
Chris Bronk, Ph.D.
University of Houston

Follow this and additional works at: https://digitalcommons.usf.edu/jss
pp. 126-128

Recommended Citation
DOI: https://doi.org/10.5038/1944-0472.16.2.2142
Available at: https://digitalcommons.usf.edu/jss/vol16/iss2/9

This Book Review is brought to you for free and open access by the Open Access Journals at Digital Commons @ University of South Florida. It has been accepted for inclusion in Journal of Strategic Security by an authorized editor of Digital Commons @ University of South Florida. For more information, please contact digitalcommons@usf.edu.
This summer, the big action blockbuster in the People’s Republic of China is “Born to Fly,” a film about Chinese test pilots laboring to produce stealth combat aircraft able to meet their American adversaries on equal terms. It marks another shift in Sino-US relations, in offering the People’s Republic of China’s view on decline in the relationship. “Born to Fly” calls out the United States as an enemy, much as Top Gun clearly identified the Soviets as the bad guys. The movie fits well into the framework established in her first book, which made compelling arguments as to how US film companies, cognizant of potentially massive box office earnings in China, toned down anti-China story lines. Hollywood’s acceptance of non-hostility towards China produced at least one completely unbelievable film, MGM’s remake of John Milius’s “Red Dawn,” in which Chinese invaders were reimagined as North Koreans late in production. Amusingly, the 2012 “Red Dawn” reboot never appeared on Chinese movie screens.

Beginning her academic career with Hollywood Made in China, the aforementioned study of China’s influence on the American film industry, she somewhat unexpectedly shifted to Internet and social media issues. She’s gone from the scholarship regarding feature films to TikTok videos and the enormous troves of data collected from apps and platforms developed by Chinese firms such as AliBaba and Tencent. Moving away from film, Kokas, a professor in media studies at the University of Virginia, recently released her second book, Trafficking Data, which covers topics of international relations and information issues in a manner superior to much scholarship in political science. She covers an enormous topic, but never does so in a manner that could be dismissed as breezy.

While movie studios fretted about upsetting the Chinese market, China scholars like Dr. Kokas were largely shut out of the country both physically and virtually. One of the aphorisms of constructivist scholarship that I will paraphrase is that international relations scholars go to the places they
study, learn the language, eat the food, and ride the train. By going to China and researching it so completely, Dr. Kokas has earned her stripes as a fully qualified scholar of it. That she has published a book so critical of Beijing’s leadership should be alarming, as she would be only the most reluctant of China hawks. As her career has evolved, she has witnessed a massive change in how she can engage in China scholarship. She admits, “Beginning with Chinese president Xi Jinping’s ascent to power in 2012, the politics of access to China for international scholars have shifted dramatically...As Chinese government laws overseeing online conduct become more stringent and extraterritorial, they constrain how researchers can safely conduct their work.” Whether blocked by entry to travel at the visa window or online access to China by its national level firewall, scholarship on China has been truncated mightily in only a few short years.

What Dr. Kokas shows the reader is that China’s rise as a data power comes with a large stack of attendant baggage. In the 1990s, the world worried about the monopolistic power of Microsoft. More recently Google and Facebook, both re-badged as Alphabet and Meta, have been concerns to data activists and regulators alike. *Trafficking Data* clearly illustrates that whatever our concerns regarding American technology giants might have been, Chinese technology companies are likely far more worrisome. The rise of Chinese state-managed hyper capitalism coupled with the obsession on market growth for domestic firms to connect with global audiences has created an environment in which, “Chinese tech platforms serve as a vehicle for economic statecraft.” She rightly observes that Beijing exerts massive influence on its tech companies, and offers healthy subsidy, while US firms in the same sector largely avoid government oversight and regulation.

And herein lies the problem. While US tech companies have profited enormously from Shoshana Zoboff’s “surveillance capitalism,” China’s government may ultimately convert the proceeds of such activity undertaken by Chinese firms to national power. Among the many things we learned from Edward Snowden’s massive leak of state secrets is that no direct line from Facebook or Google’s servers existed at the time, but rather the US National Security Agency came up with clever schemes to collect intelligence data from them. Kokas understands the imperfection of the US system as well as the extension of government control, first
identified by Milton Mueller, of data being stitched into the framework of sovereign territory. Two decades ago, alarm bells rang on data being routed through the United States for intelligence purposes. Today, there is concern on packets of data from Zoom calls winding up on servers in China, even when the participants are located anywhere but China.

Perhaps the greatest contribution Kokas makes with *Trafficking Data* is in explaining Chinese data politics. Nearly two decades ago, at a global cybersecurity summit, the head of China’s industry and information technology ministry made reference to “our Internet” several times in his remarks. Was this a global Internet that we all shared or a Chinese Internet of which he spoke? With time we have come to see an answer. Inside its borders, China has erected the edifice of a surveillance state unlike anything we have seen outside it. It is one where the forces of economic activity, including surveillance capitalism, intersect with the interests of state control. Kokas asserts, I believe correctly, that, “Through the combined power of Chinese corporations and the Chinese government’s data governance regulations, China exerts a level of control over users that Silicon Valley can only imagine.”

We now live in a world where the Sino-US relationship has not reached its bottom and has precious few guardrails. There is an unwinding of the vision for shared prosperity and serious talk of economic decoupling. Aynne Kokas’s *Trafficking Data* offers a superb assessment of how soft power and the power derived from the collection and analysis of user data intersect. While security studies may ponder the possibility of China and the US being insnared in Thucydides trap, there is a much more immediate concern of how China may collect, aggregate, analyze, and disseminate data to harm other actors on the global stage. One of the answers to the Chinese data problem Kokas offers is in data stabilization, an approach to rebalancing state and corporate power regarding personal data. Stabilization, she offers as a middle path between “unbridled capitalism” of the sort found in Silicon Valley and restrictive national controls of the sort seen in the People’s Republic of China. This middle path, she hopes, will ensure, “openness with guardrails, supporting individual users, equitable trade, and national security.” Let us hope so.