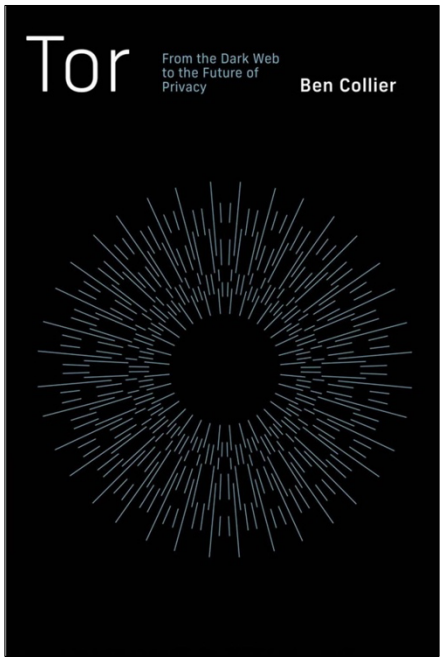
International Journal of Communication 19(2025), Book Review 3403–3405 1932–8036/2025BKR0009

Ben Collier, **Tor: From the Dark Web to the Future of Privacy**, Cambridge, MA: MIT Press, 2024, 242 pp., $40.00 (paperback).

Reviewed by
Min Wang
Wuhan University, China[1]



Ben Collier's ***Tor: From the Dark Web to the Future of Privacy*** offers a "biography" of one of the digital age's most paradoxical technologies: the Tor anonymity network, which uses onion routing to anonymize Internet traffic by routing it through multiple layers of encryption and volunteer relays. Collier demystifies this often-misunderstood backbone of the so-called *Dark Web* by tracing its origins, purposes, and transformations under long-term study. For this project, Collier draws on over two decades of source material, including design documents, mailing-list archives, and interviews with Tor's developers, activists, and users. Published by MIT Press, the book arrives at a critical moment: Global debates over encryption, online harms, and digital sovereignty are on the rise. As authoritarian regimes tighten control over digital dissent and democracies struggle to balance cybercrime enforcement with civil liberties, Tor emerges in Collier's account as both a lifeline for dissidents and a lightning rod for controversy.

Several audiences will find Collier's book valuable. Communication and media scholars will appreciate its analysis of the politics of digital infrastructure, surveillance, and activism. Policymakers and regulators can gain insights into why Tor persists despite its association with crime. Practitioners and activists in digital rights advocacy will recognize a thorough account of the social work that keeps Tor operational. Designers, developers, and everyday Tor users (some of whom Collier interviews) will find their experiences reflected in the narrative. Even general readers interested in digital culture and the "Dark Web" beyond sensational headlines will find Collier's clear, jargon-free account accessible.

In structure, Collier's book reads like a cultural biography of Tor, framing the network as a lens on the contested politics of privacy and surveillance. He traces the conceptual roots of what he calls "privacy worlds" (p. 9) and recounts the competing visions of Internet infrastructure that shaped Tor's invention in the 1990s. Subsequent chapters explain the design of onion routing, the emergence of volunteer Tor "maintainers," and the network's institutional growth through partnerships with NGOs such as the Electronic Frontier Foundation. Collier then examines Tor's contested reputation as a host of the

[1] This research was supported by the Humanities and Social Science Fund of Ministry of Education of China "Categorized and Classified Protection of Personal Information in Facial Recognition Technology Use" (Grant No. 22YJC860027).

"Dark Web" (p. 123) and its adoption by activists and journalists as a tool for evading censorship. He details the unlikely convergence of U.S. naval researchers and hacker-activists (the Cypherpunks) that gave rise to Tor in that era. Collier also discusses internal conflicts, notably the Appelbaum scandal, which exposed tensions among activists, libertarians, and maintainer communities. The final chapter, titled "Privacy Futures" (p. 194), explores Tor's uncertain trajectory amid debates over technical integration, anticensorship innovation, and competing activist visions of its future.

A key theoretical contribution of the book is to reframe Tor as a social infrastructure rather than merely a technical system. Collier adopts a science and technology studies perspective, portraying Tor as a sociotechnical system shaped by struggles over values and control. In doing so, he extends scholarship on anonymity, surveillance, and network culture. For example, Collier's historical approach complements Robert Gehl's (2018) analysis of legitimacy in anonymous networks by showing how Tor's legitimacy was contested among diverse actors—from U.S. military sponsors to libertarian hackers to civil society advocates. Bartlett (2014) popularized the imagery of an encrypted underworld of deviant subcultures, but Collier focuses on the builders, maintainers, and visionaries of the Tor community, revealing their collaborations and conflicts. In contrast to more skeptical accounts such as Levine (2018), Collier offers a nuanced interpretation: He acknowledges Tor's national security origins without reducing it to a government instrument, situating it instead within a broader historical struggle over Internet freedom and control. This approach enriches the literature on surveillance and digital resistance by bridging analyses of state power with those of grassroots technological activism.

Another strength of Collier's book is its conceptual innovation. He introduces terms that help readers rethink privacy infrastructures. The notion of "privacy worlds" (p. 9) reframes privacy not simply as personal data control and flow but as socially constructed spaces where values and power are negotiated. Collier similarly uses the concept of a "global passive adversary" (p. 63) to describe an actor capable of monitoring all Internet traffic, underscoring why Tor's design must anticipate extreme surveillance threats. He also highlights what he calls "infrastructural politics," showing how technical systems embody ideological struggles rather than operating as neutral tools. Metaphors help make complex ideas clear, such as Collier's description of onion routing as "three layers of encryption like a Russian doll" (p. 41). Finally, he analyzes Tor's maintainer cultures, demonstrating how volunteer operators and developers form a distinct community whose norms and conflicts shape the network's legitimacy and sustainability. By combining theoretical depth with vivid analogies and clear exposition, Collier offers useful categories for studying how infrastructures enact, rather than merely protect, privacy—while ensuring readers without a computer-science background grasp the stakes.

Collier also explores privacy-policy dimensions surrounding Tor, such as government attempts to undermine encryption and the paradox that the same governments often fund Tor for censorship circumvention abroad while decrying its use by criminals at home. For example, Collier notes that U.S. government grants supported Tor to promote free Internet access in authoritarian regimes even as law enforcement agencies worried about the "going dark" problem (Weimann, 2016). The book situates Tor in key 21st-century developments—such as the Arab Spring, the rise of darknet marketplaces, and the post-Snowden surveillance era—to show Tor's double-edged nature: It has enabled both digital resistance and illicit activity. Collier remains balanced in discussing these issues, avoiding both techno-utopianism and

moral panic. He acknowledges abuses facilitated by Tor, such as cybercrime, extremist forums, and anonymous marketplaces like Ross Ulbricht's Silk Road, yet emphasizes that for every illegitimate use there are vital legitimate uses—anonymous political speech, secure communication for vulnerable groups, and so on. This even-handed approach will help scholars and policy analysts grasp the trade-offs inherent in online anonymity.

A particularly compelling insight is Collier's account of privacy as inseparable from power and politics. He observes that "privacy is deeply linked to power and politics" and provides "a framework for thinking about the creation and demarcation of different kinds of space" (pp. 9–10). This framing expands privacy debates beyond personal data management and control to the infrastructural and spatial dimensions of influence. However, Collier's view that privacy concerns and issues "rarely seem to resolve into specific instances of harm except in rare cases" (p. 9) may underestimate real-world consequences of privacy violations, such as discrimination, surveillance abuse, and repression in authoritarian regimes. In those contexts, the denial of private communication often leads to immediate harm; in democracies, the erosion of privacy under national-security pretenses can gradually reshape civic life.

In conclusion, *Tor: From the Dark Web to the Future of Privacy* succeeds in its objectives. Collier effectively bridges technical and social analysis, showing how decisions in code and architecture entwine with questions of governance, trust, and power. His lucid, engaging writing makes complex sociotechnical issues comprehensible without oversimplification. His portrayal of the Tor community is both critical and empathetic, revealing internal diversity—including tensions between those who see Tor primarily as a surveillance-fighting civic tool and those who emphasize stability or neutrality. Collier is generally sympathetic to Tor's pro-privacy mission but does not shy away from its limitations. He candidly discusses episodes where Tor came under criticism and examines how the community responded. These discussions add balance, showing that while Tor champions anonymity as a social good, it also grapples with abuse and funding challenges. A minor drawback is the book's U.S.-centric focus: Readers seeking extensive coverage of Tor's deployment in non-Western contexts or comparisons to parallel tools may find those topics less addressed. Likewise, although the final chapter gestures toward future challenges (as signaled by the title "the future of privacy"), it stops short of detailed policy prescriptions or conflict-resolution strategies. These critiques, however, do not significantly detract from the book's achievement. Collier provides readers with a rich, nuanced analysis of Tor as a privacy infrastructure—one that will shape ongoing debates about encryption, digital rights, and the nature of freedom in the digital era. In sum, Collier's book is timely, accessible, and rigorously researched, offering broad insights into privacy, power, and the evolving digital landscape.

References

Bartlett, J. (2014). *The dark net: Inside the digital underworld*. London, UK: William Heinemann.

Gehl, R. W. (2018). *Weaving the dark web: Legitimacy on Freenet, Tor, and I2P*. Cambridge, MA: MIT Press.

Levine, Y. (2018). *Surveillance valley: The secret military history of the Internet*. New York, NY: PublicAffairs.

Weimann, G. (2016). Going dark: Terrorism on the Dark Web. *Studies in Conflict & Terrorism, 39*(3), 195–206. doi:10.1080/1057610X.2015.1119546