Anthropology Book Forum
Open Access Book Reviews

JACQUELINE D. LIPTON, 2022, *Our Data, Ourselves: A Personal Guide to Digital Privacy*, Oakland: University of California Press, 224 pp., ISBN 9780520390508

Keywords: digital privacy, privacy law, US, digital marketplace, individualism

In *Our Data, Ourselves*, Lipton provides a thorough overview of digital privacy in nine domains of American life: home, work, social media, children's data, school, the digital marketplace, health, money, and the government. The book also has a chapter dedicated to digital privacy laws in the EU and a concluding chapter where Lipton ruminates on the future of digital privacy given present legal challenges. The biggest challenge is that the US has "never had – and likely will never have – strong legal privacy protections" on a federal level (197). As Lipton points out, this is problematic in the digital age, where various institutions and organizations take our personal data for scientific study, efficiency, profit, surveillance, and more. Moreover, the documents made available to us, which outline how our data is being collected and for what purpose, are often difficult to parse. For example, tech companies' terms of service (TOS) and HIPAA consent forms ostensibly exist to inform consumers yet are written in an inaccessible legal register. Lipton tackles these issues through offering detailed explanations of 1) digital privacy issues in each domain of life; 2) the pertinent laws and legal attempts that seek to address the lack of privacy protections in the US; 3) what we – as individuals – can do to protect our digital privacy and personal information. Thus, the book should be understood as a guide for *individuals* that draws on the author's legal expertise to inform people about contemporary challenges to personal privacy in the digital era.

How effective is Lipton's attempt to explain the complex legal and political terrain of privacy to the average user without a legal background? I think Lipton writes effectively in this sense, although, of course, I am reading from a standpoint of relative privilege. The main thrust of the book is clear: in lieu of a sweeping federal privacy law, privacy issues in the US are addressed through a web of state and federal legislation. Individuals' health information privacy, for

example, is protected on the federal level under the Health Insurance Portability and Accountability Act (HIPAA) (p. 144). Meanwhile, tort law – which concerns "situations where the law allows one person to sue another for causing [civil] harm" – operates on the state-level (pp. 34-35). For instance, doxing – "the gathering and publishing of private information, which may be aggregated from publicly available websites or require physical and/or digital incursions into a person's private space" – is usually addressed through tort law (p. 35). In contrast, several European countries consider privacy a basic human right through Article 8 of the European Convention on Human Rights (ECHR) (p. 131). Lipton does a fair job of defining terms, clearly describing the histories of various legislation, and outlining the implications of laws addressing digital privacy for business interests and individual freedom of speech.

Yet, Lipton's individualistic framework is limited at best and neglectful of systemic violence at worst. First, she takes the social, political, and economic factors shaping her audience's lives for granted. Reading this book as anthropologist, I got the sense that she reflected little on the inequalities among potential readers. This is particularly evident in the last section of each chapter, titled "Privacy Tips and Tricks," where she lists the steps individuals might take to safeguard their privacy in each domain. In several chapters, she recommends that people read companies' privacy policies, terms of service (TOS), and other documents pertaining to user privacy. For example, in the chapter titled "Our Data at Home," she recommends that when buying devices like Alexa or Nest Cam, readers "do [their] homework…[and] read each company's privacy policy and compare policies across companies" (p. 43). This not only contradicts the point of her book, i.e., to parse the legal register for non-legal experts, but also reflects the unrealistic expectation that people have the time and resources to sift through *multiple* policy documents. Moreover, such documents were not written to be read: companies write them to avoid liability and protect themselves from future litigation. In this way, documents like social media platforms' TOS should be understood as mechanisms to protect corporations' profit and disempower users. The book would be stronger if Lipton, at the very least, acknowledged the fact that her advice is applicable to a very thin slice of the US population: white, wealthy people who have the resources to enact her suggestions.

Second, Lipton's individualistic framework leads her to ignore systemic inequalities. While the lack of robust all-encompassing privacy protections affects everyone, it is especially a problem for marginalized communities, whose data are disproportionately misused and harvested by

corporations and the state. It is worth noting, of course, that this phenomenon is not new: surveillance technologies have long been used to control people of color in the US and colonized peoples in the "Global South" for centuries. The scale and efficiency of surveillance has only intensified in the digital age. For example, when Roe v. Wade was repealed, the commodification of cis women, non-binary, and trans men's location data when seeking reproductive healthcare became a matter of serious risk to their safety.[1] Lipton occasionally acknowledges such inequities, but she does so unevenly and in ways that neglect their systematic character. For example, in the chapter "Who Owns Our Data?" she discusses the case of Henrietta Lacks, a Black woman whose cancer cells were acquired by Johns Hopkins without her consent for cancer research in the 1950's. Lipton writes that Lacks' case constitutes "one of the more high-profile and significant unauthorized uses of a person's biological material" (p. 15) but does not acknowledge how this breach of privacy was made possible by a racist system that continues to deprive Black people of their dignity as human beings.

In sum, this book is best regarded as a reference for understanding just how little we have in the way of legal privacy protections in the US. Insofar as the book constitutes a "guide" to protecting one's privacy, however, it fails to offer any solutions that get at the root social causes of privacy issues. Lipton's lack of attention to power means that her suggestions fit squarely within neoliberal logics of individual responsibility, which is problematic in the digital economy not only because few can apply her "tips and tricks," as I pointed out, but also because it reinforces the defeatist notion that our only recourse comes from individual action. I submit, instead, that our only hope is through organizing and collective action: it is only by drawing connections between our experiences and mobilizing on the basis of this shared – albeit uneven – reality of exploitation that we can hope to protect our privacy.

Rae Jereza is a queer, Filipinx anthropologist based in the US. They are a research assistant professor and senior researcher at the Polarization and Extremism Research and Innovation Lab (PERIL) at American University. They are currently researching the hate speech/free speech dichotomy in the digital age, gun violence, content moderation, and how disabled users make

[1] Lai, Samantha and Brooke Tanner, "Examining the Intersection of Data Privacy and Civil Rights," *The Brookings Institute*, July 18, 2022, https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights/.

sense of those who question their diagnoses on social media. Geographically speaking, their work focuses on North America.