regarding data handling, and how it interacts with private-sector companies that dominate the data space in China.

Kokas seems to accept, somewhat uncritically, that the Chinese government demands and can access all data collected and processed by Chinese technology platforms. The book also argues that the Chinese government seeks to put together bits of information from different Chinese and Western sources under the concept of “mosaic theory,” which holds that such data points, when taken together, present risks to individuals or companies (see p. 147). Both of these approaches assume that China has grand designs to control all data and leverage it for nefarious ends. But on closer examination, the validity of building further constructs upon these assumptions looks quite dubious.

The standard assessment of China’s national security and intelligence laws (including the Cybersecurity Law) as mandating companies to turn over data to the government is inaccurate on several levels (see p. 120).

---

PAUL TRIOLO is a Senior Associate with the Trustee Chair in Chinese Business and Economics at the Center for Strategic and International Studies (United States). He can be reached at <ptriolo@albrightstonebridge.com> or on Twitter <@pstAsiatech>.

The language of these laws is vague, and while they do mention cooperation on national security–related issues, they say nothing about releasing bulk data to the government on demand. Additionally, the Chinese government has never published implementation regulations for the national security or intelligence laws.

A detailed review of China’s evolving data governance approach reveals much more nuance than is presented in the book. For example, among the concerning parts of China’s Cybersecurity Law, Article 28 states that “Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.”<sup>1</sup> This vague language, which is similar to language in the 2015 Counterterrorism Law and National Security Law, does provide an opening for the government to compel companies to collaborate with intelligence services and law enforcement.<sup>2</sup> However, it is not clear that “technical support” means turning over encryption keys or actual real-time data or other data monitoring by the security services mentioned in the text of the law.

Broad assertions about China’s Personal Information Protection Law (PIPL) mandating that all private data be controlled by the state and that Beijing aspires to weaponize data as a strategic state resource and be the world’s data broker—lines of argument that are not made in the book but are often made by Western pundits—are less helpful in gauging what these laws mean for companies operating in China’s complex data space. Instead, it is useful to keep in mind two government/party goals behind China’s new data regimes that are driven primarily by domestic objectives. One is related to data security and is designed to protect Chinese data from foreign government extraction and access. Another is mapping the data held by large technology platforms—mainly domestic internet platforms—and what harm or good could come from that data. Any discussion of China and data must deal with the primarily domestic focus of all regulatory efforts.

The details here matter, and broad statements in the book such as “Chinese government policies allow regulators to maintain an iron grip

---

<sup>1</sup> National People’s Congress of the People’s Republic of China (PRC), “Cybersecurity Law of the People’s Republic of China,” passed November 7, 2016, effective June 1, 2017, trans. Rogier Creemers, Graham Webster, and Paul Triolo, DigiChina, June 29, 2018  $\approx$  <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017>.

<sup>2</sup> National People’s Congress (PRC), “Counter-Terrorism Law of the People’s Republic of China,” adopted December 27, 2015, amended April 27, 2018, trans. China Law Translate, December 27, 2015, <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015>; and National People’s Congress (PRC), “National Security Law of the People’s Republic of China,” July 1, 2015, trans. China Law Translate, July 1, 2015  $\approx$  <https://www.chinalawtranslate.com/en/2015nsl>.

both at home and abroad on these firms and their data” (p. 3) are not clearly backed up by evidence, nor is it clear what they mean in practice. For example, in China, as in some other jurisdictions such as the European Union, there are different regulations around personal data and nonpersonal data. In the case of TikTok, for instance, the most sensitive data is actually in the videos created by users, and this data is freely available to anyone with access to the app.<sup>3</sup> The idea that TikTok videos would be useful for developing profiles that could be used by the Chinese government to recruit someone is fanciful and not the way governments and intelligence agencies pursue recruitment efforts. The book implies that this could be part of a data-trafficking problem, but is much less explicit about how realistic or beneficial this type of data harvesting would be to Chinese intelligence services, for example. In general, however, it does an excellent job of laying out the challenges posed to regulatory and national security authorities by an app such as TikTok (see p. 7 and p. 102).

When some of these facts are recounted by those watching China’s evolving data governance regime up close, the typical response of some China watchers is that it does not really matter because the government can always get access to people’s data. The book does not imply this or explore that assertion. But the assumptions behind such thinking, let alone the technical processes and resources involved if it were even partially true, are seldom examined and warrant consideration. All governments theoretically have access to any personal data held by private-sector companies via legal channels and law-enforcement requests. This type of access happens every day in the United States, the EU, and China, each of which has a markedly different legal system. Large Chinese domestic companies that hold the most data on Chinese citizens, such as Alibaba, Tencent, and ride-sharing leader DiDi, must abide by legal requirements for law-enforcement access.

The reality is that the Chinese government has the same access to data as other law-enforcement agencies around the world. The difference is that in China, the Chinese Communist Party (CCP) may decide to investigate an individual for crimes that may not be considered crimes outside of China. Though this claim is not made in the book, Western commentators typically see this as the CCP overriding any legal constraints, but, due to lack of data, the scale of this activity remains largely unclear. In addition,

---

<sup>3</sup> Milton Mueller has written an excellent critique of the national security arguments around TikTok. See Milton L. Mueller and Karim Farhat, “TikTok and U.S. National Security,” Internet Governance Project ∞ [https://www.internetgovernance.org/wp-content/uploads/TikTok-and-US-national-security-3.pdf?\\_gl=1\\*1bxckwm\\*\\_ga\\*MjAxNjMwMTAwOC4xNjg0ODUwMzQ1\\*\\_up\\*MQ](https://www.internetgovernance.org/wp-content/uploads/TikTok-and-US-national-security-3.pdf?_gl=1*1bxckwm*_ga*MjAxNjMwMTAwOC4xNjg0ODUwMzQ1*_up*MQ).

there is some evidence that major platform players, such as Tencent, delete personal information within a certain time window due to concern over provisions in the EU's General Data Protection Regulation (GDPR) and to avoid supplying data as part of government requests.

One of the central issues of China's evolving data governance regime is the advanced framework being developed under the Data Security Law (DSL) and PIPL, and the book would have benefited from a deep dive into these issues. The rich literature around these laws is critical to understanding the evolving Chinese government approach to data governance, both from the perspective of data control and from the government's intention to leverage data as the "fifth factor of production."<sup>4</sup> There are no specific new authorities, for example, in the DSL and PIPL regime that provide expanded Chinese law enforcement or security services access to data held by companies.

Although the Chinese authorities are becoming more assertive in demanding companies share data, these demands are primarily motivated by economic objectives—such as the monitoring of electric power and water supplies—and less about mosaic theory. Still, some analysts point to Xi Jinping's moves to assert control over data as a strategic asset as evidence that the more opaque regulations in the DSL and PIPL will be implemented in the worst-case, most far-reaching scenario. That view is understandable; however, it is also highly subjective. Such is the case with the following statement:

By permitting pervasive data gathering, they also sap consumers' will to resist such invasions of their privacy. Social media platforms, online games, and payment apps, as well as a wide range of connected devices and infrastructure, can produce enhanced data sets accessible to the Chinese government that synthesize everything from video to speech and beyond. Applications in artificial and augmented intelligence, surveillance, bioengineering, and a host of other emerging technologies lay the foundation for long-term economic power (p. 7).

It would have been helpful if the book had clearly defined which part of the Chinese government is doing the acting, which organizations are

---

<sup>4</sup> See, for example, Alexis Lee et al., "China's Draft Privacy Law Adds Platform Self-Governance, Solidifies CAC's Role," DigiChina, May 3, 2021  $\approx$  <https://digichina.stanford.edu/work/chinas-draft-privacy-law-adds-platform-self-governance-solidifies-cacs-role>; Rogier Creemers, "China's Emerging Data Protection Framework," *Journal of Cybersecurity* 8, no. 1 (2022)  $\approx$  <https://academic.oup.com/cybersecurity/article/8/1/tyac011/6674794tyac011>; and Dehao Zhang, "China: The Interplay between the PIPL, DSL, and CSL," OneTrust DataGuidance, April 2022  $\approx$  <https://www.dataguidance.com/opinion/china-interplay-between-pipl-dsl-and-csl>.

synthesizing the data as well as to what end, and which companies are laying the foundation for long-term economic power. Without getting into specifics about how companies and technology platforms—the main actors in China’s data economy—are leveraging data and how this is benefiting the Chinese government and China’s overall economic power specifically, broad generalizations about “China and data” lack any real explanatory power, but they do sound ominous, particularly to those uninitiated in the complexities of China’s evolving data governance regime.

Finally, the book does not tackle the issue of how China’s data governance could intersect with a host of regional trade regimes that China is already a part of (such as the Regional Comprehensive Economic Partnership), is in the accession process for (such as the Digital Economy Partnership Agreement), or aspires to join (such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, or CPTPP). This is an important part of the data governance picture, and while the author does mention the CPTPP, the book would have benefited from a comprehensive discussion of this intersection. Chinese officials, for example, contend that China’s data governance regime and provisions like the DSL and PIPL are flexible enough to allow China to meet the requirements of the CPTPP regarding data, which are the gold standard for digital trade. Chinese companies such as Alibaba, Huawei, and others have internal data protection offices and claim that their data practices align with global best practices in markets where they operate, such as the GDPR.

The book would have benefited from a serious and nonideological analysis of how China is currently participating in plurilateral and multilateral data regimes and how these might influence its data governance regime going forward. Although China’s data governance is different from that of other countries, there is no “data corpus” under construction in China that is likely to allow Beijing to gain some strategic advantage. In the end, data trafficking is an interesting concept, but big tech such as Google, Facebook, Apple, and ByteDance hold far more data and have better resources to use it for profit than any government organization in China could likely conceive. ◆

## Author's Response: Reactions to *Trafficking Data* Reflect Debates about Global Data Security Risk

Aynne Kokas

Global data governance is highly fragmented, and policy debates about it reflect intense disagreements about the expected role of corporations, the state, and civil society. The impact of data governance practices remains unsettled both within and across nations. Most central to these policy debates, and at the core of how new technologies develop domestically and internationally, is the notion of what constitutes risk and how best to prevent or mitigate it—by either taking a precautionary approach to data governance or attempting to abate data governance problems once they occur. I feel fortunate to engage in this debate. A major focus of my book *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty* is on how the United States, China, and other developed digital economies perceive and respond to risks differently. Whereas *Trafficking Data* urges a precautionary approach, the reviews of this book reflect the robust debate about when and how to address the risks inherent in our increasingly digital world.

I want to thank Emily S. Weinstein, Kendra Schaefer, Paul Triolo, and *Asia Policy* for the opportunity to engage on the book's themes with thinkers from the academic research, consulting, and think tank worlds. The issues that *Trafficking Data* raises concern many people, from journalists and regulators to investors and everyday citizens. Writing about U.S.-China relations in the current moment presents a challenge due, at least in part, to heightened domestic tensions in both countries. Using critiques of the United States' data governance system first, followed by critiques of China's approach, *Trafficking Data* argues that both approaches exploit users in their own distinctive ways. Indeed, interactions between the tech and data oversight practices of China and the United States present a worst-case scenario for users globally.

---

AYNNE KOKAS is the Director of the East Asia Center, an Associate Professor of Media Studies, and the C.K. Yen Chair at the Miller Center at the University of Virginia (United States). She is the author of the award-winning book *Hollywood Made in China* (2017). Her newest book, *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*, received the IPPY Award for Best Book in Finance and Investment from the Independent Publishers Association, was a medalist in the Axiom Business Book Awards globalization and international business category, and is on the long list for the 2023 International Convention of Asian Studies Best Books in Social Science. She can be reached at <ak3ff@virginia.edu>.

One area of seeming agreement among all three reviewers and the book is the importance of more comprehensive data oversight in the United States. Disagreement about what this might look like and the appropriate level of risk underscores one of the central points of the book and, indeed, in contemporary debates about data governance: Should countries follow an approach based on risk regulation or precautionary principles when responding to data gathering, integration, and movement?<sup>1</sup> That is, does it make more sense to prepare for potential harm or to make policies that respond to harms that have already occurred or are knowable? This is not just a difference among specialists on China's tech policy; it is a raging debate among tech analysts more broadly. Policymakers that rely on the precautionary principle, which is most common in European lawmaking, do not wait for harm to happen or for uncertainty to be resolved.<sup>2</sup> Rather, this approach recommends, at minimum, to avoid inaction on potential risks and, at maximum, to regulate "until it is clear that there is no danger of serious harm."<sup>3</sup> In Japan, Australia, India, and other U.S. allies and partners, there are also clear policy efforts in place to address risks of data transfer with precaution. In contrast, risk-based regulation, which is more common in the U.S. context and responsible for the current U.S. regime of surveillance capitalism, is more accepting of both known and unknown risks in exchange for economic and social benefits.<sup>4</sup> In the book's introduction, it is no coincidence that I discuss data trafficking in relation to climate policy, one of the areas that pioneered precautionary policymaking. In climate policy, Europe, Japan, Australia, and other U.S. allies and partners have also taken a different path from the United States, acting to protect their citizens from risks rather than waiting for those risks to materialize before pursuing mitigation.

This debate between precautionary and risk-based regulation in data oversight is at the core of not just U.S.-China tech relations but how the United States and other countries respond to a whole host of new technologies, from generative artificial intelligence to bioengineering, in which risks are significant but unpredictable. Although I appreciate points from two of the reviewers that the full risks posed by China's extensive

---

<sup>1</sup> Jale Tosun, "How the EU Handles Uncertain Risks: Understanding the Role of the Precautionary Principle," *Journal of European Public Policy* 20, no. 10 (2013): 1517–28.

<sup>2</sup> *Ibid.*

<sup>3</sup> Margot E. Kaminski, "Regulating the Risks of AI," *Boston University Law Review* 103 (forthcoming, 2023), available from SSRN, August 19, 2022, 23 ~ <https://doi.org/10.2139/ssrn.4195066>.

<sup>4</sup> *Ibid.*



domestic and extraterritorial data governance have not yet been realized, the key point articulated in chapter 3 of *Trafficking Data* is that China's laws are vague and have wide-ranging implications for potential harm. As Triolo notes:

The language of these laws is vague, and while they do mention cooperation on national security-related issues, they say nothing about releasing bulk data to the government on demand. Additionally, the Chinese government has never published implementation regulations for the national security or intelligence laws.

The nebulousness of the idea of “cooperation on national security-related issues” and lack of implementation regulations in these Chinese laws are precisely why it is important for other countries to develop robust domestic regulations when considering data oversight from the perspective of the precautionary principle. Triolo further notes the vague language in China's Cybersecurity Law:

For example, among the concerning parts of China's Cybersecurity Law, Article 28 states that “Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law.”<sup>5</sup> This vague language, which is similar to language in the 2015 Counterterrorism Law and National Security Law, does provide an opening for the government to compel companies to collaborate with intelligence services and law enforcement.<sup>6</sup> However, it is not clear that “technical support” means turning over encryption keys or actual real-time data or other data monitoring by the security services mentioned in the text of the law.

Schaefer concurs with Triolo's assessment that it is difficult to pin down precise risks for policymaking, noting that this makes it “difficult for policymakers to develop a sober assessment of the state of play.” This is exactly right. Even if we acknowledge the value of risk-based policymaking to mitigate risk and maintain openness, as Triolo points out, the vagueness of Chinese policies makes it nearly impossible to accurately assess risk.

---

<sup>5</sup> National People's Congress of the People's Republic of China (PRC), “Cybersecurity Law of the People's Republic of China,” passed November 7, 2016, effective June 1, 2017, trans. Rogier Creemers, Graham Webster, and Paul Triolo, DigiChina, June 29, 2018  $\approx$  <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017>.

<sup>6</sup> National People's Congress (PRC), “Counter-Terrorism Law of the People's Republic of China,” adopted December 27, 2015, amended April 27, 2018, trans. China Law Translate, December 27, 2015  $\approx$  <https://www.chinalawtranslate.com/en/counter-terrorism-law-2015>; and National People's Congress (PRC), “National Security Law of the People's Republic of China,” July 1, 2015, trans. China Law Translate, July 1, 2015  $\approx$  <https://www.chinalawtranslate.com/en/2015nsl>.

Thus, we see the precautionary vs. risk-based philosophical disagreement in tech policymaking.

The reviewers' critiques of *Trafficking Data* further underscore the complexity of tracking these risks, even for experts. Schaefer's discussion of whether transnational censorship exists on WeChat demonstrates how difficult such risk is to assess. Schaefer points to the Citizen Lab report "We Chat, They Watch" to argue that there is no evidence of Chinese censorship outside China: "This report explicitly found that communication between users outside of China on Chinese social media platforms was not censored."<sup>7</sup> But the report also notes that China-registered accounts (those under WeChat's Chinese terms of service) include all accounts that were originally registered to phone numbers in mainland China. According to the report, these accounts "fall under these terms of service, and they remain under them even if the user later links their account to a non-Chinese phone number" and are also subject to "pervasive political censorship."<sup>8</sup> Thus, WeChat accounts of users who establish accounts in China and later change them to numbers outside China are, according to the Citizen Lab report, subject to censorship outside China. This would include, for example, foreign students, immigrants, and businesspeople who first download WeChat in China but switch phone numbers after moving from China—WeChat's main use case. Such fluidity underscores how invisible data trafficking can be camouflaged amid the dark forest of corporate terms of service.

In chapters 4 through 9 of *Trafficking Data*, I articulate how the integration of data-gathering capabilities in the U.S. commercial economy presents a wide range of long-term risks. These include the risks Weinstein focuses on in her review, such as enhanced competitive advantages for Chinese firms in strategically important emerging industries, ranging from communications to health to connected devices. In chapter 4, the book details the cost and security risks presented by the investment of ChemChina-owned subsidiary Syngenta in the U.S. precision agriculture sector,<sup>9</sup> whose whole-farm management system AgriEdge managed over 10.5 million acres of arable U.S. land in 2021 (p. 85). Such infrastructure

---

<sup>7</sup> Jeffrey Knockel et al., "We Chat, They Watch: How International Users Unwittingly Build Up WeChat's Chinese Censorship Apparatus," University of Toronto, Citizen Lab, Research Report, no. 127, May 2020, 8, <https://citizenlab.ca/2020/05/we-chat-they-watch>.

<sup>8</sup> *Ibid.*

<sup>9</sup> As of July 19, 2023, Syngenta was approved for, but had not yet undergone, an initial public offering on the Shanghai Stock Exchange.

investments cannot simply be unwound if the Chinese government chooses to fully exercise its power over Chinese companies. Rather, they would require costly, complex replacements that impose their own risks.

As *Trafficking Data* details throughout the book, tech and data regulation in the United States exemplifies the failures of this risk-based approach to data governance. This was clear in the TikTok congressional hearings in March 2023, which Weinstein aptly terms an “ill-informed spectacle,” regardless of how we may agree or disagree about the risks and implications of data gathering on the app. One area of seeming agreement among the reviewers is that waiting until the risks of a technology have become fully realized—after it has been fully integrated into international corporate and social ecosystems—is not a time in which most countries, and, in particular, the United States, will be successful in implementing effective policy solutions or responses.

Indeed, the sharp divergence of the reviewers’ responses about where to draw the line in this debate underscores why critical analysis of transnational data governance is so important for U.S. policymakers and the public. *Trafficking Data* argues for precaution when moving forward with robust data trade with China due to the lack of transparency in Chinese laws and the lack of protections in the United States. But having this roundtable debate allows for important consideration of how the United States assesses and manages risk as U.S. regulations diverge from those of its allies and partners. As new data-driven technologies emerge to further challenge global norms for tech regulation, they bring with them new risks as well, both on their own and as part of relations with China. ♦