BOOKS *et al.*

Data inflow and outflow are regulated differently in different jurisdictions, affecting what we see online.

POLICY

Data geopolitics

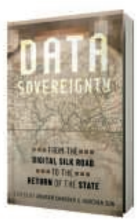
A group of scholars explore the implications of how governments control and restrict digital information

By **Dov Greenbaum**

In an era of escalating global polarization, when jurisdictions enforce data sovereignty, imposing governance or control over the data produced within their borders, "the news you see, the facts you see, and even the maps you see change depending on where you are," observes legal scholar Mark Lemley (*1*). And with the expanding role of artificial intelligence in society, constraints on access to the data on which such technologies are trained can have severe and systemic ramifications.

In their timely tome *Data Sovereignty*, editors Anupam Chander and Haochen Sun aim to provide a comprehensive understanding of this issue. The book is divided into four parts, covering digital sovereignty basics, the intersection of technologies and institutions with data sovereignty, trade regulations related to data flows, and issues specific to data localization.

A central challenge concerning the analysis of data sovereignty is the absence of a precise definition for the term. The editors assert that data sovereignty encompasses the data protection laws, competition laws, and security laws designed to control aspects of data both within and beyond a territory. They describe this concept, deemed both "necessary and dangerous," as the "exercise of control over the internet" serving as a protective barrier against both foreign states and corporations.



Data Sovereignty: From the Digital Silk Road to the Return of the State
Anupam Chander and Haochen Sun, Eds.
Oxford University Press, 2023. 408 pp.

Compared with its relatively positive reception in the Global North, data sovereignty is often perceived in the Global South as "the government hijacking the Internet to protect itself," write Chander and Sun. In acknowledging that data sovereignty is both a necessity for democratic government and a potential tool to "immunize oppression," they contend that digital sovereignty ought to be operated within a framework of checks and balances.

Governments are often motivated to invoke data sovereignty by at least three considerations: a desire to protect citizens from illegal content and from having their content illegally usurped, a desire to promote their jurisdiction's own technology, and a desire to control populations by limiting access to incoming and outgoing data streams. Throughout the book, many of the chapters look to the four most prominent stakeholders in the area of data sovereignty: China, the European Union, the United States, and global industry leaders.

Colloquially known as the "Great Firewall of China," Chinese infrastructure and regulation showcase extensive state control over the inflow and outflow of data. Additionally, exported Chinese internet infrastructure seeks to project this sovereignty worldwide. The European Union employs regulations to principally control foreign technology firms. In what has been called the "Brussels effect," the EU aims to use its regulatory oversight to expand its influence beyond its immediate territory.

Meanwhile, the United States projects soft power through "functional sovereignty" mediated by its dominant technology and social media companies. Within the US itself there has historically been minimal government control over data flow owing to the country's concentration of corporate powers, its expansive speech protections, the nature of its intellectual property laws, its relatively weak privacy laws, its ineffective domestic regulatory bodies, and the severe limitations placed on corporate regulation imposed by international groups.

Unencumbered by governance, private US corporations that make the market and manage data can thus also promote and censor information as they see fit, setting up what philosopher Luciano Floridi has referred to as a clash "between companies and states" (*2*). Growing recognition of this problem has led to bipartisan support for the idea that the internet ought to be more heavily regulated before it undermines democracy. Although the book mentions some of the legislative efforts that have been proposed, given the speed of change in this area, this analysis is already somewhat dated.

Individual citizens ought to also have control over their personal data ("self-sovereignty"). However, this control, when it is granted and ostensibly managed through consent and oversight, is frequently illusory because even seemingly insignificant bits of information can be used to deduce highly private details as a result of advances in data processing and artificial intelligence.

Ultimately, this volume provides an insightful exploration of data sovereignty, shedding light on the multifaceted challenges and opportunities that lie ahead in the evolving landscape of data governance. ■

The reviewer is at the Zvi Meitar Institute for Legal Implications of Emerging Technologies and Harry Radzyner Law School, Reichman University, Herzliya, Israel, and Department of Molecular Biophysics and Biochemistry, Yale University, New Haven, CT, USA.
Email: dov.greenbaum@aya.yale.edu

REFERENCES AND NOTES

1. M. A. Lemley, *Duke Law J.* **70**, 1397 (2021).
2. L. Floridi, *Philos. Technol.* **33**, 369 (2020).

10.1126/science.adm9960

PHOTO: OLEG BLOKHIN/ISTOCK PHOTO