6-3-2019

Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P

John Schriner
CUNY Queensborough Community College

John Schriner
Assistant Professor
Web Services Librarian, Queensborough Community College, City University of New York

n.b. This is a pre-print. This paper is published in the Taylor & Francis journal *Internet Histories* and may be found here: https://doi.org/10.1080/24701475.2019.1623002

Book Review

Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P by Robert W. Gehl. Cambridge, Massachusetts: The MIT Press [2018]. 288pp., $30.00, Hardcover. ISBN: 9780262038263

Few books approach the dark web without leaving the reader with a mystified understanding of it. Gehl not only defines and demystifies the dark web, but through well-organized and scaffolding chapters makes *legitimacy* a central–and conceptually-loaded–theme throughout.

Gehl's approach is multidisciplinary, as he draws concepts from philosophy, software studies, digital ethnography, management studies, and other areas, to build a methodology using Adele Clarke's concept of situational analysis: this is the idea that we can map and explore heterogeneous elements that relate to one another across disparate disciplines. Gehl couples the analysis of power and legitimacy throughout with "participant observation and interviewing" *a la* digital ethnographers such as Tom Boellstorff and Gabriella Coleman.

In the introduction, Gehl makes the case for the term *dark web* instead of *deep web* or *dark net*, as he desires to keep the focus on web technologies instead of other internet services and protocols like IRC, bittorent, or email. We can then narrow the discussion to websites that are only accessible through these dark web technologies.

Organizationally, each chapter builds the case for, among other things, the importance of legitimacy in thinking about the dark web. After an introduction and detailed plan for the book in chapter 1, we move to *Violence, Propriety, Authenticity: A Symbolic Economy of the Dark Web* in chapter 2. Gehl writes "legitimacy is always about communication and power," and describes three kinds of legitimacy: the State's legitimated monopoly on violence, legitimacy as propriety–a process by which an entity satisfies stakeholders, and legitimacy as authenticity. Although clearly different, the three uses of legitimacy share traits, are socially constructed, and each involves making sense of power both in making claims to their own legitimacy and making sense of their subjugation to power. Freenet, Tor Project, and I2P have each made claims to organizational legitimacy by having administrators, budgets, and developing websites, logos, and marketing materials.

The chapter on anonymity network software development introduces us to the network builders. Gehl provides succinct histories of Freenet, Tor Project, and I2P from their beginnings. Ian Clarke, in first developing Freenet, worked to solve the problems of centralization and lack of anonymity with the world wide web. The idea of a decentralized world wide web is still discussed these days, and it's worth noting that Clarke's thesis was

written twenty years ago in 1999. Gehl describes how Freenet works to deliver static websites to users, how each user contributes to the network, and how popular sites and media are the most healthily-distributed. We trace the beginning of Tor Project through The Free Haven Project for long-term storage of anonymously-published materials that could also be read anonymously. Location-hidden services were announced in 2004 with the first website likely being the Hidden Wiki. I2P's origins lie in Lance James's desire for an anonymous Internet Relay Chat, and unlike Freenet and Tor, Gehl notes that its roots aren't in academia but in "street coders" or *hackers*.

Gehl admits his own technical limitations: "I have no training in computer science" and yet the book still satisfyingly explores technical aspects of the anonymity networks including the non-reliance on clearnet DNS, Freenet's nodes and file keys, simplified I2P tunneling architecture, and Tor network's rendezvous points for onion services (née *hidden services* as noted by the author who preferred the more common term). Carefully balancing the technical and the ontology of the dark web leaves a few problems: although many of the technologies are examined, terms like *DDoS* and *LEO* aren't defined. This may seem trivial, but when each technology has a dozen acronyms, readers new to the area will be confused.

A chapter is devoted to discussing how agorism–a market libertarian philosophy that holds that "society should be guided by market exchanges"–also guided the dark web market Silk Road. Agorism is intrinsically anti-state and the markets that were built on this philosophy must naturally work outside of the state's control. Agorism and the radical libertarian dark web community created a culture of constructive activism, and one that was meant to replace and delegitimize the state. The historical and archival texts of the Silk Road are as fascinating as the knowledge of Ross Ulbricht's double life sentence is sad. Gehl makes the case that operational security, or OPSEC, has largely replaced agorism as the dominant philosophy following the fall of Silk Road. The shift to OPSEC meant more forum threads prescribing ways to stay safe and under the radar of law enforcement, discussion of obligatory use of PGP for communications, and as the Grugq intones, being "'proactively paranoid [because] you can't be paranoid' in hindsight." OPSEC, a term with military and NSA roots, alongside paranoia, would come to define dark web markets on the day-to-day and become how relationships are structured. We learn about the OPSEC failures of AlphaBay and Hansa Market, as well as the Bitcoin escrow "exit scam" in Evolution market. We then discuss dark web markets for credit cards. To stretch the metaphor of OPSEC and vulnerability, Gehl seems to blame victims of carding for their bad OPSEC instead of the corporations that we trust to secure our financial information.

In chapter 5, Gehl discusses the quest for legitimate portals to the dark web in the form of search engines. We work through different approaches to what is acceptable content in search results from search engines like Ahmia (for Tor), AFKindex (for Freenet), and the idea of a default search engine service for I2P: to have an official or default search engine acts as a legitimacy exchange that then gives that service legitimacy.

Moving forward in chapter 6 we examine dark web social networks and the fascinating phenomenon of creating, building, and personalizing pseudonymous identities without leaving identifying information. The dark web social network is to some an answer to social networks with real name policies, invasive tracking, and commercialization. We discuss Galaxy2, technical prowess with PGP for secure communication, and misogyny consistent with chans on the clearnet. This type of malign disinhibition too often rears its head when users reveal they are female, and they are pressured to provide *more* identifying information which, of course, goes against the principles of the social network. Gehl provides a deep look into the culture of Galaxy2, candidly

interviewing an administrator as they grapple with issues of free speech and authenticity and whether Galaxy2 can be a refuge and home for those who seek it.

Perhaps the most convincing example of the trials of legitimacy are Tor Project's process for *.onion* registration and Facebook's concomitant adoption of an onion service gateway for its social media services launched on Halloween 2014. Chapter 7 is the culmination of previous discussions of legitimacy and authenticity. What started as a collaborative project with the Internet Engineering Task Force (IETF) to get six Top Level Domains (TLD) legitimated–*.i2p* and *.onion* among them–ended up with RFC 7686 which registered only *.onion* a special-use TLD, and thus integrated Tor into the "legitimate" internet. We discuss the potential collaboration and why it fell apart. The fact that Facebook created their *.onion* address helped to legitimize Tor Project and at the same time de-legitimized smaller projects like I2P and GNUnet. To illuminate this history, Gehl unearthed debate from deep in IETF mailing lists. We explore the collision of how Facebook, which is arguably the "largest identity authenticator" in the world, also provides a gateway for Tor users who tend to use it to dissociate their identity from their browsing habits. To Gehl, this represents a blurring of the dark web and the clearnet. The registration of *.onion* as a special-use TLD was expedited and likely made possible with the advocacy of Facebook.

As Gehl concludes the book, we look to how the dark web is a direct challenge to surveillance and monitoring of the clearnet. He intones that it has the potential to support social justice advocates in building anonymous networks. Of course, at the same time, white supremacist websites have moved to the dark web as they get banned from clearnet hosting. Gehl notes the work of academics like Daniel Moore and Thomas Rid who believe, given that there is so much illegal content on the dark web, we must either greatly add legitimated sites to the dark web, or the development of hidden services should cease. Do we want to continue moving in the direction of an "identified and authenticated internet" or is there a legitimate place for users wishing to protect their privacy? It's important to ask: what are we talking about when we are "enabling new political speech that is not possible in corporate- or state-monitored networks?" Gehl maintains that new political ways of thinking will emerge from the margins and they can take to the "dark web to develop their organizations and challenge the new hegemony of hate and exploitation." Gehl quotes a user of Galaxy2: "We tend to shed layers of societal convention and become closer to who we really are."

Gehl is careful to spend discussion time with each technology, but as expected, Tor dominated the discussions throughout, followed by I2P, and lastly Freenet as it's not particularly useful for dark web markets and not among the networks in the TLD discussions. It may be worth noting that something that sets I2P and Freenet apart from Tor is the fact that a user doesn't need to contribute bandwidth to other users in the Tor network to participate: in I2P and Freenet, to explore servers and content, the user volunteers their router or hard drive space, respectively. Noting that, however, in Tor, the thousands of volunteer relays worldwide and the sense of cooperation among users for a healthy network could have been discussed, as it is the backbone of the technology.

Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P presents legitimacy through thoroughly-researched and organized frames. The telling of esoteric computer science history, the use of archival text from listservs, interviews with developers and users, and concepts from varied disciplines deepen the exploration and leave the reader satiated. The chapters weave and complement each other as we struggle with legitimacy in

communication and in power.