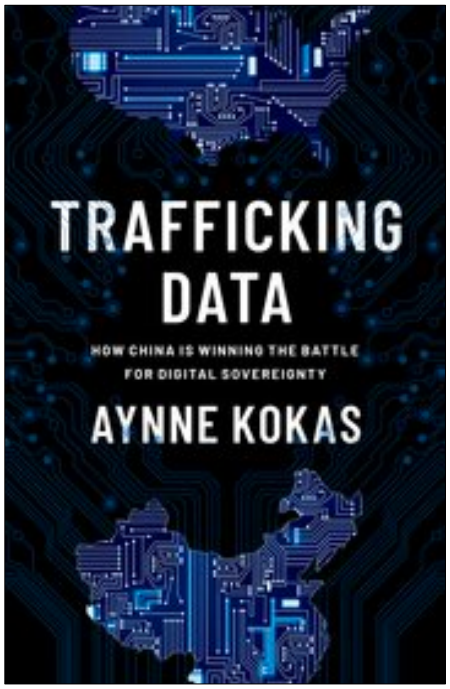
International Journal of Communication 18(2024), Book Review 1718–1720 1932–8036/2024BKR0009

Aynne Kokas, **Trafficking Data: How China Is Winning the Battle for Digital Sovereignty,** New York, NY: Oxford University Press, 2022, 340 pp., $29.99 (paperback).

Reviewed by
Jing Zeng
Utrecht University



Trafficking Data: How China Is Winning the Battle for Digital Sovereignty by Aynne Kokas critically examines the intersection between soft and hard power in this data-driven age. This timely work employs data as its entry point, delivering an insightful overview of the dynamics and complexities inherent in the enduring power struggle between two economic giants.

The book invites readers to envision the consequences of exploitative data practices that extend beyond personal privacy concerns. It encourages readers to contemplate how the gathering and use of consumer data could potentially erode democracy and sovereignty within their own country. In the book, Kokas offers astute accounts of corporate practices, national legal frameworks, and consumer exploitation fostering the transnational flow of data, from the United States to China. Kokas describes this process as *data trafficking*. What is data trafficking, and why is it the best lens to employ for the book? Kokas carefully answers these questions in chapter 1. Rather than using a neutral term, such as "data transfer," Kokas deliberately uses the word "trafficking," as it implies "the abuse of power and positions of vulnerability, the trading of benefits to achieve consent, and coercion and deception" (p. 10). Data trafficking is a normatively loaded concept, which serves Kokas well for delivering a variety of normative accounts about how the Chinese government seeks to "erode digital sovereignty in the US" (p. 75).

While seeming to single out China as the preeminent threat to American digital sovereignty, Kokas does not shy away from laying blame at the feet of the U.S. data regulatory framework and the profits-above-all Silicon Valley corporate model. In chapter 2, Kokas succinctly describes the current state of play in which the pursuit of profits, a culture of self-governance, and a fragmented, politically vulnerable, and ineffective system of checks and balances within the U.S. tech industry leave U.S. consumers vulnerable to exploitation by China's state apparatus. This starkly contrasts with China's digital governance and technological expansion approaches. As Kokas describes in chapter 3, the Chinese regulatory framework "defines data as a national asset through laws, principles, specifications, policies, and plans" (p. 60). The author highlights that this control also extends to U.S. firms wishing to tap into the Chinese market. The state of affairs Kokas outlines echoes other contemporary observations of what may be referred to as an "authoritarian advantage" over more open, pluralistic systems of governance. By focusing on the Chinese government's sovereignty framework, Kokas convincingly sheds light on how data gathering has been prioritized, legitimized, and manifested as a high-priority agenda within the country. The tangible outcome

of this vigorous data sovereignty scheme is what Kokas describes as the "national data corpus" (p. 73), which is aggregated from within and beyond its borders.

One strong contribution of the book is Kokas's detailed account of the various digital realms vulnerable to data trafficking. In chapters 4 through 9, Kokas presents concrete cases spanning a diverse array of sectors and platforms, ranging from agriculture to public health and from TikTok to Fortnite. These illustrative instances serve to underscore the risks associated with the expansion of China's tech sectors and capitals into the United States. Despite the thorough detailing of each case study, what could be more convincingly articulated is evidence and examples illustrating the malign activities a rival government with unfettered access to the U.S. consumer data may wish to undertake and how it is more worrisome than what could be done with foreign people's data in the hands of the U.S. government.

However, the author did not merely depict a dystopian world with undermined U.S. national security and agency-less U.S. consumers being exploited by Chinese tech firms. In chapter 9, Kokas concludes the book with a cogent proposal for better securing U.S. data in the face of known and evolving risks (from China). To mitigate the risks of data trafficking, Kokas posits that, instead of implementing data localization, the most feasible solution to the issues expounded upon in her book is *data stabilization*. Kokas aptly cautions that data stabilization should not be viewed as a panacea for resolving all the challenges outlined in the book but rather as "a mechanism for managing an overwhelming challenge" (p. 192). It represents a balanced approach, positioned somewhere between unbridled capitalism and data nationalism, and requires working toward a comprehensive framework for stable global data migration or "openness with guardrails" (p. 205). Kokas provides a toolkit comprising strategic "wedges" designed to bring this concept to fruition. The realization of these strategies necessitates legislative changes, the involvement of supranational governing bodies, and active participation from the financial and education sectors. This she admits will not be easily implemented because of the entwined natures of tech products in our societies and is mired in political disagreement.

The rapid digitization of information and the ubiquity of interconnected technologies have ushered in an age where data has emerged as a valuable and transformative asset. As businesses, governments, and individuals alike harness the power of data-driven insights, the ethical, social, and political dimensions of this phenomenon come under scrutiny. In light of this backdrop, there is a pressing need for critical scholarship on procedures through which data is harvested, commodified, and governed. With a particular focus on transnational and geopolitical aspects of data practices, Kokas's work makes a timely and strong contribution to ongoing debates.

While the book primarily centers on China and the United States, the cautions, prognoses, and solutions it offers are not only applicable but also highly relevant when discussing politically driven transnational exploitation of data in broader contexts. In prior scholarship on data colonialism and digital imperialism (Couldry & Mejias, 2019; Kwet, 2019), researchers seek to draw postcolonial and decolonial insights to interrogate datafication in a translational context. Kokas's data trafficking can foster complementary insights when implemented to scrutinize exploitive data practice from a geopolitical perspective.

One premise of the book, at least as implied by the title, is that the United States and China are engaged in a "war" (the author uses a softened version of the term—"battle") for global supremacy across several fronts, and that, in the case of digital sovereignty, China currently has the upper hand. It is worth viewing this narrative in light of a larger conversation around the "rise of China" and the "new cold war" rhetoric that is seen as politically expedient within both countries. Kokas, herself a China scholar, alludes to past episodes of Western concern over the intentions of inscrutable oriental powers—the Japan panic of the 1980s as one such example. The opening chapter of the book also provides a brief critique of the "China threats" discourse, citing Pan Chenxing, describes them as a "self-fulfilling prophecy" (p. 5) and mentions its impact in fostering anti-Asian sentiment. This points to an awareness of not wishing to ride a wave of unfounded paranoia. Again, some more convincing evidence of the tangible risks to security would help allay such criticisms.

Rivalry is a prominent theme in the book, but achieving what Kokas outlines as data stabilization necessitates cooperation among nation-states. In this regard, what can be productive and beneficial is discussions that foster trust and cooperation. Throughout the book, Kokas draws comparisons between climate change and data trafficking. Let us continue with this analogy. Just as with climate change, it is not solely about "U.S. vs. China"; it is about "U.S. and China," along with many other countries, inspiring, motivating, and learning from one another. Just like climate change, it is not a zero-sum game.

References

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking Big Data's relation to the contemporary subject. *Television & New Media, 20*(4), 336–349. doi:10.1177/1527476418796632

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class, 60*(4), 3–26. doi:10.1177/0306396818823172