WEAVING THE DARK WEB

Legitimacy on Freenet, Tor, and I2P

ROBERT W. GEHL

The Information Society Series

Laura DeNardis and Michael Zimmer, Series Editors

Interfaces on Trial 2.0, Jonathan Band and Masanobu Katoh

Opening Standards: The Global Politics of Interoperability, Laura DeNardis, editor

The Reputation Society: How Online Opinions Are Reshaping the Offline World, Hassan Masum and Mark Tovey, editors

The Digital Rights Movement: The Role of Technology in Subverting Digital Copyright, Hector Postigo

Technologies of Choice? ICTs, Development, and the Capabilities Approach, Dorothea Kleine

Pirate Politics: The New Information Policy Contests, Patrick Burkart

After Access: The Mobile Internet and Inclusion in the Developing World, Jonathan Donner

The World Made Meme: Public Conversations and Participatory Media, Ryan Milner

The End of Ownership: Personal Property in the Digital Economy, Aaron Perzanowski and Jason Schultz

Digital Countercultures and the Struggle for Community, Jessica Lingel

Protecting Children Online? Cyberbullying Policies of Social Media Companies, Tijana Milosevic

Authors, Users, and Pirates: Copyright Law and Subjectivity, James Meese

Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P, Robert W. Gehl

Weaving the Dark Web

Legitimacy on Freenet, Tor, and I2P

Robert W. Gehl

The MIT Press
Cambridge, Massachusetts
London, England

© 2018 Robert W. Gehl

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher.

This book was set in ITC Stone Serif Std by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data is available.

ISBN: 978-0-262-03826-3

eISBN 9780262347570

ePub Version 1.0

I wrote parts of this while looking around for my father, who died while I wrote this book. I miss seeing him sitting at his desk among his books, looking over his glasses, typing, thinking, smiling.

Table of Contents

Series page

Title page

Copyright page

Dedication

Acknowledgments

1 Introduction

2 Violence, Propriety, Authenticity: A Symbolic Economy of the Dark Web

3 The Dark Web Network Builders

4 From Agorism to OPSEC: Dark Web Markets and a Shifting Relationship to the State

5 Searching for the Google of the Dark Web

6 Being Legit on a Dark Web Social Network

7 Facebook and the Dark Web: A Collision

8 Conclusion

Bibliography

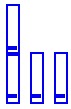
Index

List of Tables

Table 2.1 Objects, power and discursive practices, relevant social groups, and academic fields for each meaning of legitimacy

Table 5.1 Search engines across various Dark Web networks

Table 5.2 Actors and interest relations potentially mediated by Dark Web search engines



Acknowledgments

Multiple people read portions of this book and offered generous and critical feedback. Nathalie Maréchal read chapter 3 and offered copious amounts of correction to factual errors, for which I'm grateful. She's also been a great panel mate at meetings of the Association of Internet Researchers (AOIR), and I'm looking forward to reading more of her work. Megan Cullinan, Oscar Mejia, and Jeremy Freed, all PhD students at Utah, read early versions of the manuscript and helped me clarify the legitimacies. Michael Stevenson, Maria Bakardjieva, and Fenwick McKelvey, who have become great collaborators and friends, also provided lengthy feedback on the manuscript or advice at key stages. And of course, I am deeply indebted to the editors and peer reviewers at the MIT Press. Gita Manaktala, Michael Zimmer, and Laura DeNardis have been tremendously supportive of this project, and the three peer reviewers did a thorough job examining a later draft of the manuscript. One of them later revealed himself to be Nicholas John, and I am very flattered that the author of *The Age of Sharing* supported the publication of my book. The staff at the MIT Press, including Virginia Crossman, Kyle Gipson, and Susan Clark, have been wonderful to work with. Special thanks goes to Melanie Mallon who copyedited the manuscript, checking up on every link—no small task in a book about the Dark Web.

I met many of the above people through AOIR, and I need to acknowledge the support of that organization. When I'm asked about writing, I often use the cliché of the roller coaster: sometimes I'm up, and sometimes I'm down. At one very low point in writing this book, I got a surprise e-mail from AOIR informing me that my last book won that organization's Nancy Baym Book Award.

Immediately, the writing roller coaster went back up, and I returned to this manuscript with new energy. I owe a lot to AOIR for that.

I am grateful to Graham Denyer Willis, Jaime Amparo Alves, and Jim Martin for discussions at the "Policing the City" symposium at Stanford University about legitimacy, the state, and trust in online interactions. Angele Christin served as a respondent to my presentation (an early version of chapter 4) and her comments were invaluable. Firat Bozcali deserves extra praise for all the work he did making "Policing the City" a success. I also presented parts of chapter 4 to the iSchool at the University of Texas. Daniel Carter, a PhD student who arranged my trip, has my thanks, as do the faculty and students there who attended my talk. Special thanks go to the dean of the iSchool, Andrew Dillon, who expressed enthusiasm for my work, and to Casey Boyle for feedback, beer, and ramen. Finally, my gratitude goes to the Critical Genealogies Workshop, particularly Brad Stone, Perry Zurn, Colin Koopman, Andrew Dilts, and Verena Erlenbusch.

Like my previous work, this book was influenced by my friends from my time at George Mason. Professor Paul Smith once gave me a D. In a moment I will never forget, he corrected me in class when I said "legitimate use of force" by reminding me that it's "legitimate*d* use of force." Denise Albanese invited me to return to Mason to speak to the cultural studies program, where I got feedback on chapter 5 from my advisor Hugh Gusterson as well as faculty members Roger Lancaster and Tim Gibson. PhD students and alumni there, especially Fan Yang and Gavin Mueller, also provided comments. I owe a debt to Katy Razzano, who pointed out the link between state discourses of legitimated violence and nonstate, hacker appropriations of those discourses. She also allowed me to guest lecture in two of her media courses.

And, of course, I could not do this work without the support of my friends at my home university, the University of Utah. Several colleagues deserve special thanks: Kevin Coe for enthusiasm over my citation of M. C. Hammer; Avery Holton for generously helping research Twitter hashtags; Rachel Griffin for the best hallway conversations; Mike Freemole for help with computer meltdowns;

David Roh and Lisa Swanstrom for inviting me to participate in digital humanities; Michael Middleton for all he does—win; Ashley Givens for putting together the soccer team; Sean Lawson and Cynthia Love for their cooking, thinking, and friendship; and Lucas Moyer Horner for his calmness, camaraderie, and for letting me beat him at games on rare occasions. Above all others at Utah, I have to thank Kent Ono and Dianne Harris who provided career support that is increasingly rare in the academy. Their work made mine possible.

This book could not have been written without guides to the Dark Web. I found one such guide, as well as a collaborator, in G. M. H. His idea to host a literary magazine on Tor was brilliant, and I was honored to help with that project. Thanks for showing me "all things counter, original, spare, strange." I found other guides on Galaxy and later Galaxy2, some now gone, but many still active. Thanks to Lameth for doing the work of keeping that social network alive for so long. And my gratitude goes to all those who took the time to talk Dark Web with me in interviews.

More than anyone, however, I have to thank my family. My son, Teddy, was patient with me, even as I became a grumpy writer-dad. He also helped me practice soccer. My partner, Jesse: I am not sure how to thank her. My best bet is to take her on a long vacation (consider this a promise!). I wrote portions of this book while visiting my in-laws, Joe and Karen, who have treated me like a son. I wrote other parts at my mom's house. My mom taught me the importance of writing. I feel I did the best writing at her house.

Thank you, all.

1 Introduction

Truth and Light, a now-defunct Dark Web site hosted on the Tor network, had the purpose of bringing people to Christ. As the site's "About Us" page put it,

> We are a very small group of people who in one way or another have become "brothers." We all are unified in wanting to help you. It may sound strange to you but we do not know you and we want to help you. Let us prove it to you with our kindness. We have no hidden agendas. We are sick of corporations who "Grind the faces of the poor" crushing the needy and injured to get more money for themselves. We are upset with the Governments we've trusted who are more concerned with their private agendas then those that suffer underneath them.
>
> Our Purpose: Help those that need it, lift people to Christ, Build His Kingdom.

This site was a blog, soliciting questions from curious visitors. One visitor asked,

> why do you believe in what you believe in? Like, how can you just randomly believe in stuff like this??? What about proof??? Proof if it's real, or nay???

Truth and Light's response presented their theory of truth and reality:

> Is "Proof" what can be proven by science? What about conflicting scientific theories? Is proof what you can detect with your senses? Radio waves cant be detected by your senses, do you disbelieve them? To me true "knowledge" is only given from God. I realize that many people won't believe what we say, but we can make you believe that we genuinely care for you through our actions.

Another visitor asked a very different question:

> Truth and Light! I need your help I have questions! Oh so many questions! ... OK so I have been involved in the credit card game for a while during university then stopped, it was mostly centered on getting ccs from a friend that had $ money on the cards and going to a few stores, buying some stuff and selling it on kijiji/facebook etc. However now I heard that you can buy ccs from tor network WITH the pin#???

Rather than take this as an opportunity to turn this credit card fraudster on to Jesus Christ, Truth and Light offered more practical advice:

> The truth is there are no legitimate card (Credit or debit) vendors on TOR anywhere. I am sorry my friend.

This is a book about the Dark Web and legitimacy.

Of course, when I refer to the "Dark Web," or collections of websites that can only be accessed with special routing software, "legitimacy" is probably the last word to come to mind. The term Dark Web very likely evokes some decidedly illegitimate associations: drug markets, unregulated guns for sale, child exploitation images, stolen credit cards for sale, or phishing attacks. You might think of Silk Road, the infamous drug market busted in 2013, after it allegedly made billions of dollars selling everything from psychedelic mushrooms to heroin. Or you might recall the 2015 warning from James Comey, former head of the U.S. Federal Bureau of Investigation, that terrorists are "going dark," hiding their communications behind veils of encryption and anonymous routing.[1] Perhaps you think first of the Ashley Madison data dumps on the Dark Web, where personal information exfiltrated from the adultery site ended up for sale.

Associating Dark Web with "legitimacy" may seem odd, if not wrong. Or perhaps not. For each nefarious use of the Dark Web, we can find beneficial uses: the *New York Times* set up anonymous whistleblowing systems for people to point out government and

corporate malfeasance. The *Times* also mirrors its content as a Tor hidden service, as does the nonprofit news organization *ProPublica*. Political dissidents use encryption and anonymizing networks to share their ideas. Bloggers take to the Invisible Internet Project (I2P) to write about personal privacy and computer security. As Jeremy Hunsinger has noted, people use the Dark Web to share and trade knowledge about "political theory, gender studies, physics, chemistry, and engineering," knowledge that can be empowering to users and thus helps the Dark Web "gain legitimacy through the presence of this information."[2] Online communities develop open-source social networking software on Freenet to escape the confines of corporate social media giants Facebook and Twitter. And, as the quotations that open this chapter show, Christian evangelists have taken to the Dark Web to reach out and offer love to others. These sites promise access to "the real" or "the truth"—that is, legitimate knowledge.

Indeed, legitimacy can be a powerful window into the Dark Web. As I show in the next chapter, Dark Web users and site administrators, journalists and academics, law enforcement agents and dealers of illegal goods all use variations on the word "legitimacy" to describe Dark Web sites, practices, and technologies. They call certain things legitimate and others illegitimate (or, to use the parlance of the Tor- and I2P-based Hidden Answers site, "legit or sh!t"). At the core of this discernment is a trial of legitimacy, where the Dark Web's uses and meanings are under intense scrutiny by a range of social groups. This trial is more complex than a stark illegitimate/legitimate dichotomy: "legitimacy" is a highly context-dependent term, with many shades of meaning and interpretation. Along the way, declarations of something being "legit," in contrast to other, illegitimate things, mark moments of power practices.

To explore this trial of legitimacy, I focus in this book predominantly on the users and builders of Dark Web systems and sites. That is, rather than exploring how external entities (say, law enforcement agents or journalists) put the Dark Web through a trial

of legitimacy, I am more concerned with the arguments of Dark Web builders, administrators, and participants about which networks, sites, practices, and uses are legitimate. As I show throughout this book, the construction—or denial—of the Dark Web's legitimacy by network builders and Dark Web site users hinges on questions of violence, propriety, and authenticity. Specifically, I consider the Dark Web's fraught relationships with the state, the legitimated holder of the monopoly on violence; with corporate or organizational propriety and power; and with the intense adjudication of authenticity, of inclusion and exclusion. The book draws on three years of participant observation, two dozen interviews with Dark Web site admins and users, and analysis of large archives of computer science papers, e-mail lists, and Internet Relay Chat (IRC) logs, all focusing on the makers of, administrators of, and participants in various Dark Web systems.

The consideration of violence, propriety, and authenticity in relation to the Dark Web provides a model for similar analyses of networks, communication, and technology more broadly. For example, for Internet scholars, focusing on legitimacy may help illuminate how states, corporate platforms, and user practices intersect, collide, and grate against one another. Much as Truth and Light justified their Christian evangelical blog on the Dark Web, we have to attend to questions of government, corporate, and social power practices as we consider any networked technology. Likewise, this book should be useful for communication scholars reflecting on how legitimacies are rhetorically constructed through the making of claims. Finally, for sociologists of technology, thinking through these legitimacies may help illuminate how any given technical achievement is, in part, an association of coercion, resources, and social categorization.

What Is the Dark Web?

But what do I mean by the Dark Web?

Journalism, academic literature, and popular books provide competing and contradictory definitions, centering on *depth*, *morality*, and *technology*. I find only the last useful. In terms of depth, a common definition offered is that the Dark Web comprises everything that search engines (i.e., Google, Bing) have not indexed. This could include material behind paywalls or login screens, databases, web pages generated based on short-term data (think of stock quotes or weather reports), or encrypted data. When journalists or academics use this definition of the Dark Web, they tend to suggest that the Dark Web is many times the size of the regular World Wide Web.[3] Visually, they use images of icebergs or ocean depths to convey the sheer size and below-the-surface qualities of the Dark Web. This depth definition can be traced back to a 2001 white paper by Michael K. Bergman, titled "The Deep Web," in which Bergman calls attention to all the resources not easily indexed by search engines.[4] The depth approach to the Dark Web conflates Deep Web—which has been consistently defined as websites that search engines (especially Google) haven't crawled—with Dark Web, which I take to be something else altogether, especially because many search engines do in fact crawl the Dark Web (including a custom Google engine).

Second, there is a definition of the Dark Web that plays on the moral or ethical connotations of "dark," defining it as basically anything bad that happens on the web. For example, a research team at the University of Arizona sees the "reverse side of the Web as a 'Dark Web,' the portion of the World Wide Web used to help achieve the sinister objectives of terrorists and extremists."[5] The research team carries this through in their 2012 book *Dark Web*, confusingly including terrorist activities in the nonweb virtual world Second Life in the mix.[6] Journalist Jamie Bartlett's 2014 book *The*

Dark Net uses a similar definition, detailing a host of subcultural activities, such as producing pornography, seeking child exploitation images, working on cryptographic systems, and trolling, as "dark" activities.[7] In contrast to the use of icebergs and oceans, news stories using this definition tend to use images of hooded, faceless figures hunched over computer keyboards, green text on black backgrounds (a la *The Matrix*), or hands menacingly reaching through computer screens.

I reject those definitions in favor of a third, centered on technology. I define the Dark Web as websites built with standard web technologies (HTML, CSS, server-side scripting languages, hosting software) that can be viewed with a standard web browser, such as Firefox or Chrome, which is routed through special routing software packages. I do not define these sites in terms of whether Google has crawled them (the "deep" definition) nor based on the legality or morality of their content (the "morally dark" definition). The former is technically misleading, and the latter is subject to contentious debate. Moreover, the latter definition can be applied to a range of Internet technologies, including sites on the regular World Wide Web (including, as I discuss in chapter 7, Facebook).

Thus what makes the Dark Web "dark," from a technological point of view, is that to access these sites, one must route Chrome or Firefox (or other browsers) through special routing software. This is the key difference between the Dark Web and what I will call the "Clear Web," the regular World Wide Web. So, to access Dark Web sites on the Freenet network, one must be running the Freenet router. With that router running, Dark Web sites hosted on Freenet can be accessed with a standard browser via "localhost" (often the reserved IP address 127.0.0.1) with a port specified (often 8888). Accessing sites on the Invisible Internet Project (I2P) or on the Tor network can be done through similar techniques. Complicating this technology-based definition, the Dark Web is not singular but a variety of systems. This book explores three—Freenet, Tor, and I2P—but there are more, including ZeroNet and GNUnet, just to name two.

The major differentiating factor between the Dark Web and the Clear Web is that these special routing systems are designed to provide anonymity for both *visitors* to websites and *publishers* of these sites. On the Clear Web, when we visit a website, at the very least our Internet protocol (IP) address is logged. IP addresses are key tools to track users across the Internet, thus linking browsing histories to user identities. Similarly, when we visit websites, we can pretty easily figure out where they are based in geographic space, and from there we can link their contents to the identities of publishers. This is especially the case with major corporations using Extended Validation SSL certificates (which produce the HTTPS in our browsers), because these corporate sites' identities have been verified by third-party certificate authorities (more about this in chapter 7). Conversely, Dark Web technologies hide the IP address of site visitors as well as the physical location of the website publishers. As we browse Dark Web sites, information that could potentially deanonymize us is obscured. Likewise, using Freenet, Tor, or I2P, a publisher can set up a website without revealing the publisher's physical location or identity.

Thus, although Freenet, Tor, and I2P implement anonymous web technologies in very different ways, they all provide readers and publishers with anonymity by allowing them to browse and publish anonymous websites. Here, the connotation of "darkness" in Dark Web has more to do with encryption, anonymization, and leaving standard communications channels (as in the phrase used by James Comey, "going dark," meaning avoiding overly public communications channels). "Web" refers, of course, to websites, web browsers, HTML, and CSS.

Using this definition, we can see that the other definitions are flawed. The depth approach is not quite right because it presents the Dark Web as many times the size of the Clear Web. In fact, the Dark Web comprises only thousands, possibly tens of thousands, of sites —far, far fewer than the billions on the World Wide Web.[8] The repeated image of the Dark Web as the "iceberg" under the World Wide Web's "tip" is simply wrong. Moreover, accessing the Dark

Web is not quite like penetrating deeper and deeper layers of the web, each one more difficult to access than the last. To be certain, configuring browsers to use special routing software to access Dark Web sites can be daunting to new users, but such configurations and software are well documented and can be installed and running on a computer within minutes. In the case of Tor, a preconfigured version of Firefox, the Tor browser, is available for download. With the routing software in place and a bit of Googling, one can find easily find Dark Web sites to visit. Indeed, some Dark Web sites, especially multivendor markets where vendors and administrators have a financial interest in attracting a lot of traffic, are quite easy to get to and have hired publicists to get the word out about them.[9] The now-defunct Tor-based drug market search engine Grams, for example, actively made finding drug vendors simpler. Of course, other Dark Web sites, hidden behind login walls and available only to those who are vetted, are harder to access. But this is the case with the Clear Web, as well, where some sites are easy to find and access and others much harder. If anything, the Dark Web functions much like the regular web—with the key exception that one needs special routing software to access it, software that can protect the identity of site readers and publishers. It is not deeper than the regular web in any logical sense.

And unlike the moral or ethical connotations of "dark," my definition of the Dark Web as websites only accessible with special routing software does not predetermine any normative judgment about the content these sites contain. As I show in this book, many sites and services on the Dark Web would, at the very least, not rise to the level of terrorist or extremist activities, or even warrant salacious news stories. Some Dark Web sites are downright boring, providing cat facts, highly specialized computer networking technology discussions, an implementation of the ELIZA chatbot, or a means to play chess anonymously. As I describe in chapter 7, some major Internet corporations, such as Facebook, are moving onto the Dark Web. In more generous interpretations, many Dark Web sites might be judged as valuable forums of personal and

political expression, allowing political dissidents to express their views without fear of government reprisal, or enabling people to socialize without fear of corporate surveillance. To be certain, the Dark Web contains some very troubling content: stolen personal information, so-called revenge pornography, and child exploitation images, to name a few. But as Bartlett's book and the Arizona researchers show, this is the case with the Clear Web, too.[10]

All too often, the depth, morality, and technology definitions of the Dark Web get conflated into a confusing mix. Take for example Gabriel Weimann's academic article "Going Dark: Terrorism on the Dark Web," in which he argues that

> the deepest layers of the Deep Web, a segment known as the Dark Web, contain content that has been intentionally concealed. The "Dark Web" can be defined as the portion of the Deep Web that contains generally illegal and anti-social information and can only be accessed through specialized browsers. Thus, for example, the Dark Web is used for material such as child pornography, unauthorized leaks of sensitive information, money laundering, copyright infringement, credit card fraud, identity theft, illegal sales of weapons, and so on. … In 2014, journalist Jamie Bartlett in his book *The Dark Net* describes a range of underground and emergent sub-cultures, including social media racists, cam girls, self-harm communities, drug markets, crypto-anarchists and transhumanists. In recent years, the Dark Web has been moving toward more secretive locations due to the crackdown of government agencies on it.[11]

Here, Weimann mixes many of the confusing meanings of the Dark Web. To be fair, he notes it comprises websites that "can only be accessed through specialized browsers," which is somewhat similar to the definition I work with here. But he also notes that it is the "deepest layer of the Deep Web," as if we can arrange the web into such layers, and that these deep layers contain "anti-social information," playing on the moral connotations of "dark." And he

cites Bartlett's book, which studies subcultures we may or may not find morally acceptable (racists, pornography-producing "cam girls," transhumanists, crypto-anarchists), all of whom we can find on the regular web.[12] Moreover, Weimann also suggests, somewhat confusingly, the "Dark Web has been moving toward more secretive locations," again implying that there are deeper and deeper layers of the web (and that parts of the web "move" to other parts). The problem with such confusing sets of conflations is that they perpetuate the idea that the Dark Web is (a) a massive, deeper layer "underneath" the regular web; (b) comprised solely of illegal, "dark" activities; and (c) only accessible to highly skilled computer users willing to continually delve deeper into the web. It's a seductive, terrifying trope, the idea that some monstrous collection of horrifying data lurks beyond the reach of the average web user. These connotations can help sell newspapers and security research white papers, but as attractive as they are, they are wrong.[13]

So, after all this, should I even use the loaded term Dark Web? Why not Anonymous Web, Invisible Web, or Hidden Web? Or why not coin a new name? The truth is that no perfect term describes the systems I am studying, but the Dark Web term has some advantages. First, many participants on the Dark Web use the term, so it is recognizable among those whom I study, even if they also regularly argue over its definition, let alone its accuracy or desirability as a name for anonymous websites.[14] Indeed, mindful of the nefarious connotations of "dark," the Tor Project at one point hired a marketing firm to come up with a new label for anonymous Tor-based websites. The results have been mixed, however, with "onions" or "onionspace" (references to Tor's top-level domain name, .onion) being proposed but not catching on.[15] Thus, even the creators of these networks have trouble moving away from the pithy, provocative, and commonly used moniker Dark Web. Other names, such as Anonymous Web, Invisible Web, and Hidden Web, are sometimes used but have not caught on. Any name I coin would be immediately ignored by the thousands of people who use these systems. The only other terms commonly used are Deep Web and

Dark Net. I reject the first because of the reasons I give above. I don't use the second—which is arguably the most common term—because Dark Web helps narrow the focus to web technologies, as opposed to broader Internet technologies, such as IRC, BitTorrent, or e-mail protocols, which can be routed through the same network software that enables anonymous web publication and browsing. Focusing on the "Web" in Dark Web thus helps limit the scope of this book to sites marked up with HTML and presented in web browsers. Thus, even as the term brings with it some confusion, I use Dark Web (or, since I am writing about three systems, the plurals Dark Webs and Dark Web systems) throughout this book.

Methodology: Dark Web Situational Analysis

How did I arrive at legitimacy as a key lens through which to look at the Dark Web? To put it simply, I felt that the data demanded an engagement with this concept. To show the path toward my focus on legitimacy, I want to take a moment to talk about the methodology of this study. Perhaps the best guide into complex heterogeneous associations, such as the Dark Web, is Adele Clarke's excellent *Situational Analysis: Grounded Theory after the Postmodern Turn*.[16]

Clarke's emphasis is on "situations," collections of elements that, through gestalt, become greater than the sum of their parts. Drawing on Chicago sociology and mixing in the feminist scholarship of Donna Haraway, Clarke argues situations are "relentlessly relational and ecological" and must be attended to in their specificity.[17] Many elements go into any given situation: visual features, "knowing subjects," discourses, narratives, histories, technical capacities, and materialities.[18] In this, Clarke is drawing on the actor-network theory within the school of science and technology studies, which includes scholars such as John Law, Madeleine Akrich, Michel Callon, Annemarie Mol, Susan Leigh Star, and Bruno Latour. Clarke is also deeply indebted to Michel Foucault. All these scholars, from Clarke to Haraway, Law to Foucault, demand that the researcher attend to a bewildering array of objects, from other subjects to images to technical infrastructures. Moreover, rather than seeking ultimate causes for a situation, the concern is with the situation as such and the relations among its elements. As John Law puts it, instead of tracing back to causes, the researcher considers elements as "effects" of larger networks.[19]

Researching such situations is a daunting task. For Clarke, the way forward is through charting relationships between heterogeneous elements involved in a situation: discourses, visual

elements, and nonhuman elements. The goal is to answer questions such as "Who and what are in this situation? Who and what matters in this situation? What elements 'make a difference' in this situation?"[20] As researchers trace relations among these elements, they pay attention to both visibility and invisibility, presence and absence, voice and silence.[21]

To trace such relations, I draw on three main streams of data. First, I rely on Foucaultian genealogical sensibilities by exploring archives or building new ones.[22] Any student of Dark Web systems has quite a few preexisting archives to draw on, including those of developer mailing lists, IRC logs, wikis (including their version histories), code versioning systems, and online forum posts. For example, an important resource for chapter 4 is Gwern Branwen and colleagues' archive of Darknet Markets.[23] These markets are important, purposely archived sources. In addition, thousands of interactions are happening right now on Dark Web social networking sites, bulletin boards, forums, and chat systems. Some of these interactions are more or less persistent, being stored and visible on these sites for months or even years, but many are ephemeral: Dark Web sites regularly appear and then disappear after a few months or days.[24] Throughout my research, I sought to capture such items (using screenshots and Zotero web archiving) and construct my own coded archives of Dark Web interactions, but of course I missed much more than I could gather.[25]

Whether intentionally archived (as in the case of mailing lists) or archived by me or other researchers, these data provide not only a wealth of textual information, but also visual artifacts—logos, avatars, shared photos, memes—all of which could be "mapped" in the sense Clarke describes. Thus, textual and visual information combine into a multimodal form, a discourse that shapes and is shaped by social interaction and that reveals traces of power dynamics. As Clarke argues, "If knowledge is power in the Foucaultian sense, attending to the ways in which knowledges are produced, legitimated, and maintained through language/through discourse/through discursive practices becomes central in analyzing

power of all kinds."[26] Indeed, looking ahead to the key term of the book, legitimacy, power practices are a central concern, and thus I must attend to how power relations appear in these archives.

The second main stream of data for this project is drawn from participant observation and interviewing. For example, I've made accounts on dozens of Dark Web sites over three years, paying attention and in some cases contributing to the daily life of interactions on these sites. I contributed to Dark Web wiki pages, ran a blog, collaborated on a privacy policy for a social networking site, inserted Freenet files, hosted my homepage on Tor and I2P, and helped co-edit a Dark Web literary magazine. I've gotten to know key members of several Dark Web sites, and in two dozen cases, I moved from interactions "in public" (which is to say in the more "public" portions of these hidden sites) to "private" conversations and "branching and building" semistructured interviews (following, of course, principles of informed consent and confidentiality).[27]

For guidance here, I turn to the work of digital ethnographers, such as Nancy Baym, Annette Markham, Monica J. Barratt, Tom Boellstorff, Alexia Maddox, and Gabriella Coleman. Boellstorff, author of *Coming of Age in Second Life*, offers an especially invaluable methodological insight. Whereas many ethnographers seek to ground online interaction in offline identities—a move that certainly adds to the researcher's understanding of the dynamics of online interaction—Boellstorff chose to treat the virtual Second Life as a culture unto itself, deciding not to link Second Life avatars and activities to their "First Life" counterparts.[28] For the participant observation and interviewing I engaged in for this project, I did not have such a choice: as a rule, Dark Web site participants do not reveal any personal information that could be used to resolve their online identities to offline identities, because Dark Web systems provide a great deal of anonymity.[29] This is the case even for those engaged in seemingly mundane activities, such as sharing recipes or playing chess. Thus, especially in moments of informing potential interviewees about my position as a researcher seeking to publish

articles and books, I stressed that I was not seeking any personal information (age, gender identity, location, ethnicity, etc.). But, in the spirit of Boellstorff's work, interviewees still had much to offer even without anchoring their online identities in their offline identities, including insights into power dynamics, daily practices, and histories of the sites I studied.

Finally, I explored the nonhuman aspects of these networks, especially the networking software they rely on. Fortunately, the networks I consider in this book (Freenet, Tor, and I2P) are all open-source projects, which means that their source code and documentation are open for inspection and that they are built through a collaborative, iterative process.[30] And of course, to access Dark Web sites themselves, I had to download, install, run, and update these software packages on my computers, tablets, and smartphones. My engagement with this software is in many ways just as intense as my engagements with the Dark Web participants: each software package demands configuring, updating, and constant attention, especially because of the discourses about privacy and security that accompany them (in other words, the ideal is to keep the software and its dependencies up-to-date to avoid security vulnerabilities). This combination of open code, open documentation, and the experience of running software provides more data that can help me understand the Dark Web situation.

Here, I draw on insights from the field of software studies, which includes scholars such a Matthew Fuller, Anne Helmond, David Berry, and Wendy Chun. Researchers in this field consider software in layers, from operation, interface, functions, and lines of code, down to the hardware platforms on which the code runs.[31] Following Rob Kitchin and Martin Dodge, I thus paid attention to Dark Web "software as both product and process … [which] needs to be understood within a framework that recognizes the contingent, relational, and situated nature of its development and use."[32] As products, anonymizing network software packages are produced by many different types of developers, ranging from self-taught, self-described hackers to PhD-holding computer scientists specializing

in encryption algorithms, many of whom work from different locations around the world. Moreover, such software is produced through open-source practices, which include combinations of ad-hoc and formal organizational structures, control of software versions, and lively technical debates.[33] As processes, they run in the background on a computer, networking the computer with others around the world, shunting data to and fro, and shaping interaction with protocols. We can interface with them in various ways, through command lines or graphical interfaces, both of which carry certain assumptions about how end users are to be configured.[34] Thus, the Dark Web software systems described in this book offer rich insights into the power relations of this situation.

Any of these research streams on their own would, I feel, be inadequate for a wider view of the Dark Web systems discussed in this book. Taken together, however, they provide multiple layers to move across. To digest this array of data (archival, interview, and software), I've found Clarke's pragmatic, detailed approach to be extremely valuable. Her emphasis on diagramming diverse situational elements, including technologies, social groups, cultural tropes, social institutions, and debates, is a key approach I take in this book.

Pragmatic Keyword Analysis

In the course of observing, participating in, and mapping the relationships among the discursive and technical elements of the Dark Web, the curious term "legitimacy" and its variants came up again and again. As I show throughout this book (starting especially in chapter 2), this term appeared in offhand comments made on Dark Web social networking sites. The term is commonly used in markets, where new users anxiously seek to distinguish legit vendors from scammers (note its use in the Truth and Light example that opens this chapter). The term appeared in Clear Web coverage of the Dark Web, especially in reports on the efforts of law enforcement to find and shut down illegitimate websites. It appeared in comments made about changes to encryption algorithms in the code, and in comparisons between illegal and legitimate business models.

Legitimacy thus became for me what Clarke calls a "sensitizing concept" and what Colin Koopman and Tomas Matza call a "category."[35] Legitimacy became a lens with which to look at the Dark Web. And, as we will see, this is a trifocal lens—or, perhaps better, a progressive lens, as various connotations of "legitimacy" traffic into one another in a symbolic economy. Although focusing so much on this one category of inquiry may appear to limit the analysis of the heterogeneous Dark Web situation, the multivalent uses of "legitimacy" among Dark Web participants and commenters offer complex insights into power practices, social organization, and technological development, even as the concept helps narrow the focus of the book.

Thus, to consider this sensitizing concept, I turn to pragmatic keyword analysis. Here, a good guide is Nicholas A. John's excellent book *The Age of Sharing*. In his study of the word "sharing"—an important term for today's social media practices—John takes up a "pragmatic approach" from linguistics. That is, rather than asking

"What practices *should* we call sharing?," he asks, "What practices *do* we call sharing?"[36] In other words, rather than seeking to adjudicate which activities can properly be called "sharing" and which should not, John is more interested in the lively, messy, multiplicity of meanings of sharing as the term is used across various domains. In his book he considers "the sharing economy" alongside sharing one's thoughts alongside sharing a portion of one's food, with these overlapping and sometimes contradictory meanings revealing "insights into contemporary culture, and especially digital culture."[37]

John draws on the work of Raymond Williams, particularly his book *Keywords*. Based on situational analysis of Dark Web systems, from computer science paper archives, developer mailing lists, IRC logs, and thousands of forum posts, to site participant observation and interviews with site administrators and users, to lines of code and software interfaces, I came to see the term legitimacy as a keyword in Williams's sense. Much like Williams's keywords, the word "legitimacy" "virtually forced itself on my attention because the problems of its meanings seemed to me inextricably bound up with the problems it was being used to discuss."[38] This problematic word—just as slippery as "sharing"—provides a progressive lens into Dark Web practices, at one moment drawing attention to violence, then to propriety, and then to authenticity. With this concept in mind, and following the iterative process Clarke advocates for, I then returned to Dark Web sites and further refined the analysis, using legitimacy as a sensitizing lens to rethink the archival and interview data I had collected. This book is a product of these approaches.

Plan of the Book

Because this is a book about legitimacy, the next chapter, "Violence, Propriety, Authenticity: A Symbolic Economy of the Dark Web," presents three distinct meanings of that word. First is a meaning that appears predominantly in political philosophy: Max Weber's conception of a state that has made a successful claim to a monopoly on legitimated force. Thus, this meaning of legitimacy is intimately tied to violence: who can wield it and with what effects. But more precisely, it is tied to struggles over claims to the monopoly on violence in a society. The second meaning of legitimacy I address in chapter 2 is found in organizational and managerial communication: legitimacy as propriety, in the double sense of respectable behavior and proprietorship—in other words, commanding both respect and resources. Whereas the power practices of states involve violent force (military interventions or policing), for organizations, the struggle is over which organizations command what resources, and how well those claims to resources are respected by other social groups. Finally, a meaning of legitimacy not often explicitly defined can be found in streams of writing about popular culture: legitimacy as authenticity, or "legit." This form of legitimacy is tied to communities of practice, who develop—and monopolize—shared sets of symbols and languages. Whereas power at the state level can be expressed through violence, and power in an organization is often expressed through command of resources, power among the "legit" is tied to social inclusion and exclusion. After laying out these three meanings in chapter 2, I present a symbolic economy by which legitimacy is trafficked across domains, with methods such as inheritance, exchange, appropriation, purchase, and delegitimation. All the meanings of legitimacy and symbolic economic practices associated with legitimacy are tied back to statements made by Dark Web participants and commenters.

Chapter 3, "The Dark Web Network Builders," details the development history of the three Dark Web systems discussed throughout this book: Freenet, the Tor Project, and the Invisible Internet Project (I2P). I trace how each project developed networks that can anonymize both readers and publishers of web technologies. Thus, the chapter emphasizes the importance of web publishing on these networks, which was not necessarily the original intention of the network builders but nonetheless emerged quickly as the networks took shape. Web publishing on these anonymous networks became known as Dark Web publishing. I also consider the projects' places within the three legitimacies (violence, propriety, and authenticity), examining the relationship between these projects and states, the ways in which these projects appear as organizations, and the struggles over authenticity as project developers contest one another's network designs. As the chapter shows, the Freenet, Tor, and I2P projects have each engaged in complex negotiations with state power, organizational propriety, and the performative dimensions of being legit software developers who can make successful anonymous networks.

The heart of the book focuses on the specific forms of legitimacy in turn. Chapter 4, "From Agorism to OPSEC: Dark Web Markets and a Shifting Relationship to the State," takes on the relationship between Dark Web markets and state violence. Specifically, I consider a shift in thinking among Dark Web market participants about the state's claims to a monopoly on legitimated violence. The chapter starts with agorism. Agorists are radical market libertarians who believe that state violence is illegitimate, and that justice and security ought to be solely distributed via market mechanisms. Agorism became a dominant political ideology of the Silk Road, the first major Dark Web drug market. The Silk Road agorists argued that selling drugs outside state control would undermine the state altogether. However, the Silk Road was seized in 2013 and its founder arrested. Rather than curtailing political thinking, the end of the Silk Road ushered in a new relationship to state violence in the form of what I call "OPSEC politics." OPSEC, or operations security, is a practice originally developed by the U.S. military and

later appropriated by Dark Web market participants. I show in chapter 4 how OPSEC politics helps produce new social formations that are more in line with larger discourses associating communication and violence.

The next chapter, "Searching for the Google of the Dark Web," explores search engines as legitimate organizations. Drawing on interviews with software developers who have taken on the challenge of searching Freenet, I2P, and Tor web content, I consider their claims to legitimacy as propriety, that is, commanding respect and commanding resources. I trace how Dark Web search engines integrate themselves into networks and become obligatory points of passage, mediating between a host of other entities, including users, site administrators, law enforcement agents, and software protocols. I conclude with an analysis of the techniques by which Dark Web search engines lay claim to an important inheritance: the legitimacy of being called the "Google of the Dark Web."

Chapter 6, "Being Legit on a Dark Web Social Network," focuses on the final meaning of legitimacy, as authenticity. To illustrate this meaning, I consider how members of a specific Dark Web social networking site, Galaxy2, negotiate the tensions between social networking practices, pseudonymity, and administrative rules, seeking to be "legit" members of the site. While contemporary social networking has a set of now-standard practices (gather friends, gather likes, share content), these practices take on different shapes when introduced into anonymizing networks. Community norms and explicit rules are used by Galaxy2 members and administrators to cultivate a particular site culture. Those who are included in the culture are legit; those who are not legit are excluded from the site. The predominant mode of interaction hinges on building profiles while refraining from offering personal information. As the chapter shows, however, in some cases—specifically when members disclose that they are young and female—the rules of authenticity change in disturbing ways.

Chapter 7, "Facebook and the Dark Web: A Collision," traces the symbolic economy of legitimacy that resulted in the Tor Project's successful registration of .onion with Internet standards bodies.

While Internet standards are highly technical, backgrounded, and infrastructural, they have profound consequences for the billions of Internet users. As I show in this chapter, they also have consequences for Dark Web systems. Because Internet standards groups recognize .onion—a recognition prompted in no small part by Facebook's involvement in the process—Tor hidden services can now get Extended Validation certificates. This can lead to more "legitimate" (in the sense of propriety) sites mirroring their operations on the Tor network. In addition, Tor's success hinged in part on delegitimating rival networks, such as I2P. I conclude the chapter by considering how Facebook's presence on the Tor network blurs the lines between Dark and Clear Webs.

The book concludes with a short chapter arguing for the value of anonymous political speech in a time of ubiquitous surveillance. I acknowledge the calls to end the development of anonymizing networks because so much illegitimate activity happens on them, but I argue that, in the absence of anonymizing networks and in the presence of increasingly monitored digital communications, we lose a valuable means of political speech and dissent if we shut down the Dark Web.

Caveats and Shortcomings

As a single researcher exploring three anonymizing networks, including their archives, participants, and software systems, I face many shortcomings, ranging from a skills deficit (I have no training in computer science) to strong personal views (I have particular stances on resisting the corporate-dominated Clear Web, as can be seen in my previous published work).[39] Here, I want to caution the reader a bit.

Language Limitations

I am a native English speaker. I am an American. These are limitations. There are many sites on Tor, I2P, or Freenet that are in languages other than English. I can read Spanish, but beyond that, I have difficulties with sites in other languages. I2P, for example, has many sites in Russian, and Tor is increasingly seeing a growth in Russian-language users and sites. One might simply suggest that I use an online translation system, such as Google Translate, to read the contents of non-English and non-Spanish sites. Even setting aside the problems of machine translation, however, I believe this would be a privacy violation. Google is, of course, notorious for its practice of absorbing every bit of information it encounters. This includes text entered into Google Translate. I must assume that people running Dark Web sites are doing so in part to avoid being monitored by Google, so I have never fed any site text into Google Translate. Nonetheless, one advantage I have speaking today's de facto lingua franca is that most Dark Web development (detailed in chapter 3) is conducted in English, and many Dark Web sites use English as a primary language. Even so, the analyses offered in this book are definitely limited by my language inabilities.

The Dark Web Changes Constantly

As Monica Barratt and Alexia Maddox aptly put it, the Dark Web is a constantly "fracturing digital environment."[40] Much of the Dark Web has changed, even during the course of this writing, and much will change after the book comes out. Dark Web sites are notoriously ephemeral, appearing online for a few months and disappearing without a trace. To be certain, some last years, but these are rare. The sites I write about here may very well be gone by the time this book is published. Indeed, two notable Tor hidden services, Grams and Galaxy2, have gone offline during the copyediting phase. No doubt I missed important sites as I did the research for this book. Complicating this situation, there is no Archive.org for Freenet, Tor, and I2P, and the makers and users of these sites don't think of what they are doing in historical terms, so they rarely save their old content.[41]

The result of this constant change is that my analysis will be relatively unique: the sites I examine and the people I have interviewed may be impossible for others to find. In light of this, and for the convenience of the reader, I include Clear Web links to the sources I'm drawing on whenever possible. Nonetheless, in many instances, I must refer to sources that are solely available via Tor, I2P, or Freenet. These links will be marked in any endnotes or citations with [Tor], [I2P] or [Freenet]. As discussed above, these links cannot be reached without the use of their respective routing programs, so anyone wanting to follow up and verify my work would have to install the routing software, configure a browser to use that software, and follow the links, assuming they are still active. In those cases where I believe the site owner does not want the link shared, I will withhold the link.

In addition, I focus on three key Dark Web site formats: markets, search engines, and social networking sites. This does not exhaust the types of sites found on Freenet, Tor, or I2P, such as pornography sites, chat sites, forums, and blogs. Like the Clear Web, the Dark Web has a wide range of sites, and this book cannot cover them all.

My Own Legitimacy

Finally, what of my own position as a researcher, or as a Dark Web participant? To put it in terms of this book, am I legitimate? In terms of academic work, at the very least, I hope my deep archival work and several years working with Dark Web systems, in addition to participant observation and interviews with Dark Web administrators and users, provide some answer here. As for my interpretations of all these data: they are of course subject to debate.

On a related note, I will say that I do not believe I am "giving voice" to Dark Web users. They are already quite vocal. I do not think of this work as "representing" them either. Frankly, to use a practice I discuss in this work, at best I can say that I am engaged in an exchange of the legitimacies of the Dark Web, trafficking these legitimacies from one domain into another, in this case from Dark Web sites to an academic study. I also must face the fact that, at worst, I am appropriating the legitimacy of Dark Web makers and participants, simply taking their ideas and presenting them in a book published by an academic press and thus benefiting professionally from the work of others. Mindful of this problem, I have labored to make this book as much an exchange of legitimacy as possible.

Notes

1. James Comey, “Encryption, Public Safety, and ‘Going Dark,’” *Lawfare* (blog), July 6, 2015, http://www.lawfareblog.com/encryption-public-safety-and-going-dark.

2. Jeremy Hunsinger, “Produsing the Hidden: Darknet Consummativities,” in *Produsing Theory in a Digital World 2.0,* ed. Rebecca Ann Lind (New York: Peter Lang, 2015), 60.

3. For an example of this, see Iain Gillespie, “Cyber Cops Probe the Deep Web,” *Age*, October 24, 2013, first edition, sec. Green Guide.

4. Michael K. Bergman, “The Deep Web: Surfacing Hidden Value,” *Journal of Electronic Publishing* 7, no. 1 (2001), http://quod.lib.umich.edu/cgi/t/text/idx/j/jep/3336451.0007.104/--white-paper-the-deep-web-surfacing-hidden-value?rgn=main;view=fulltext.

5. Hsinchun Chen et al., “Uncovering the Dark Web: A Case Study of Jihad on the Web,” *Journal of the American Society for Information Science and Technology* 59, no. 8 (2008): 1347.

6. Hsinchun Chen, *Dark Web—Exploring and Data Mining the Dark Side of the Web* (New York: Springer, 2012), http://www.springer.com/computer/database+management+%26+information+retrieval/book/978-1-4614-1556-5.

7. Jamie Bartlett, *The Dark Net: Inside the Digital Underworld* (London: Windmill Books, 2014). Throughout the book, I refer to what is commonly called “child pornography” as “child exploitation images” (or CEI). I adhere to pornography studies scholar Barbara DeGenevieve’s definition of pornography:

"*Consensual* acts being depicted … for the sexual arousal and masturbatory entertainment of the viewer." Thus rape scenes, snuff, abuse, revenge images, and child sex images are not pornography: they are nonconsensual and thus "prosecutable crimes." "Consent" is of course a very difficult concept to define, but I take the capacity for giving consent to include the ability to be a full citizen in a society, including the right to say yes—and more importantly no—to governance, parents or guardians, employers, or peers. Since no societies fully recognize the right of children to do this, children cannot be said to consent, including to others deriving sexual pleasure from their bodies. See Barbara DeGenevieve, "Ssspread.Com: The Hot Bods of Queer Porn," in *C'lickme: A Netporn Studies Reader*, ed. Katrien Jacobs, Marije Janssen, and Matteo Pasquinelli (Amsterdam: Institute of Network Cultures, 2007), 255.

8. Estimates of the number of websites hosted on Freenet, Tor, and I2P vary, but indexes I've seen show roughly 4,000 Freenet "freesites," 1,000 I2P "eepsites," and 5,000–8,000 Tor hidden services. These numbers fluctuate over time as sites come and go, and, as I discuss in chapter 5, indexing them is difficult.

9. For example, the now-defunct AlphaBay Market hired PR staff to manage its Reddit page.

10. One counterpoint to the Arizona researchers: Freenet freesites, Tor hidden services, and I2P eepsites—that is, the Dark Web as I define it—appear to have little in the way of ISIS propaganda. ISIS, it seems, prefers the Clear Web to promote itself. See Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no. 1 (January 2, 2016): 21, doi:10.1080/00396338.2016.1142085. See also Thomas Rid's comments in Pierluigi Paganini, "UK Police: Accessing the Darkweb Could Be a Sign of Terrorism," *Security Affairs*, July 8, 2017, http://securityaffairs.co/wordpress/60798/terrorism/darkweb-terrorism.html.

11. Gabriel Weimann, "Going Dark: Terrorism on the Dark Web," *Studies in Conflict and Terrorism* 39, no. 3 (2015): 196, http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546.

12. In fact, Bartlett's book only partially touches on the Dark Web (as I'm defining it), discussing several Tor hidden services and not exploring Freenet or I2P at all.

13. They also result in a steady stream of new users who take to forums such as Reddit to ask how to access the "Marianas Web" or the "Closed Shell System," purportedly "deeper" layers of the Internet accessible only with quantum computing. These new users cite infographics such as the one found at https://imgur.com/vvXru. These graphics are jokes, "an epic troll that people have interpreted as fact." Violet Blue, "The Myth of Mariana's Web, the Darkest Corner of the Internet," *Engadget*, December 18, 2015, https://www.engadget.com/2015/12/18/the-myth-of-marianas-web-the-darkest-corner-of-the-internet/. One upshot of them, however, is that they point to a cultural desire for something deeper, something beyond the "surface" mediascape. This impulse to go "deeper" is certainly worth investigating.

14. For example, see the comments section of Arma [Roger Dingledine], "Facebook, Hidden Services, and HTTPS Certs," *Tor Blog*, October 31, 2014, https://blog.torproject.org/blog/facebook-hidden-services-and-https-certs,for discussions about the need for a name other than Dark Web and the difficulty of coming up with an alternative.

15. Patrick Howell O'Neill, "Tor's Great Rebranding," *Daily Dot*, March 26, 2015, https://www.dailydot.com/layer8/tor-media-public-relations-perception/.

16. Adele Clarke, *Situational Analysis: Grounded Theory after the Postmodern Turn* (London: Sage, 2018).

17. Donna Haraway, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective," *Feminist Studies* 14, no. 3 (1988): 575–599; Clarke, *Situational Analysis*, 21.

18. Clarke, *Situational Analysis*, 294.

19. John Law, "Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity," *Systemic Practice and Action Research* 5, no. 4 (August 1992): 379–393, doi:10.1007/BF01059830.

20. Clarke, *Situational Analysis*, 87.

21. John Law and Annemarie Mol, eds., *Complexities: Social Studies of Knowledge Practices* (Durham, NC: Duke University Press, 2002).

22. Colin Koopman, *Genealogy as Critique: Foucault and the Problems of Modernity* (Bloomington: Indiana University Press, 2013).

23. Gwern Branwen et al., "Darknet Market Archives (2013–2015)," Gwern.Net, December 1, 2013, https://www.gwern.net/DNM-archives.

24. For example, two sites I drew on extensively to research I2P, the wiki at ugha.i2p and the user forum at forum.i2p, are no longer online, taking their extensive archives with them. In addition, I do not focus on one major category of Dark Web sites, chans (or image sharing boards), because during my research phase, chans were in disarray, appearing and disappearing regularly. During the copyediting phase of publishing this book, several important sites have shut down, including the Grams Tor search and the Galaxy2 social networking site. The latter may come back online, however.

25. This problem of missing data is not limited to my work; those who engage in systematic scraping of Dark Web forums report

that the resulting archives are largely incomplete. This is due in part to the problems of scraping anonymizing networks, including issues with network bandwidth and connection loss. For a discussion of issues with data scraping the Dark Web, see James Martin and Nicolas Christin, "Ethics in Cryptomarket Research," *International Journal of Drug Policy* 35 (September 2016): 84–91, doi:10.1016/j.drugpo.2016.05.006.

26. Clarke, *Situational Analysis*, 151.

27. Hugh Gusterson, "Ethnographic Research," in *Qualitative Methods in International Relations*, ed. Audie Klotz and Deepa Prakash (Research Methods Series, Basingstoke, UK: Palgrave Macmillan, 2008), 104. Most quotations from interviews or from Dark Web sites will be further anonymized by withholding pseudonyms, unless (a) I've received permission from the person, (b) the person involved promotes the site elsewhere (as in the case of the I2P developer forum), or (c) the content is mirrored on the Clear Web in some form (as in the case of Silk Road forum posts, which are publicly available in the Branwen et al. archive).

28. Tom Boellstorff, *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human* (Princeton, NJ: Princeton University Press, 2008).

29. Monica J. Barratt and Alexia Maddox, "Active Engagement with Stigmatised Communities through Digital Ethnography," *Qualitative Research* 16, no. 6 (May 22, 2016): 701–719, doi:10.1177/1468794116648766.

30. Steven Weber, *The Success of Open Source* (Cambridge, MA: Harvard University Press, 2004).

31. Nick Montfort and Ian Bogost, *Racing the Beam: The Atari Video Computer System* (Cambridge, MA: MIT Press, 2009).

32. Rob Kitchin and Martin Dodge, *Code/Space: Software and Everyday Life* (Cambridge, MA: MIT Press, 2011), 23.

33. Weber, *The Success of Open Source*.

34. Madeleine Akrich, "The De-Scription of Technical Objects," in *Shaping Technology/Building Society*, ed. Wiebe Bijker and John Law (Cambridge, MA: MIT Press, 1992), 205–224; Steve Woolgar, "Configuring the User: The Case of Usability Trials," in *A Sociology of Monsters: Essays on Power, Technology and Domination*, ed. John Law (London: Routledge, 1991), 57–99; Amanda Friz and Robert W. Gehl, "Pinning the Feminine User: Gender Scripts in Pinterest's Sign-up Interface," *Media, Culture and Society* 38, no. 5 (July 1, 2016): 686–703, doi:10.1177/0163443715620925.

35. Clarke, *Situational Analysis*, 293; Colin Koopman and Tomas Matza, "Putting Foucault to Work: Analytic and Concept in Foucaultian Inquiry," *Critical Inquiry* 39, no. 4 (June 2013): 817–840, doi:10.1086/671357.

36. Nicholas A. John, *The Age of Sharing* (Malden, MA: Polity, 2017), 6.

37. Ibid., 8.

38. Raymond Williams, *Keywords: A Vocabulary of Culture and Society* (rev. ed.; New York: Oxford University Press, 1985), 15.

39. Robert W. Gehl, *Reverse Engineering Social Media: Software, Culture, and Political Economy in New Media Capitalism* (Philadelphia, PA: Temple University Press, 2014). As Ian Bogost and Nick Montfort note, there is a need for cultural studies/humanities/critical scholars to engage with digital media in technical terms, even without formal training: "The training necessary to address what we call the code and platform layers of new media does not require a computer science degree, and some are quite capable in these approaches without having completed

any formal coursework. But investigation of these levels does require interest, commitment, and follow-through, and a willingness to use new and challenging methods of thinking and investigation." See I. Bogost and N. Montfort, "Platform Studies: Frequently Questioned Answers" (paper presented at the Digital Arts and Culture Conference 2009: After Media—Embodiment and Context, UC Irvine, 2009), 6.

40. Barratt and Maddox, "Active Engagement," 14.

41. There are exceptions, though. I downloaded archives from a Tor user, K-Man, who created the Torpast archiving project to scrape the HTML of Tor hidden services. It's no longer online, however. In addition, some of the search engines I discuss in chapter 5 provide access to their indexes, which preserve sites after their demise. Finally, Freenet's storage structure allows for files to be archived for quite a while, so it is possible to get a sense of the history of Freenet content. A valuable project—itself moribund—was the Freenet Graveyard: "Dead Sites Worth Visiting," Freenet Graveyard, June 14, 2011, http://127.0.0.1:8888/USK@2TPYEQHZJ7WKLunURL0RqYGOF6xbdunHQxeAQ9T1Me4,YHHp7AJJMFmW42ympU3IfOYlYfRJa7MdYcTgWCRs0Ns,AQACAAE/site/6/ [Freenet]. Freenet is also built to "forget" files that are less commonly accessed, however, so sites and files that are less popular are deleted from the network.

2 Violence, Propriety, Authenticity: A Symbolic Economy of the Dark Web

On a Tor-based market forum for customers of a counterfeit American currency vendor, one satisfied customer proclaimed, "I like the sparkly 20 [counterfeit dollar bill] because I do something to them that makes it look legit:) I also make the green eagle look legit. All by hand ;)."

Reporting on Dark Web drug markets, the business magazine *Business Insider* ran this headline: "If Silk Road Was a Legitimate Startup, It Would Be Worth ~$2.4 Billion."[1] In a comment on the story, one reader argued, "Anything worth $2.4 billion is more relevant, legitimate operation than most startups."[2]

During a debate about spam on the Freenet developer's mailing list, one developer argued, "I also wouldnt think spam would be a good form of advertising for a legitamite [*sic*] product, it would be more likely to make consumers boycott a product rather than support it."[3]

British newspaper the *Telegraph* reported on research about Tor's hidden services:

> [Security researchers] Rid and Moore commend Tor for offering vulnerable people access to anonymous browsing. But they said Tor needs to work harder to encourage its community to build a safe and legitimate browsing experience.
>
> "The developers made Tor for a different purpose—they wanted security, not crime. It's up to them to change the direction," said Rid. "It's up to them to have a sensible discussion about ways to reduce crime, to get more legitimate users in."[4]

On an I2P Frequently Asked Questions page, in response to the question "I've found some illegal content, what should I do?," one response reads, "The fact that such content is available is just a testament to [I2P's] own success, as distasteful as it is. Like a canary in a coal mine. [I2P,] Tor and Freenet are possible havens of illegal activity, but have many legit uses."[5]

As should be clear, a keyword unites these disparate quotes: *legitimacy*. During my time over the past three years on Tor hidden services, I2P eepsites, and Freenet freesites, I've seen variations on the word "legitimate" come up again and again. On Dark Web forums, social networking sites, chat sites, Reddit subs, in news reporting, and in YouTube how-to videos, people often deploy variations on the term "legitimate" when they discuss the Dark Web or activities on the Dark Web. Moreover, as should be clear from the above examples, people are using this term in very different ways.

Why does this matter? First, I want to suggest that the repeated use of the term "legitimate" (or its variants) reflects an anxiety about the Dark Web itself. Following on science and technology studies scholars Philippe Mallein and Yves Toussaint, I would suggest that the Dark Web is going through a "trial of legitimacy," as various social groups are gathering around it, struggling over its uses and boundaries.[6] As Guillaume Latzko-Toth explains, before a technology "gets integrated—or rejected—in a given social milieu, the technology is subjected to a 'trial of legitimacy,' where its relevance, meaning, and compatibility with the group's norms and values are examined and debated."[7] The controversies swirling around the Dark Web show that such a trial is clearly happening now. Specific questions for the Dark Web's trial of legitimacy include:

- What is the role, if any, for the Dark Web in our contemporary media environment?
- Who should and should not use it?
- For what purposes?

- Who should control it?
- What are the contours of access to it?
- How are violations of its legitimate uses to be prevented or punished?

Moreover, the variety of interpretations of "legitimate" indicate that the trial of legitimacy is intense, variegated, and working on multiple registers. The quotations that open this chapter reveal a range of different views that touch on legitimacy:

- There's a discussion about hand-crafting counterfeit bills to make them seem authentic.
- The distinction between one multibillion-dollar start-up and the next might hinge on social acceptability rather than on business acumen.
- Some forms of advertising on decentralized networks are respectable, and others are not.
- Crime and security are incompatible.
- The presence of illegal activity on the Dark Web means that it is protecting all users from state power.

If I am interested in exploring the Dark Web's trial of legitimacy, these diverse interpretations of "legitimate" pose a problem. How does one decide if something is legitimate? Is there a clear and objective measure? The various uses of the concept found in those quotations—and indeed, in many of my interactions with Dark Web users, administrators, and commenters—implies that a clear definition of legitimacy is lacking.

In the face of this, I have two possible responses. One is to say that some of these people are using the term "legitimate" wrong, that they don't know what the word means. I could seek to clear up this confusion by offering an unambiguous definition of the term so that we could go about the business of making criteria to judge what is properly legitimate and what is not. This would be a means to adjudicate the Dark Web's trial of legitimacy.

I am a cultural studies scholar, however, which means I take seriously how people understand the worlds around them, and how that understanding might be reflected in the language they use. Thus, a second response is not to treat some uses of "legitimate" as wrong and others as right, but to instead consider all meanings of the term as relevant, as descriptions and aims of practices rather than hard-and-fast definitions. I would then trace the symbolic economy that is trafficked across these meanings, particularly as this economy relates to specific practices on the Dark Web and the struggle to define what that system is and does and who should control it.

This chapter—indeed, this book—is dedicated to the second option. If users, law enforcement agencies, drug dealers, journalists, business analysts, counterfeiters, entrepreneurs, academics, spammers, or free speech advocates are gathering around the Dark Web and deploying variations on the term "legitimate" in their struggles over the meaning of these networks, a task before us is to (a) create a typology of these different meanings of legitimacy and (b) consider the economy of meanings that moves across these different legitimacies. From the counterfeiter's "legit" twenty-dollar bill sold on a Dark Web market to the law enforcement agent's legitimate right to arrest Dark Web site operators, legitimacy, in all its shades and transformations of meanings, is a central concept for this book. Moreover, as I argue in this chapter and throughout the book, legitimacy is always about communication and power. The development of legitimacy through a symbolic economy enables actors to claim resources, command flows of wealth and information, and make decisions about who is included in a social order and who is excluded. The multifaceted term "legitimacy" thus opens multiple conceptual lenses onto the Dark Web. Given that my focus in this book is on the social groups building anonymizing networks and using various Dark Web applications that exist within them, tracing how these groups engage with legitimacy in all its forms is an important task.

In this chapter I first present three variations on legitimacy: the state's claims to a monopoly on violent force, corporate and

organizational propriety, and authenticity (colloquially called the "legit"). Next, I consider a symbolic economy where such legitimacies are inherited, exchanged, purchased, appropriated, or denied. I conclude by considering the Dark Web's trials of legitimacy in further detail.

Three Legitimacies

The State's Legitimated Monopoly on Violence

"The relation between the state and violence," argues Max Weber, "is an especially intimate one."[8] Weber's influential lecture "Politics as a Vocation" theorizes legitimacy, specifically state legitimacy, as a monopoly on violence. Weber defines the state as "a human community that (successfully) claims the *monopoly of the legitimate use of physical force* within a given territory." The state "is considered the sole source of the 'right' to use violence." It is a "relation of men dominating men, a relation supported by means of legitimate (i.e., considered to be legitimate) violence."[9]

Weber identifies a relationship between the material tools of violence and obedience:

> Organized domination, which calls for continuous administration, requires that human conduct be conditioned to obedience towards those masters who claim to be the bearers of legitimate power. On the other hand, by virtue of this obedience, organized domination requires the control of those material goods which in a given case are necessary for the use of physical violence.[10]

In other words, obedience among populations may begin with their recognition that the state has monopolized tools of violence (weapons, armies, police, etc.), but over time—presumably to reduce the cost of control—populations are conditioned to become obedient. Politics, then, is the organized pursuit of the "top places" of this order: the command of the bureaucracies, armies, or police forces. If the state can monopolize the use of violence, condition the obedience of populations, and establish a cadre of administrative agents, it can exercise power in both violent and nonviolent ways.

For scholars in the Weberian tradition, violence is an empirically verifiable aspect of contemporary states. As C. Fred Alford forcefully argues, "Brute, physical coercion is not the last resort of the regime, any regime. It is the first, which means that it is the veiled threat behind every act of political power—that is, every act of power."[11] And as Herbert Wulf argues, "There can be no doubt that states have applied violence on a larger scale, more efficiently and more effectively since they have endeavoured to monopolize force."[12] This form of legitimacy, the legitimated monopoly on violence, finds its most obvious expression in the tools of war and policing. Military strength is inside-out state violence, directing what military theorists call "kinetic force" at targets outside the borders. In international law, "The right to declare and wage war is given only to states, some entities resembling them, and the United Nations itself."[13] Policing—what sociologist Jonathan Jackson and colleagues call "the most available and salient representative of the state"—is top-down state violence, directing state-sanctioned surveillance, arrest, seizure, imprisonment, and execution at citizens who violate laws.[14] In both cases, accepted uses of these violent practices is called legitimate.

Moreover, as Jackson and co-authors argue, the belief that the state has the monopoly on violence is correlated with the belief that "private violence" (vigilantism, revenge, or political rebellion) is morally unacceptable. "The nature of legitimacy invites the hypothesis that recognizing that the right of the police to dictate appropriate behavior is also to believe that one should not use violence to achieve certain goals—that is, that the police have a right and just monopoly over violence in society."[15] Similarly, as Chandan Reddy argues, states promote themselves as "the pre-eminent vehicle for the conquest of arbitrary and irrational violence by a legitimate violence."[16] This leads to the view of citizens' docility (or at least physical nonviolence) as morally right and rational: "When people believe that legal authorities have the right to power and the right to dictate appropriate behavior, they tend to defer to, and

cooperate with, legitimate authorities because they feel it is the right thing to do."[17] In short, they cede violence to the state.

Importantly for the central object of this book—the Dark Web—the language used by these theorists is that of claims, beliefs, and perceptions. This is not an argument that some essential, measurable phenomenon known as legitimacy exists, or that the state collects or essentially comprises such a substance. Rather, the state seeks to *cultivate* the belief in its claim to the monopoly on violence. As the sociologist François Bourricaud argues, "What interests us is not the state of legitimacy but the process of legitimization."[18] Likewise, political theorist Rodney Barker contends, "What characterizes government … is not the possession of a quality defined as legitimacy, but the claiming, the activity of legitimation."[19] What is claimed is the monopoly over violent force *and* the rightness of that monopoly; the evidence for the successful claim is to be found in whether the state's "political subjects overtly follow its commandments."[20]

Here, we can see how the hard core of state violence can permeate outward into other social institutions. If state legitimacy is subject to claims, beliefs, and perceptions, then a key arena in which the monopoly on violent power is constructed and contested is in mediated communication. States' claims can be contested and of course often are. The contests might be violent, as when rebel factions take up arms against a ruling faction. They might be nonviolent, as when one government is challenged during an election. In either case, the claim is that those in power should not have the monopoly on violent force and that the contesting faction or party should. Here, the central mechanism is communication: whether or not political change happens through violence, the struggle for the monopoly of violence often plays out in mediated debates and discourse: slogans, speeches, videos, broadcasts, websites, tweets, or memes.

Thus, broadly speaking, the relationship between media and the state is extremely important. As Jessica Beyer and Fenwick McKelvey put it, "the modern state depends on an informational

infrastructure that makes its territory and population legible."[21] For states that control mass media, propagating their self-legitimating messages is easy. States that don't directly control mass media still have means to get self-legitimating messages out, through tactics such as granting access to top officials for interviews to select media companies, partnerships, or sophisticated public relations campaigns. Those who oppose the ruling elites must either seek out alternative channels or make their own inroads into mass media broadcasting. We can therefore think of mass media as key sites for discourses about state violence.

Of course, the argument that mass media are tools of the state grates against the idealized role of mass media as a "fourth estate"—a critical check on state power. If mass media have become the tool of the state, what about Internet media? The Internet has been an object of what Armand Mattelart has called the "messianic discourses about the democratic virtues of technology."[22] It has been lauded as a means for anyone with a computer and modem to circumvent mass media systems, a "networked fourth estate," an avenue for criticism of the state.[23] This has direct relevance for claims to the monopoly on violent force: established elites struggle to adopt new technologies, such as social media, to defend their monopolies, and those who challenge them do the same.[24] I return to these points in the next two chapters.

Of course, states are often more than police and military forces proclaiming their status in media. States also build complex institutions that may not directly rely on violence but only refer to it on occasion: diplomacy, land management, licensing, record keeping, taxation, or civil courts, to name a few. Such institutions can diffuse violent practices and thus deemphasize the articulation between states and violence. In fact, this leads to another conceptualization of legitimacy: organizational legitimacy, or legitimacy as propriety.

Legitimacy as Propriety

The state's claim to a monopoly on violent power is not the only form of legitimacy. As capitalism has developed into the transnational corporate form we see today, organizations (especially corporations, but also universities and nonprofits) have sought to establish what they call legitimacy. This is on a different register from state power. Returning quickly to Weber, "The direction of capitalist enterprises, despite far-reaching analogies, follows quite different laws than those of political administration."[25]

Here, I would suggest an articulation between legitimacy and propriety. I use "propriety" to signal the connotations of proper behavior as well as proprietorship, or operating a business. Indeed, much of the scholarly literature theorizing this form of legitimacy comes from organizational and managerial communication, a field dedicated to understanding how organizations (primarily corporations) can use communication to influence their employees, shareholders, customers, and regulators. This perspective might be summed up by the common phrase "legitimate business," meaning a legal, accepted, proper business that is perceived to be operating ethically. In other words, legitimation at the level of capitalist firms is a different animal from the state's claim to violence.[26]

Organizational sociologist Mark C. Suchman defines this form of legitimacy as "a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions."[27] As Eero Vaara and Janne Tienar argue, "From this perspective, legitimation stands for creating a sense of positive, beneficial, ethical, understandable, necessary, or otherwise acceptable action in a specific setting."[28] The socially constructed system or setting that organizations operate in is transnational capitalism. Relevant actors within this system include "public opinions, educational systems, professions, ideologies, and certification and accreditation bodies," as well as "consumers, employees, investor, local communities, government, non-profits, and media."[29] These are the actors for whom a "sense of positive" perceptions must be created.

At the center of all this is the management of organizations. In the literature of organizational and managerial communication, managers are the key actors capable of constructing a perception of the organization's propriety among the various stakeholders. Roy Suddaby and Royston Greenwood argue that these actors can use persuasive arguments—that is, rhetoric—drawn from existing cultural logics in order to make organizations comprehensible and taken-for-granted. Such "logics enable actors to make sense of their ambiguous world by prescribing and proscribing actions."[30] These preexisting logics include habits of thought that might be articulated in a new organization. Similarly, as Martin Ruef argues, "Novel organizational forms are most likely to become legitimated when they fit into the pre-existing cultural beliefs, meanings, and typifications of an organizational community."[31] As the privileged actors within transnational capitalism, managers are in key positions to do this articulating work to legitimize an organization through such habits of thought. Thus, if managers are successful in aligning these perceptions, the organization is seen to be consistent with the prior cultural logic. I take up the concept of aligning perceptions in detail in my study of Dark Web search engines in chapter 5.

Much as in the case of state violence, organizational propriety is often constructed and contested through mediated communication, including strategic communication, advertising, and branding practices. And just like states, organizations traditionally rely on mass communication (television, newspapers, radio) to get their self-legitimating messages out. Indeed, the history of American mass media might be read as the history of corporate legitimation practices, where corporations took to the airwaves to peddle their wares, raise our awareness of their existence, and justify their claims to capital, resources, and labor. More recently, the advent of Internet communication, particularly social media, has seen organizations scramble to find new methods of self-legitimation, including using Twitter and Facebook to develop networks of fans

and boosters as well as engaging in sentiment analysis to monitor the legitimacy of their brands.[32]

"Whatever the method of legitimation," organizational and managerial scholars Blake E. Ashforth and Barrie W. Gibbs argue, "the intent is the same: To foster the belief among constituents that the organization's activities and ends are congruent with the expectations, values, and norms of constituents."[33] Business scholars Shuili Du and Edward T. Viera Jr. note that legitimacy "is vital for organizational survival because it ensures the continuous flow of resources and the sustained support by the organization's stakeholders."[34] To put this another way, legitimacy as propriety is important because it ensures the organization's continued control of the materials of production as well as that organization's ongoing realization of value (in economic, cultural, or symbolic forms). The goal of propriety is to preserve the capacity of the firm to act as freely as possible in the pursuit of its goals (particularly privatization of economic profit and the socialization of risk, but also the capture of symbolic or cultural resources). A business perceived to be legitimate can continue to control production processes, efficiently exploit the workers who are hired to produce using those processes, and market the products to various consumers. A nonprofit organization perceived as legitimate can continue to receive sponsorship and donations, efficiently exploit the labor of volunteers or highly idealistic employees, and market itself to the public as a necessary part of civil society. Both types of organizations are respected as they take these actions. Illegitimate organizations, on the other hand, face sanction from states who might deem them illegal (and who thus reserve the right to violently seize their assets or personnel), from workers who refuse to labor for them, or from consumers who refuse to buy from or sponsor them.[35]

Legit: Legitimacy as Authenticity

Unlike the state's claim to a monopoly on violence or an organization's claims to propriety, this final form of legitimacy is far

less theorized in academic work. A long tradition of political philosophy focuses on the state, legitimacy, and violence, and the growing field of organizational studies analyzes corporate and nonprofit legitimacy, but not much scholarship exists on what I call the "legit," or legitimacy as authenticity.

"Legit" connotes realness, belonging, coolness. A way to clarify this distinction is by drawing on a legit dictionary, rather than a proper, legitimate one such as the *Oxford English Dictionary*. According to the *Urban Dictionary*—an online crowdsourced dictionary of slang—"legit" is a "modern synonym for words such as 'cool,' 'ill,' 'tight,' or 'dope.'" To be legit is to not be fake, "one hundred percent NOT bullshit!" It "means 'for real' or in standard terms, 'fo realz.'"[36] The contributors to the *Urban Dictionary*, to illustrate their definitions, provide a range of examples of what can be legit: parties, clothes, drugs, stories, and achievements.

Legitimacy as authenticity, or legit as cool, appears often in popular music. At the height of his popularity, M. C. Hammer boasted that he was "2 Legit 2 Quit," drawing on his Oakland, California, roots and boasting, "I'll hit with a dose of Oaktown power." Likewise, in "I'm Legit," Nicki Minaj lets us know "I'm the greatest Queens bitch with the cashes flow"—in other words, she's "the shit legit." In "So Legit," Lana Del Ray critiques Lady Gaga for selling out, asking, "What happened to Brooklyn? / What happened to New York? / What happened to my scene? / What happened to punk rock?/ … I don't get it / I'm so legit."

These lyrics reflect what popular music scholars have found, that the vernacular term "legit" is tied to authenticity, which is itself determined in the relatively autonomous spheres of artistic cultures. In other words, states and corporations (and other large-scale aggregates) do not necessarily sanction what is legit and what is not. Rather, this form of legitimacy is sanctioned by specific, bounded communities of practice, such as artist groups, practitioners of a musical genre, denizens of a specific geographic community, academic schools of thought, or, most relevant to this book, users of particular online sites and services.

Although this form of legitimacy is less theorized than the others, a key figure has written about it extensively: Pierre Bourdieu. Artistic sanction, as opposed to political sanction, appears in his analysis of the birth of the symbolic goods market: he notes that artists initially drew their legitimacy from their political or religious patrons (i.e., from state authorities), but as they shifted to a secular, market-based practice, artists defined their own form of legitimacy in terms of their own practices.[37] In other words, artists established restricted fields of relations that determined what *authentic* (legit) art is, rather than relying on political or religious authority to establish what *legitimate* (state-supported) art is. As Michael Stevenson summarizes Bourdieu's field theory, "A field comprises a range of actors (e.g., artists, galleries, museums, and cultural intermediaries such as critics) competing for prestige, as well as the 'rules' that govern their actions: these unwritten 'laws' are socially defined and historically contingent agreements about what constitutes quality and legitimacy within the field."[38] These fields are relatively autonomous of other fields (such as the political, the realm of legitimated violence, or the economic, the realm of propriety).

Furthermore, because field theory focuses on fields of production, it is useful for thinking about objects and practices as well as people. Much of the emphasis is, of course, on humans: artists and critics, for example. But this view extends to authenticity in terms of objects: What type of art belongs in this field? What sort of images? What technical artifacts? And it extends to practices: What repeated fusions of language, objects, and movement are for real and thus belong? Which ones are bullshit and must be kept out of the field?

We can further see this form of legit when it is challenged. Writing about legitimacy and authenticity in hip hop, philosopher Leigh Roche argues, "In music we see challenges to supposed authenticity when a middle-class suburban white kid is rapping about their struggle in the 'hood. Regardless of how good their rap skills, their verbiage, or their groove, *legitimate* rap artists and their audiences know it's just [bullshit]."[39] In other words, authentic

rappers socially construct what is legitimate and establish in-group and out-group distinctions along those lines. Crossing that line is failing at the legit game, violating the criteria of a "field of restricted production" by misusing others' "legitimate and monopolized use of a certain class of symbolic goods."[40] Here, Bourdieu echoes Weber's conceptualization of the state's claim to violent power. To be marked as legit, one must demonstrate command of a class of symbolic goods, and one must also police the possession of those symbolic goods. We see this in Elizabeth Currid-Halkett's theory of the "aspirational class," where today's social winners convey their

> class position through cultural signifiers that convey their acquisition of knowledge and value system—dinner party conversation around opinion pieces, bumper stickers that express political views and support for Greenpeace, and showing up at farmer's markets. ... In each of these decisions, big and small, they strive to feel informed and legitimate in their belief that they have made the right and reasonable decision based on facts (whether regarding the merit of organic food, breast-feeding, or electric cars).[41]

In other words, legit is about the social construction of insiders and outsiders, the insiders marked by command of the restricted class of symbolic goods.

Alice Emily Marwick's book on Silicon Valley culture provides examples of this practice. As she argues, "Status hierarchies are partially maintained through erecting and reinforcing boundaries between insiders and outsiders."[42] She describes the practice of networking at conferences such as South by Southwest and the various tech conferences and parties held in Northern California. One story she tells points to the construction of insider/outsider dynamics:

> While the tech community emphasizes networking as a necessary skill for business success, people attending large tech parties who aggressively pitch their company to people whom they don't know are considered somewhat pathetic. Technology journalist and former C|Net blogger Caroline McCarthy explained this hierarchy when describing the New York Tech Meetup, a very large-scale event: "That's the sort of thing where afterwards. … you're going to be getting like business cards passed to you left and right, and you don't know who's legit. … I don't want to call it the bottom of the pecking order, but that's like the most open-entry, and it still is."[43]

As Marwick notes, "Implicit in this quote is that some people are 'legit' and others are not, a distinction that is primarily determined through social relationships."[44] In the creative technology industry, social knowledge of symbolic practices—say, how to meet someone at a party, the proper way to pass a business card, where to stand, whom to talk to and whom not to—can mark someone as legitimately belonging and others as hapless outsiders.

With this sense of legit—of being judged as real or authentic—we're far from the debates in international relations concerning the legitimacy of a government fomented during a coup, or debates in organizational studies about how social media might help a business legitimate its brand. But ignoring this conceptualization of legitimacy would be foolish, especially because—like the other two meanings I've explored—it can tell us much about how various social groups are struggling over the meaning and uses of the Dark Web.

Objects and Power

Although the various uses of the term "legitimacy" have significant differences, each meaning also echoes aspects of the others. States engage in clear practices of power—such as executing enemies and imprisoning criminals—but the power practices that mark the legit may be less clear. As I show throughout this book, practices of inclusion and exclusion are incredibly important on the Dark Web. Each legitimacy is marked by communicative practices, whether they be broadcasting nationalist spectacles on television, advertising one's propriety on Facebook, or making claims to a legit identity on Twitter. Each has its objects: citizen-subjects for the state; employees, shareholders, and customers for the corporation. Interestingly, the insular legit's objects are the same as its social groups: artists take other artists as objects, critics other critics (and artists), and hackers other hackers as all decide who's in and who's out.

Above all, then, legitimacy is about power. As Thomas Luckmann argues, "It conforms with Max Weber's position as well as with ordinary linguistic usage to say that legitimation is making sense of power. The real sociological questions—which are not definitional questions—start at this point."[45] This "making sense of power" involves those in power making claims about their capacity to act as well as those subjugated to power making sense of their subjugation.[46] In other words, legitimacy is a socially constructed judgment about whether a given institution, object, or person ought to enjoy the capacity to act and in so doing affect the conduct of others who do not enjoy that same capacity. In table 2.1, I have laid out each type of legitimacy's objects, power practices, discursive practices, social groups, and academic fields.

Table 2.1 Objects, power and discursive practices, relevant social groups, and academic fields for each meaning of legitimacy

Legitimacy	Objects	Power practices	Communicative practices	Social groups	Academic fields
Violence	Citizen-subject, enemy	Deprivation of life or time	Nationalist spectacles, rhetorics of patriotism, propaganda	Law enforcement, military, politicians	International relations, political theory
Propriety	Employees, investors, consumers	Firing, lawsuits, discipline	Public relations, advertising, branding, internal propaganda	Managers, administrators, moderators	Organizational sociology, organizational and managerial communication, business
Authenticity	Artists, intellectuals, critics, hackers	Inclusion and exclusion, distinction and differentiation, criticism	Criticism, identity claims, social sorting	Artists, intellectuals, critics, hackers	Popular culture studies, literary criticism

Further Articulating “Legitimacy” and “Dark Web”

I want to return to the quotations I began with and place those different conceptualizations of legitimacy in this framework.

The first, regarding the legit counterfeit twenty-dollar bills, comes from a Dark Web forum where a counterfeiter and his clients gather to discuss the artistry of making passable fake money, as well as techniques for passing counterfeits at cash registers. This is clearly not legitimate in the state sense—states tend to violently protect their ability to coin money—nor is it legitimate in the sense of propriety. Rather, these counterfeiters demonstrate their abilities through their command of symbolic and technical practices, placing them in the legit, or legitimacy as authenticity, category. Although counterfeit money is, by definition, fake, the goal of counterfeiting is arguably artistic: using paper, design, printing, and social engineering skills to produce a viable, passable note. Those are the skills of an authentic (not bullshit) counterfeit artist.

The next two quotations deal with legitimacy as propriety. As for Silk Road’s potential value were it a legitimate start-up, in the estimation of technology and business journalist Willard Foxton, if some “freewheeling entrepreneur” had bought it and nurtured it, they could have become “the [Mark] Zuckerberg of online drug dealing.”[47] Several business publications espoused similar views, noting that Silk Road was an innovative, compelling new market platform with many benefits, including making recreational drug purchasing safer and more convenient than going to the dealer on the corner—and its growth as an online market was unprecedented, even compared with Amazon or eBay.[48] Silk Road’s failure, in this perspective, was its inability to become legitimated—that is, a failure to become perceived as proper and acceptable, which was more a function of the (illegitimate?) War on Drugs than on rational business sense about markets and commerce.[49] It commanded resources, but it did not command enough respect.

The Freenet spam quotation comes from a longer mailing list discussion about the difference between legitimate speech—including speech advertising businesses and services—and illegitimate speech, specifically spam. Again, the question of propriety is central: proper businesses advertise. Illegitimate ones spam.

The tension between security and crime, as revealed in the final two quotations, registers at the level of state legitimacy. The report on the research of Moore and Rid suggests that Dark Web network builders have erred in protecting Dark Web site administrators from state power.[50] By making it difficult for states to geographically locate Dark Web sites, Dark Web systems have allowed for crime to flourish. The state's capacity to arrest criminals and seize the tools of crime is reduced by anonymizing networks. Yet, the researchers note that the Dark Web could host legitimate—in this case, noncriminal—activities that the state can accept.

On the other hand, the answer to the I2P FAQ regarding illegal content suggests that the developers of I2P see illegal activity as a sign that the network is secure, specifically secure from state surveillance and intrusion. If professional criminals find I2P safe, this logic goes, then political activists and free speech advocates will as well. This argument suggests that free speech trumps state power; in other words, we need systems by which to challenge and limit the state's claims to the monopoly on violent force.

A Symbolic/Material Economy of Legitimacy

Understanding the particular legitimacies expressed in the chapter-opening quotations still leaves the question of how such legitimacies are produced. Drawing on theorists ranging from Weber to Suchman to Bourdieu, I have suggested throughout this chapter that legitimacy—in any of its forms—is socially constructed. How is this construction achieved?

To explain this, I echo the work of Pierre Bourdieu and elaborate a symbolic economy of legitimacy.[51] Each of the three forms of legitimacy has an economic aspect. In Weberian theory, the state's claim to legitimacy rests on monopolizing the materials and techniques of violence. An organization's claims to propriety are a means to ensure its continued survival in competitive environments. And authenticity is measured within restricted fields of production that claim a monopoly on a class of symbolic goods. Meanings can traffic across the three legitimacies, much as other symbolic or material goods might traffic across artistic, economic, or political spheres. Indeed, such meanings are often trafficked to produce or strengthen claims to monopolies.

The symbolic economy of legitimacy has five key practices:

- Inheritance
- Exchange
- Purchase
- Appropriation
- Delegitimation

Inheritance

A long-standing conception of how legitimacy passes from one person to the next is *inheritance*. This was especially important for feudal and aristocratic societies, where new generations of nobility

inherited titles, land, and power networks from their parents. The heir to a title or fortune was referred to as the "legitimate" offspring. Although this form of governance is largely obsolete, its influence is seen in contexts such as post-Revolution France, where displaced aristocrats formed a political alliance, the Legitimists, who maintained that the true political leader of France is the genealogical heir to the Bourbon dynasty.[52] This alliance continues to this day. The Legitimists keep records of offspring and inheritance, making the lineages legible to their democratic opponents.

Yet, the inheritance of legitimacy is not necessarily straightforward. As historian Ann Twinam notes in her study of colonial Spanish America, for those born to noble families but outside sanctioned marriage—that is, the illegitimate, the bastards—legitimacy could be conferred by those in power.[53] Legitimacy for bastards could be purchased or sought through petition to the sovereign, and once received, it conferred on its holder social standing that could be passed on to heirs. The practice of petitioning the state to legitimate previously illegitimate offspring and establish lines of inheritance continues to this day.[54] Twinam thus shows that the inheritance of legitimacy is not essentially about objectively tracing lineages so much as it is a complex social institution. The fact that one could petition to have one's status as "bastard" removed and hence receive all the benefits of a legitimate birth—and pass this improved status on to one's children—means that inherited legitimacy is more of a social construction. Via Foucauldian/Nietzschean genealogy, we can extend this idea past family lineages and speak of the inheritance of legitimacy by other entities, including forms of government, institutions, political leaders, practices, and technologies, all of which have genealogies that take much work to trace.[55] For example, Jay David Bolter and Richard Grusin's remediation thesis, in which old media are represented within new media, can be read as a process of legitimacy inheritance.[56] YouTube, for example, represents previous

media forms (such as videotape playback interfaces) in a claim to be the inheritor of previous video technologies.

Exchange

Beyond inheritance of legitimacy across time, sociologists, historians, and rhetorical and organizational scholars have also demonstrated that legitimacy can be gained in a second manner: through cross-network *exchanges*. Sociologist of science Geoff Bowker's study on the field of cybernetics notes that cyberneticists engaged in "legitimacy exchange," where "an isolated scientific worker making an outlandish claim could gain rhetorical legitimacy by pointing to support from another field—which in turn referenced the first worker's field to support its claims."[57] In other words, a biologist might make claims about the fundamental informational core of biology by citing a mathematician, who would then turn around and cite the biologist to support the claim that mathematics is biological. This sort of cross-disciplinary exchange of legitimacy enables two or more communities of practice to bolster their reputations by drawing on the work of each other. Building on this, historian Fred Turner explores how the New Communalists (the countercultural back-to-the-land movement of the late 1960s) exchanged legitimacy with cybernetic scientists and network theorists.[58] The New Communalists sought to bolster their claims that technologies can be individually empowering, and they got support for that idea by citing cyberneticists. Cyberneticists, in exchange, drew on the counterculture to add an aura of rebelliousness and coolness (i.e., an aura of legit) that belied the field's Cold War origins. Another term for this might be Bourdieu's concept of "consecration." Likewise, Marouf Hasian, Sean T. Lawson, and Megan McFarlane argue that the U.S. national security complex has turned to science as a "practice to be mimicked and a storehouse of knowledge from which to borrow[:] science serves as a rhetorical resource for the construction and legitimation of military theories, strategies, and doctrines," suggesting a state-to-legit cross-domain legitimacy exchange.[59] Finally, organizational

studies scholars note the importance of endorsements (e.g., press coverage) to build the reputations of new businesses.[60] The journalists covering the new business gain the reputation for being up-to-date on business developments, and the new business can put the news organization's logo on its website.

Purchase

Purchasing legitimacy is another exchange practice, but the exchange is of nonlegitimacy resources for legitimacy. For example, as Greg Elmer has argued, corporate sponsorship of a music festival is a means by which that corporation might associate itself with the "authentic" culture of musicians, fans, or settings (as in the Molson Polar Beach Party).[61] According to Weber, a charismatic leader—perhaps one democratically elected—may make promises to constituents that their support (votes or donations) of her claim to legitimate leadership will be rewarded with material goods, say, lower taxes or increased public subsidies.[62] A state may also purchase the services of legit hackers to bolster the state's capacity to secure computer and information networks.[63]

Appropriation

A more exploitative form, legitimacy *appropriation*, echoes the economy of cultural or symbolic appropriation.[64] This practice is perhaps easiest to see with legitimacy as authenticity (i.e., legit), especially in music genres. For example, in American culture, white appropriation of black musical styles (from jazz to rock and roll to hip-hop) is marked by appropriating perceptions of realness, rawness, and urban credibility.[65] Likewise, American country and rock musicians often rely on appropriating rural and working-class culture. As Steve Redhead and John Street note about the legitimacy of Bruce Springsteen, "The multimillionaire Bruce Springsteen wears tattered jeans," thus appropriating a cultural symbol to bolster his authenticity as a working-class hero.[66] Appropriation can be readily seen in American politics, as candidates seek to

appropriate the legitimacy of the so-called middle class by using particular language or employing "retail politics"——meeting potential voters in bars, at rock concerts, or at baseball parks. Would-be state leaders (the would-be masters of the state's claims to legitimate violence) can bolster their claims by associating themselves with the authentic people they would represent.[67] Finally, we see legitimacy appropriation when private security firms mimic the symbols of police or military forces: consider the example of Texas-based Statewide Patrol, a "security services provider," whose employees carry badges, wear uniforms that closely resemble iconic police patrol uniforms, and drive Dodge Chargers painted and marked to mimic Texas State Police vehicles.[68]

Delegitimation

The final practice, *delegitimation*, refers to claiming that an institution, organization, practice, or person is not legitimate, often as a way to implicitly bolster one's own legitimacy. Echoing Weberian theories of the state, political theorist Naomi Sussmann describes an example of this practice in the use of just war theory in relation to terrorism: "There is an ongoing attempt to delegitimate terrorism within the framework of just war theory—namely, the idea that terrorists lack a just cause, that their means are disproportionate to their ends, and that they fail to distinguish between combatants and non-combatants, [and] indeed intentionally target those who should not be targeted."[69] In terms of authenticity, medical anthropologist Norma Ware, in her study of people with chronic fatigue syndrome, discusses CFS sufferers' experiences being delegitimated by others who denigrated their illness as "not real," as psychosomatic, thus denying them access to the social category of "medical patient."[70]

Perhaps the best contemporary example of delegitimation comes from someone seeking his own legitimacy: Donald Trump. During and after his general election campaign for the presidency of the United States, Trump delegitimated a dizzying array of people and

institutions: the previous president, Barack Obama, as not American by birth; his opponent, Hillary Clinton, whom he accused of rigging the election; the news media, particularly CNN, as "fake news"; the popular vote count (since he lost the popular vote); a U.S.-born judge presiding over the Trump University lawsuit (Trump claimed the judge was "Mexican"); and the U.S. intelligence agencies, to name a few targets. Arguably, all Trump's delegitimating activity was intended to bolster his own legitimacy. Delegitimation is a powerful move.

Overall, the symbolic economy of legitimacy production traces the complex movements between economic and cultural value that these inheritances, exchanges, purchases, appropriations, and denials imply. A great deal is at stake in this economy. As sociologists Karen A. Hegtvedt and Cathryn Johnson argue, once accrued, legitimacy can "enhance compliance with behavioral rules or group structures, often leading to the acceptance of distributions —even objectively unfair ones."[71] These new distributions are none other than redistributions of power, playing out in different spheres (the state, the corporation, the nonprofit, the hacker collective) as they produce new subjectivities. As Keith Ansell-Pearson argues, "Discourses of right and legitimacy are not simply ways of protecting individuals from the existence of power, but also disciplinary practices which constitute human subjects in new relationships of power."[72] Likewise, as Ashforth and Gibbs argue, "Once conferred, legitimacy tends to be taken largely for granted. A favorable reputation acts as a sedative on constituents."[73] Once children inherit parents' wealth, scientists acquire research funding and prestige, or wealthy politicians receive votes from their working-class supporters, such pathways tend to stay in place. If a government is formed and its executives seize the tools of violence, citizens will face difficulty in challenging the officials' legitimacy, let alone removing it. Once a corporation is established as the legitimate source for a particular product or service, it tends to maintain that position. Becoming established as an "authentic" member of a community grants a person the authority to adjudicate

insider/outsider distinctions through exchanges and delegitimation. Over time, these flows and practices solidify.

In other words, when something is legitimated, its position as a node in a network of power is enhanced; the channels drawing resources to it are widened, and the channels drawing resources away are choked. Moreover, we tend to accept this. After all, it is legitimate.

The Dark Web's Trials of Legitimacy

Returning to Mallein and Toussaint's argument that a new technology undergoes a "trial of legitimacy," I suggest that, given the symbolic economy of the three legitimacies, a more accurate, if awkward, phrasing is *trials of legitimacies*, which take on different valences and are fueled by the five different symbolic/material practices I outline above.[74]

First, and most obviously, the Dark Web is certainly undergoing a trial in terms of its relationship to violence. State actors regularly delegitimate it as a system that only aids and abets terrorists and criminals. The history of the Dark Web is punctuated with law enforcement investigations, seized servers, and arrests. Moreover, the language of state violence has been appropriated by hackers, who use terms such as operation (often shortened as "op"), war, attack, and operational security (OPSEC). These words and phrases regularly appear in Dark Web forums and social networking sites, and they feed into larger securitization discourses about cyberspace as a new frontier for fighting wars. Finally, one of the most commonly requested hidden websites is the infamous—and most certainly fake—Red Room, where viewers can watch a live feed of someone being (illegitimately) tortured and killed.[75]

And yet, one of the most common justifications offered for the Dark Web is its usefulness for political dissidents. Freenet, Tor, and I2P developers suggest that their projects, as systems designed to anonymize and protect free speech, enable people to contest state power, including the state's very claim to legitimated use of violence. Indeed, if state legitimacy hinges on the *claims* to the monopoly on violent force, counterclaims are necessary to provide a check on state excesses. This is how the users and developers of these projects justify their emphasis on anonymity: the political dissident who cannot be identified cannot be arrested or executed. More recently, with the advent of whistleblowing software such as

GlobaLeaks and SecureDrop, hidden web services dedicated to revealing the internal operations of governments have appeared. This leads to legitimacy exchanges as news organizations and Dark Web network builders collaborate to build new technologies that can further check state power.[76]

The Dark Web is also perceived as a security (and propriety) threat to corporations; when data breaches occur (as happened to the extramarital dating site Ashley Madison), those data often end up for sale on Dark Web markets. Botnet operators frequently use anonymizing networks for command-and-control systems to manage their spamming and phishing operations. Critics of Tor, I2P, and Freenet argue that these systems aid and abet illegal activities, such as black markets and the trade in child exploitation images.

In contrast to how they are often portrayed, the developers of Freenet, Tor, and I2P have built organizations, complete with budgets, administrators, logos, and marketing campaigns, to make claims to organizational legitimacy. Dark Web search engine operators seek to inherit the legitimacy of Google and provide easier access to the information stored on the Dark Web by building their own versions of "Google for the Dark Web."

Finally, how might the Dark Web figure into questions of authenticity, or the legit? Much of the Dark Web is animated by questions of who's in, who's out, what's legit, and what's bullshit. Although developers have worked to make using the Dark Web easier, accessing Tor hidden services, Freenet freesites, or I2P eepsites requires technical know-how that can exclude average computer users. Once on these Dark Web sites, a new user is confronted with a bewildering range of jargons, drawn from the cultures of hacking, computer science, information security, narcotics, anarchist or libertarian philosophy, and teenage masculinity.

The perceived benefits of accessing these networks, however, include the implied freedoms of anonymity, giving rise to real, raw, authentic communication that transcends the strictures of Clear

Web communication. There is a mythology of a deeper reality—one that pierces the veils of corporate media, state propaganda, and social norms—only accessible on the Dark Web, of answers to questions about government and corporate conspiracies, of the "real" human being emerging through online discourse. Along the way, one might be able to find real counterfeit bills, drugs, gore images, stolen credit cards, or hacker services. Complicating this quest for the authentic are hosts of scammers, frauds, and pranksters, as well as undercover law enforcement agents and tourists (in the form of academics and journalists). To be a legit Dark Web user is to be able to navigate these networks and to command restricted vocabularies. Such symbolic and cultural capital can be parlayed into economic benefits, including administrative roles on Dark Web sites or government, academic, or journalism jobs.

The remainder of this book is an exploration of the intersection between the Dark Web, these forms of legitimacy, and the symbolic economy of meanings that traffic across the three legitimacies.

Notes

1. Willard Foxton, "If Silk Road Was a Legitimate Startup, It Would Be Worth ~$2.4 Billion," *Business Insider*, October 4, 2013, http://www.businessinsider.com/silk-road-valuation-worth-2-or-3-billion-2013-10.

2. Ibid. (note that *Business Insider* has since removed its comments section).

3. Glenn McGrath, "[Freenet-chat] Deep Philosophical Question," Freenet-chat mailing list, January 2, 2002, https://emu.freenetproject.org/pipermail/chat/2002-January/000604.html.

4. Cara McGoogan, "Dark Web Browser Tor Is Overwhelmingly Used for Crime, Says Study," *Telegraph*, February 2, 2016, http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/.

5. "Crime Problems," I2P FAQ, Ugha.I2p [wiki], February 23, 2015, http://ugha.i2p/CrimeProblems[I2P].

6. Philippe Mallein and Yves Toussaint, "L'intégration Sociale Des Technologies d'information et de Communication: Une Sociologie Des Usages," *Technologies de l'information et Société* 6, no. 4 (1994): 315–335.

7. Guillaume Latzko-Toth, "The Socialization of Early Internet Bots," in *Socialbots and Their Friends: Digital Media and the Automation of Sociality*, ed. Robert W. Gehl and Maria Bakardjieva (New York: Routledge, 2016), 51.

8. Max Weber, *From Max Weber: Essays in Sociology*, ed. C. Wright Mills and Hans Heinrich Gerth (New York: Oxford

University Press, 1946), 78.

9. Ibid.

10. Ibid., 80.

11. C. Fred Alford, "What Would It Matter If Everything Foucault Said about Prison Were Wrong? Discipline and Punish after Twenty Years," *Theory and Society* 29, no. 1 (2000): 141.

12. Herbert Wulf, "Challenging the Weberian Concept of the State: The Future of the Monopoly of Violence" (Occasional Paper Series, Australian Centre for Peace and Conflict Studies, Brisbane, 2007), 5, http://www.mobi.tamilnet.com/img/publish/2008/01/h_wulf_occ_paper_9.pdf.

13. Christopher J. Finlay, "Legitimacy and Non-State Political Violence," *Journal of Political Philosophy* 18, no. 3 (September 1, 2010): 287, doi:10.1111/j.1467-9760.2009.00345.x.

14. Jonathan Jackson et al., "Monopolizing Force? Police Legitimacy and Public Attitudes toward the Acceptability of Violence," *Psychology, Public Policy, and Law* 19, no. 4 (November 2013): 480, doi:10.1037/a0033852.

15. Ibid.

16. Chandan Reddy, *Freedom with Violence: Race, Sexuality, and the US State* (Durham, NC: Duke University Press, 2011), 37.

17. Jackson et al., "Monopolizing Force?," 479.

18. François Bourricaud, "Legitimacy and Legitimization," *Current Sociology* 35, no. 2 (1987): 63.

19. Rodney Barker, *Legitimating Identities: The Self-Presentations of Rulers and Subjects* (New York: Cambridge University Press, 2001), 2.

20. Bryan S. Turner, "Nietzsche, Weber and the Devaluation of Politics: The Problem of State Legitimacy," *Sociological Review* 30, no. 3 (August 1, 1982): 374, doi:10.1111/j.1467-954X.1982.tb00659.x.

21. Jessica Beyer and Fenwick McKelvey, "You Are Not Welcome Among Us: Pirates and the State," *International Journal of Communication* 9 (2015): 893, http://ijoc.org/index.php/ijoc/article/view/3759.

22. Armand Mattelart, *Networking the World, 1794–2000*, trans. Liz Carey-Libbrecht and James A. Cohen (Minneapolis: University of Minnesota Press, 2000), 92.

23. Yochai Benkler, "Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate," *Harvard Civil Rights–Civil Liberties Law Review* 46 (2011): 311.

24. Jack Bratich, "User-Generated Discontent," *Cultural Studies* 25 (September 2011): 621–640, doi:10.1080/09502386.2011.600552.

25. Weber, *From Max Weber*, 82.

26. Matthew V. Tilling, "An Overview of Legitimacy Theory" (Commerce Research Paper Series, Flinders University, Adelaide, South Australia, 2004), http://www.flinders.edu.au/sabs/business-files/research/papers/2004/04-6.pdf.

27. Mark C. Suchman, "Managing Legitimacy: Strategic and Institutional Approaches," *Academy of Management Review* 20, no. 3 (1995): 574.

28. Eero Vaara and Janne Tienar, "A Discursive Perspective on Legitimation Strategies in Multinational Corporations," *Academy of Management Review* 33, no. 4 (2008): 3.

29. Shuili Du and Edward T. Viera Jr., "Striving for Legitimacy Through Corporate Social Responsibility: Insights from Oil Companies," *Journal of Business Ethics* 110, no. 4 (September 27, 2012): 414, doi:10.1007/s10551-012-1490-4.

30. Roy Suddaby and Royston Greenwood, "Rhetorical Strategies of Legitimacy," *Administrative Science Quarterly* 50, no. 1 (2005): 38.

31. Martin Ruef, "The Emergence of Organizational Forms: A Community Ecology Approach," *American Journal of Sociology* 106, no. 3 (2000): 661.

32. Elanor Colleoni, "CSR Communication Strategies for Organizational Legitimacy in Social Media," *Corporate Communications* 18, no. 2 (2013): 228–248; Du and Viera, "Striving for Legitimacy."

33. Blake E. Ashforth and Barrie W. Gibbs, "The Double-Edge of Organizational Legitimation," *Organization Science* 1, no. 2 (1990): 182.

34. Du and Viera, "Striving for Legitimacy," 2.

35. Erwin van der Aart, "The Influence of Legitimacy on Access to Resources: A Case Study" (master's thesis, University of Twente, Netherlands, 2015), 14, http://essay.utwente.nl/68653/.

36. See the collection of definitions of "legit" at *Urban Dictionary*, accessed May 31, 2017, https://www.urbandictionary.com/define.php?term=legit.

37. Pierre Bourdieu, *The Field of Cultural Production: Essays on Art and Literature* (New York: Columbia University Press, 1993), 113.

38. Michael Stevenson, "The Cybercultural Moment and the New Media Field," *New Media and Society* 18, no. 7 (August 1, 2016): 1091, doi:10.1177/1461444816643789.

39. Leigh Roche, "Authenticity," *Philosophy Now* 92 (November 26, 2012): 31, my emphasis.

40. Bourdieu, *The Field of Cultural Production*, 116.

41. Elizabeth Currid-Halkett, *Sum of Small Things: A Theory of the Aspirational Class* (Princeton, NJ: Princeton University Press, 2017), 18.

42. Alice Emily Marwick, *Status Update: Celebrity, Publicity, and Branding in the Social Media Age* (New Haven, CT: Yale University Press, 2013), 91.

43. Ibid.

44. Ibid.

45. Thomas Luckmann, "Comments on Legitimation," *Current Sociology* 35, no. 2 (June 1, 1987): 111, doi:10.1177/001139287035002011.

46. Barker, *Legitimating Identities*.

47. Foxton, "If Silk Road Was a Legitimate Startup."

48. Tristan Pollock, "Silk Road Was the Fastest Growing Online Marketplace Ever—Here's Why," *500 Startups* (blog), October 27, 2015, http://500.co/silk-road-marketplace-growth/.

49. Chris Matthews, "The War on Drugs Comes to Corporate America," *Fortune*, December 2, 2014, http://fortune.com/2014/12/02/drug-war-corporate-america-silk-road/.

50. See Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no. 1 (January 2, 2016): 7–38, doi:10.1080/00396338.2016.1142085, for the original academic article.

51. Bourdieu, *The Field of Cultural Production*.

52. Roger David Price, *The French Second Empire: An Anatomy of Political Power* (Cambridge: Cambridge University Press, 2007), 272.

53. Ann Twinam, *Public Lives, Private Secrets: Gender, Honor, Sexuality, and Illegitimacy in Colonial Spanish America* (Stanford, Calif.: Stanford University Press, 1999).

54. For example, see a recent change in Georgia law regarding fathers of children born out of wedlock: "New Child Legitimation Law a Success," Georgia Department of Human Services, September 1, 2005, https://dhs.georgia.gov/new-child-legitimation-law-success.

55. Colin Koopman, *Genealogy as Critique: Foucault and the Problems of Modernity* (Bloomington: Indiana University Press, 2013); Michael Mahon, *Foucault's Nietzschean Genealogy: Truth, Power, and the Subject* (Albany: State University of New York Press, 1992).

56. Jay David Bolter and Richard Grusin, *Remediation: Understanding New Media* (Cambridge, MA: MIT Press, 2003).

57. Geoff Bowker, "How to Be Universal: Some Cybernetic Strategies, 1943–70," *Social Studies of Science* 23, no. 1 (1993): 116.

58. Fred Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism* (Chicago: University of Chicago Press, 2008).

59. Marouf Hasian, Sean T. Lawson, and Megan McFarlane, *The Rhetorical Invention of America's National Security State* (Lanham, MD: Lexington Books, 2015), 18.

60. Monica A. Zimmerman and Gerald J. Zeitz, "Beyond Survival: Achieving New Venture Growth by Building Legitimacy," *Academy of Management Review* 27, no. 3 (2002): 419.

61. See chapter 5 of Greg Elmer, *Profiling Machines: Mapping the Personal Information Economy* (Cambridge, MA: MIT Press, 2004).

62. B. S. Turner, "Nietzsche, Weber and the Devaluation of Politics."

63. Martin C. Libicki, David Senty, and Julia Pollak, *H4cker5 Wanted: An Examination of the Cybersecurity Labor Market* (Santa Monica, CA: RAND, 2014).

64. Whitney Anspach, Kevin Coe, and Crispin Thurlow, "The Other Closet?: Atheists, Homosexuals and the Lateral Appropriation of Discursive Capital," *Critical Discourse Studies* 4, no. 1 (April 2007): 95–119, doi:10.1080/17405900601149509; Helene A. Shugart, "Counterhegemonic Acts: Appropriation as a Feminist Rhetorical Strategy," *Quarterly Journal of Speech* 83, no. 2 (1997): 210–229.

65. Baruti N. Kopano, "Soul Thieves: White America and the Appropriation of Hip Hop and Black Culture," in *Soul Thieves*, ed. Tamara Lizette Brown and Baruti N. Kopano, Contemporary Black History (New York: Palgrave Macmillan, 2014), 1–14, doi:10.1057/9781137071392_1.

66. Steve Redhead and John Street, "Have I the Right? Legitimacy, Authenticity and Community in Folk's Politics," *Popular Music* 8, no. 2 (May 1989): 179, doi:10.1017/S0261143000003366.

67. Regina Bendix, *In Search of Authenticity: The Formation of Folklore Studies* (Madison: University of Wisconsin Press, 1997).

68. Statewide Patrol, accessed July 6, 2016, http://www.statewidepatrol.com/mobile-patrol-services.

69. Naomi Sussmann, "Can Just War Theory Delegitimate Terrorism?," *European Journal of Political Theory* 12, no. 4 (October 1, 2013): 440, doi:10.1177/1474885112464478.

70. Norma C. Ware, “Suffering and the Social Construction of Illness: The Delegitimation of Illness Experience in Chronic Fatigue Syndrome,” *Medical Anthropology Quarterly* 6, no. 4 (1992): 350.

71. Karen A. Hegtvedt and Cathryn Johnson, “Power and Justice: Toward an Understanding of Legitimacy,” *American Behavioral Scientist* 53, no. 3 (November 1, 2009): 376, doi:10.1177/0002764209338798.

72. Keith Ansell-Pearson, *An Introduction to Nietzsche as Political Thinker: The Perfect Nihilist* (New York: Cambridge University Press, 1994), 174.

73. Ashforth and Gibbs, “The Double-Edge,” 183.

74. Mallein and Toussaint, “L’intégration Sociale.”

75. Eileen Ormsby, “Waiting in the Red Room,” *All Things Vice* (blog), August 29, 2015, https://allthingsvice.com/2015/08/29/waiting-in-the-red-room/.

76. Patrick Howell O’Neill, “Tor’s Ex-Director: ‘The Criminal Use of Tor Has Become Overwhelming,’” *Cyberscoop*, May 22, 2017, https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop/.

3 The Dark Web Network Builders

This chapter covers Dark Web development from two primary angles. First, drawing on archives such as e-mail lists, IRC logs, and software repositories, I detail the development history of the three Dark Web projects discussed throughout this book: Freenet, the Tor Project, and the Invisible Internet Project (I2P). The histories I present here are brief and focus mainly on the development of the specific technologies in question, considering how the projects develop networks that can anonymize both readers and publishers. I also emphasize the early stages of web publishing on these networks, the practice that has become known as Dark Web publishing. Freenet, Tor, and I2P were built in the late 1990s and early 2000s in relation to previous networking technologies, including the World Wide Web. Indeed, the World Wide Web, with its ease of publishing hypertextual media, looms large in the Dark Web network builders' imaginations. These systems were strongly bent toward supporting WWW-like publishing, with the twist of anonymizing both publishers and readers and even decentralizing web hosting. A study of these network builders, even the brief one that appears in this chapter, can shed light on the technical and social roots of Dark Web practices and systems, such as markets, search engines, and social networking sites, which are covered in later chapters.

Second, I consider the projects' places within the three legitimacies theorized throughout this book, namely violence, propriety, and authenticity. I explore the relationship between these projects and states, how these projects appear as organizations, and the struggles over authenticity as project developers contest one another's network designs. If legitimacy (across all three registers) is about communication and power, then we must attend to how the Dark Web network builders have engaged in complex negotiations with state violence, organizational propriety, and the performative

dimensions of being authentic, legit anonymity software developers. The stakes are high: to survive, these organizations must construct their legitimacies through the symbolic economy and fend off challenges to them.

Freenet: The Web, Decentralized and Anonymized

In its first decade (1989–1999), the World Wide Web's popularity grew at an explosive rate. It was a cultural phenomenon that attracted a great deal of attention from computer scientists. One such scientist was Ian Clarke, a master's student in computer science at the University of Edinburgh. In 1999, he defended his thesis, titled "A Distributed Decentralised Information Storage and Retrieval System."[1] The thesis is notable because of its somewhat unorthodox description of the World Wide Web. For Clarke, the WWW is a "key-indexed [information] storage and retrieval system … [allowing] anyone connected to the Internet to retrieve information corresponding to a key."[2] As he explains, "The key used to access a piece of information is known as a Uniform Resource Locator (URL), and as the name suggests, it essentially represents the computer on which the information resides, as well as the location within that computer where the information can be found."[3] This is a peculiar description of the World Wide Web. The web is often described as a graphical interface to the Internet, or as a context for hypermedia (that is, media objects that can be linked to one another); it is not typically described in terms of keys. But Clarke's description is accurate: files on the web are found via URLs, which provide to a web browser the scheme (i.e., a protocol, such as HTTP), the server, the directories on the server, and the name of the file itself. The web does indeed function as a key-based storage and retrieval system.

Although Clarke's thesis praises the web for its efficiency in allowing users to retrieve information with a URL/key, he also has critiques:

- The web relies on a centralized addressing system, namely the domain name system (DNS). This system endows its administrators with too much power over the registration of

valuable names (e.g., http://www.realty.com or http://www.porn.com), and no technical barrier prevents an administrator from censoring a web server by removing it from the DNS.

- Popular pages on the web can be made inaccessible if too many clients request them; the web server hosting them can be overwhelmed with traffic. This is another central point of failure.
- WWW servers can be identified by their IP addresses; thus, there is no anonymity for publishers.
- Computers that request data from servers can also be identified by their IP addresses; thus, there is no anonymity for readers.

Clarke's critique identifies two key problems of the World Wide Web: centralization and lack of anonymity. Both could lead to "our lives being monitored, and our thinking manipulated and corrupted to a degree that would go beyond the wildest imaginings of Orwell."[4] If our reading habits and publications are always tied to us, Clarke reasons, powerful entities such as governments or corporations could use that information to control us. Moreover, if the web relies on centralized infrastructures, such as DNS, blocking access to particular sites—say, those critical of ruling parties and leaders—is trivial.

Clarke's thesis describes an alternative to the web, Freenet, which offers weblike information publishing and retrieval performance while radically changing the relationship between keys and information. Just as he had drawn inspiration from the web, he also drew inspiration from open-source models of production; a few months after defending his thesis, he started the Freenet Project, posting his thesis online and recruiting a team of programmers to implement Freenet in Java.[5]

Development of Freenet moved rapidly. In May 2000, the team released a beta version. By the time Clarke published a coauthored paper on Freenet in *IEEE Internet Computing* in 2002, the team had reached a 0.4 release (the current release is 0.75), had run

simulations of Freenet using 200,000 nodes, and had been covered by the *Guardian*, the *New York Times*, *Salon*, and *New Scientist*. Freenet was even mentioned in a *Doonesbury* comic strip.[6]

So how does Freenet work? The system allows file uploading and downloading while attempting to protect user identity in several ways:

- Freenet is a peer-to-peer network comprising nodes. Following the small-world topology, each node connects to a small number of neighbor nodes as well as random distant nodes.[7] Thus any given node has a map of the logical location of only a small collection of nodes; no node has a complete map of the network.
- Information is distributed across the Freenet network and stored as encrypted files on Freenet nodes. Every node participates in the storage of data; however, node operators cannot decrypt the data on their nodes. This enables distributed storage of massive amounts of data, while giving node operators plausible deniability about data their nodes contain.
- Files are located not by addresses (which, as in DNS, resolve to specific locations on the network) but by unique keys. For example, an HTML file such as "hacking.html" might be identified by the key A1B2C3.[8] This key is generated mathematically based on the digital content of the file (i.e., its 1s and 0s)—not the semantic content (i.e., the human-readable content of the file). This file would be stored with other files based on the similarity of their keys, say A2B2C3 and A1B3C3. The files are distributed to Freenet nodes and stored in an encrypted directory. Users who access them do not know where in the network they are stored.
- Publishing to the network involves "inserting" a file. Freenet creates the key for the file based on the digital content, and then pushes the file to nodes with files that have similar keys.

- As files are requested, they are cached on nodes along the path between requester and server. Thus, popular files become distributed across the network rather than being stored in only one location.

To summarize, using a quotation that Freenet developers proudly repeat, Mr. Bad of *PigDog Journal* calls Freenet "a mix of Usenet, the web, and a RAID disk system, all fudged up into a super-crypto wet dream."[9]

Freenet and the World Wide Web clearly have multiple differences. Files on the web are found through a centralized addressing scheme (the DNS), while files on Freenet are found through a small-world search of keys, thus distributing across the network knowledge about what information is where.[10] Whereas the domain name system enables DNS operators to have global views of the web network, Freenet's peer-to-peer structure limits any given node's knowledge of the network to a small collection of neighbor nodes. On the web, information is accessible via domain names that are registered with companies such as Network Solutions; on Freenet, information is found based on keys generated from files themselves. Freenet files are distributed across the network based on these keys in such a way that no one knows the physical location of the files, but anyone can find them logically with the key. Moreover, on the web, only one copy of a file might be available; for example, a web server might have the only version of a particular PDF. If that file becomes popular, the web server providing it could get overloaded with requests. In Freenet, popular files are copied and distributed across the network as they are requested.

These Freenet features all enable users to publish and access files —including MP3s, images, videos, and text—anonymously. A user can "insert" a file into the network; this file will be stored in a logical location (based on its key) but the publisher of that information will not know where it is physically stored. Another user can access that file based on its key, but will not know where the file is coming from, only that it's available.

Although Clarke's thesis compared Freenet to a new, decentralized World Wide Web, in the time between his thesis and Freenet development, file-sharing systems became big news, especially when Napster became popular. Press coverage of Freenet in the early 2000s likened it to an anonymous Napster, noting that Freenet's protection of publisher and reader identities would protect distribution of pirated intellectual property. Indeed, Clarke likely provoked such coverage, especially with his anticopyright proclamations, such one quoted in a 2000 article in the *New York Times*: "If this whole thing catches on, … I think that people will look back in 20 to 40 years and look at the idea that you can own information in the same way as gold or real estate in the same way we look at witch burning today."[11]

As intriguing as file sharing is, my focus in this book is on anonymous web hosting and reading. Given that Clarke's thesis drew inspiration from the World Wide Web, it's not surprising that web-hosting applications were developed early in Freenet's history. One of the first notable developments was Fproxy, part of the 0.2 release in May 2000. Fproxy functions as an HTTP proxy, allowing Freenet users to browse Freenet files with a web browser, as opposed to, say, navigating Freenet files with a command line interface. As Ian Clarke puts it, this takes "advantage of your web browser's talents for presenting information."[12] HTML files quickly appeared on the network, with three being listed in a key index in May 2000: a Swedish copy of Peter Singer's *Animal Liberation*, the U.S. Constitution, and the Unabomber manifesto.[13]

These were simply "ports" on Freenet to access HTML files. Soon, native Freenet web publishing—now called freesite publishing—was developed. In March 2001, David McNab authored FreeWeb, a program to bundle HTML, CSS, and media files in freesites that could be inserted into the network.[14] FreeWeb was superseded in 2006 by jSite, built by Freenet developer Bombe.[15] According to Internet Archive snapshots of web-to-Freenet proxies, early freesites included the Content of Evil and the Content of Good. Today, according to Enzo's Index (a freesite crawler/indexer,

discussed further in chapter 5), there are more than four thousand freesites, though about 20 percent are not active.[16] These sites include personal “flogs” (Freenet blogs), social networking systems, porn sites, radical political tracts, and media-sharing sites.

The Tor Project: From Free Haven to Hidden Services

Freenet inspired a predecessor to the Tor Project: Free Haven, a system envisioned by MIT-trained computer scientist Roger Dingledine. Dingledine drew from Freenet's data storage possibilities to conceive of Free Haven as a "data haven," a place to securely and anonymously store files for lengthy periods.

The Free Haven Project began in late 1999 as Dingledine, then a graduate student in computer science at MIT, began discussions with MIT undergraduates (notably Michael Freedman) and one Harvard undergrad, David Molnar, about an information publishing system that would (a) store documents for long periods and (b) allow for both anonymous publication and reading. Dingledine led the way, posting drafts of specification and requirements that would eventually result in his master's thesis as well as a collaborative paper presented at the Workshop on Design Issues in Anonymity and Unobservability in Berkeley, California, in July 2000 (a workshop also attended by Freenet creator Ian Clarke).[17]

Both Dingledine's thesis and the Berkeley paper describe Free Haven as "anonymous storage which resists the attempts of powerful adversaries to find or destroy any stored data."[18] The developers' goals were to protect dissidents, critics of powerful institutions, and anyone who would otherwise have their privacy violated through Internet surveillance. Although this sounds similar to Freenet's goals, Dingledine, Freedman, and Molnar distinguished Free Haven from Freenet in terms of "persistence of data": "We distinguish storage from publication in that storage services focus less on accessibility and more on persistence of data."[19] In other words, while Freenet focuses on publishing data by storing highly requested files, Free Haven would store files for as long as authors wanted them to be stored. Dingledine, Freedman, and Molnar used an economic approach, proposing that Free Haven servers would exchange storage space for the right to publish data on the network.

Anonymous connections between servers would be achieved through mix-net, a system originally designed for anonymous e-mails and phone calls.[20] Dingledine and his collaborators also developed a complex set of definitions for anonymity, including *author anonymity, publisher anonymity, server anonymity, document anonymity*, and *query anonymity*.[21]

Free Haven coding began in February 2000, but Dingledine, Freedman, and Molnar quickly discovered many technical challenges that could not be overcome. One involved their stated goal of establishing the credibility and accountability of Free Haven servers: if anonymous server operators agreed to store data for a length of time, what would happen if they decided to delete the data or disappear from the network? Such accountability in peer-to-peer anonymized networks is difficult to enforce.[22]

Another problem arose at the communication/transport layer: mix-nets were proving to be very slow and unreliable. Writing in the Free Haven developer's mailing list, Dingledine lamented, "The current mix-net infrastructure has unbearably high latency and is rumored to have low reliability. In any case, it's hard to use and not very well set up. The amount of actual privacy gained from the current implementations is not well understood."[23] Around April 2003, the Free Haven Project was put on the back burner while these and other problems were being investigated.[24]

In the meantime, Dingledine had become involved in another effort: onion routing, first described in 1996 as a means to anonymize communication between two entities.[25] It was developed by researchers working for the U.S. Naval Research Lab, notable among them Paul Syverson. The "onion" is reflected in the use of multiple layers of encryption that get "peeled" back as data is relayed across a network. "Routing" is also important: data is routed through a circuit of relays, each of which knows only the identity of the previous node in the circuit and the next immediate hop. A key application of onion routing was what Dingledine, Freedman, and Molnar might call "reader anonymity": anonymous web browsing,

protecting readers of websites from being identified by web servers or intermediaries.

The Free Haven documents refer to onion routing as a possible solution for anonymous communications, but they suggest that onion routing would not anonymize to the degree that mix-nets would. The document recognized, however, that onion routing provides one key advantage: far lower latency. As such, it was seen as a possible answer to the problems of mix-nets. Moreover, Dingledine furthered his knowledge of onion routing capabilities after he began working for Paul Syverson in 2002.[26]

Dingledine soon began putting more effort into onion routing. Drawing on the work of Matej Pfajfar, a Cambridge undergraduate honors student, Dingledine and other developers, notably Nick Mathewson, implemented The Onion Router version 0.0.0, released in September 2002.[27] Although there were multiple other implementations of onion routing, Dingledine dubbed their version *The* Onion Router, arguing that it was "the actual onion-routing project, started out of the Naval Research Lab. ... Tor *is* onion routing."[28] This name would stick and eventually become Tor.[29]

Onion routing on its own, however, could not address a key idea of Free Haven: the anonymity of data publishers. Onion routing helps anonymize readers, but not necessarily publishers: readers using Tor can access and hide their identity from Clear Web sites. In contrast, a web publisher faces the problems Ian Clarke identified, namely, having to use the DNS to publicly register the website's location and metadata. In 2003, Dingledine and Mathewson took on this problem with a concept called "rendezvous points."[30] Rendezvous points allow for anonymous web hosting—that is, Dark Web hosting—on what Dingledine and Mathewson called "location-hidden services" or "hidden services" for short.[31] Much like Freenet, Tor hidden services are identified by a hash of part of the site's public key (a public key corresponding to the server owner's private key). The hidden service advertises this key to "introduction points." A reader wishing to visit this hidden service would inquire about it through those introduction points, which would help connect the

client to the hidden server via a rendezvous point.[32] And, like Freenet, all of this avoids the public DNS. “Hence, connecting to a hidden service ensures the anonymity and privacy of both users—and, remarkably, the service provider—unless, of course, either party decides to reveal his or her identity.”[33]

Thus, much like Freenet, one of the key features developed early in the history of Tor was a Dark Web implementation. Location-hidden services on the Tor network were publicly announced in a 2004 paper by Dingledine, Mathewson, and Syverson. Interestingly, the dream of Free Haven reappears in this paper: “Tor’s rendezvous points enable connections between mutually anonymous entities; they are a building block for location-hidden servers, which are needed by Eternity and Free Haven.”[34] Free Haven was never implemented, but Tor hidden services took on a life of their own. One of the first—if not the first—hidden websites was the Hidden Wiki, used by Tor developers and users to document Tor.[35] By 2016, thousands of Tor-based Dark Web sites were up and running, including blogs, social networking sites, search engines, markets, whistleblowing sites, and image sharing sites.

I2P: From Invisible IRC to Invisible Internet

While Dingledine drew inspiration from Freenet's capacity as a data storage system, another privacy-oriented developer, Lance James (known by handles such as 0x90, no-operation, and nop) took a different perspective. While James found Freenet to be "an awesome solution to anonymous expression," he also argued that it was a very slow system, with long gaps between user interactions—in other words, a high-latency system: "I liked the idea [of Freenet], got to know some of the developers there … but there were issues that I had with it. I'd like to be able to talk to people live … not having to wait 24 hours to hear back from somebody."[36] In an interview on the *InfoSec Daily Podcast* in 2012, James says that, in contrast to Freenet's World Wide Web–style model, "I was trying to build a more dynamic, light volume, real-time, instant messaging system. So I figured, 'Why rewrite the instant messaging part? Why don't we use [Internet Relay Chat]?' And [we could] build a distributed proxy system around it that could mask where the IRC server was and mask the users themselves."[37] Thus, while Dingledine focused on data storage, James drew inspiration from Freenet's interpersonal communication potentials—slow though they were. He grew frustrated with waiting for Freenet conversations to develop, so he sought to apply anonymization to IRC.

Internet Relay Chat is a text-based chat application that runs over the Internet. IRC began in 1988 in Finland and quickly grew, with hundreds of thousands of people using it worldwide by the mid-1990s. Unlike the web of the nineties, which was largely seen to be a static medium, IRC provided a high degree of what Esther Weltevrede, Anne Helmond, and Carolin Gerlitz call "real-timeness," or a particular "understanding of time that is embedded in and immanent to platforms, engines and their cultures."[38] Weltevrede, Helmond, and Gerlitz note that there is no such thing

as “real time” in any mediation, but a sense of “real-timeness” emerges through the “continuous movement of new content, its request and display in devices, as well as the engagement by users through [network] activities and the filtering of content based on freshness and relevance.”[39] Taking up this term, we could say that the World Wide Web of the 1990s had less “real-timeness” than IRC, which provided a text-based mediated experience that approached the speed of face-to-face conversation.

With its file-based model, Freenet in the early 2000s lent itself to anonymous file sharing and freesite publication. Anyone seeking the latest Britney Spears or Eminem MP3s could wait a few hours for the file to download (especially considering the download was anonymous). Likewise, anyone wishing to learn more about the Principality of Sealand could wait a few minutes to download that freesite.[40] Low-latency interpersonal interaction, in contrast, was not Freenet’s strength.[41]

Seeking to combine low-latency communication with anonymity and thus achieve a higher level of real-timeness than Freenet allowed, James conceived of the Invisible IRC Project (IIP) in October 2001.[42] IIP was designed to hide a user’s Internet protocol address from server operators, replacing the real IP with 127.0.0.1 (i.e., localhost).[43] Similarly, the IP addresses of the IIP servers were hidden from end users: “The relays act kind of like a firewall for the actual server, no one knows where the server is. The concept I came up with as a viable solution in a centralized concept was: hide the server from the users, hide the users from the server.” The result was an anonymizing IRC system. Given that James was also using Freenet (indeed, he shared the IIP code on Freenet first), it’s not surprising that Freenet users were the most common IIP users in 2001–2002, using IIP to exchange Freenet file keys.[44]

Using the open-source model, James shared the IIP code and began to recruit other developers and organize, using a mailing list, CVS (a software version system), and weekly IRC development meetings. The developers released a stable end user–oriented version in early 2003.[45] James had a larger vision for anonymous

communication than just anonymous IRC, however, a vision he called the Invisible Internet Project:

> The Invisible Internet Project: Defined as the "New Internet."... We plan to re-design the Internet by taking it a step further and having security and privacy be first priority. ... This, in essence will be an impenetrable neural-network, that is self-driven, self-defensed, and completely seamless to already applied protocols, specifically client to server. ... It will be THE next transport layer, a layer on top of the notoriously insecure Internet, to deliver full anonymity, privacy, and security at the highest level possible. Decentralized and peer to peer ... the Internet that should have been, will be soon.[46]

Notable here are concepts such as "decentralization" and "seamless to already applied protocols": this vision was similar to Freenet's in that it repudiated the centralized client-server model that dominated the Internet, and yet it would allow for many existing Internet protocols (e.g., TCP, HTTP, SMTP) to run on it.

Not long after the initial release of IIP, this vision would start to take shape. At the 47th IIP developer meeting held in July 2003, James and another developer, jrandom, announced the "anonCommFramework."[47] As jrandom explained in the meeting, "Briefly, anonCommFramework is a meta-network. a generic set of protocols & structures that an anonymous communication network could use to interoperate to provide militant grade anonymity." Like Freenet, the anonCommFramework—which would become known as I2P, or the Invisible Internet Project—would be anonymizing and decentralized.[48] Unlike Freenet, it was intended to be a multipurpose low-latency communications system. In other words, it was intended to be faster than Freenet and allow for multiple communications protocols.

Jrandom began work on I2P in earnest, posting draft specifications for the project days after the 47th IIP developers meeting.[49] Judging from the developer meeting logs and mailing list, jrandom worked feverishly at the task, even announcing in a

developer's meeting that he quit his day job to pursue I2P work full-time.[50] After hosting meetings to debate the specs, jrandom and other I2P developers began implementing the network in Java (the same language as Freenet).[51] By September, the router (a core part of the architecture) was implemented, and by early November, a functional version of I2P was released.[52]

While I2P was designed to support many existing Internet protocols, an early development that excited jrandom and other developers was anonymous web hosting.[53] By mid-November 2003, developer TC (or TheCrypto) was hosting a forum at tc.i2p.[54] "Tc's site is awesome & really reliable!" exclaimed jrandom in one developer meeting.[55] I2P-hosted sites, referred to as "eepsites," rely on HTTP and can be accessed with a browser configured to use the I2P router. Rather than paying a web host (as many people do with current World Wide Web publishing), users wishing to host an eepsite can do so by adding HTML, CSS, and media files to a folder on their own computers and turning on the I2P HTTP server. All this is done via a graphical interface (making it more user friendly than even Tor's simple config file modification process). After the server is turned on, visitors can load the eepsite by entering its key into its address book or browser URL; the I2P router then builds a temporary encrypted "tunnel" through other I2P peers from the client to the server, which in turn sends messages back to the client through a separate tunnel.[56] By March 2004, I2P's software package included a hosts.txt file (which associates 516-character keys with human-readable domain names) listing forty eepsites.[57] As of this writing, around eight hundred are available.[58] Thus, although I2P can support many network applications (BitTorrent, e-mail, and of course IRC), a core use is as a Dark Web.[59] And, much like Freenet and Tor, the domain names used in I2P are distinct from the public DNS.

Although Lance James proposed the original vision of a "New Internet" Invisible Internet Project, he did not remain with the project. After jrandom took the lead in developing I2P, James

continued work on the original program, IIP, but eventually left both projects entirely by mid-2004, citing his dislike of Java and, more importantly, his differences with jrandom over cryptography implementation and the overall goals of I2P.[60]

Jrandom also left I2P, only a bit more suddenly. After leading development from versions 0.2 in 2003 to 0.6.1.30 in 2007, jrandom left the project in November 2007.[61] His departure was nearly disastrous because only jrandom had I2P's public web server key, contract with the hosting company, and all the project passwords.[62] The project recovered, however, with developers finding new public web server space, building a 0.7 release (a milestone release with many improvements to the networking protocols), and promoting I2P on Twitter. Currently, I2P is being led by zzz, who began working on the network in 2005.[63] In 2015, the team held the first I2PCon, in Toronto, where many of the developers shared their work on Android applications, cryptography algorithms, and the overall history and future of the network.[64]

Legitimacies among the Network Builders

Here, I trace out the place of these projects within the larger contexts of violence, propriety, and authenticity—the three legitimacies I'm concerned with throughout this book. My ultimate argument is that Freenet, Tor, and I2P have sought to establish their legitimacy in relation to the three registers, using various symbolic economic practices of inheritance, exchange, and delegitimation. I argue that if these organizations fail to negotiate with state violence, fail to command respect and resources, and fail to develop legit software, they will not succeed in their missions to develop anonymizing technologies.

Violence

Like the other forms of legitimacy, state legitimacy is communicative at its core: governments make claims that they, and they alone, should be able to use violence to help maintain social order, whether military violence against external enemies who threaten the state's social order, or internal violence to arrest, imprison, and execute criminals. These claims are often contested, and mediated communication becomes a key site where these constructions and contests take place.

Mediated communication is a significant way in which the builders of Freenet, Tor, and I2P figure into the symbolic economy of state legitimacy. The developers of these networks—including Clarke, Dingledine, James, and jrandom, but also many other contributors—argue that these systems protect the communications of anyone who challenges state power. They contend that their respective networks improve on the Internet's ability to allow more political debate. In this way, the developers are explicitly engaging with questions of state legitimacy and violence: they derive their legitimacy in part by presenting their projects as a means to challenge excessive state power.

A simple way to see this is through their use of the term "dissident," a figure who is struggling against the domineering state. In such a struggle, dissidents use whatever media they can to get messages out. The network builders of Freenet, Tor, and I2P all argue that their systems make this dissidence possible.

Freenet developers, for example, believe that their system ought to help the "lone dissident in the middle of Tibet."[65] Running a Freenet node provides "a service to Chinese and Saudi dissidents who need a safe haven for documents and access to news from other countries."[66] Tor's developers make similar arguments, noting that running a Tor exit node can be justified with a "'we're helping Chinese dissidents …' angle."[67] Tor developers speak of their "beloved Chinese dissident" nicknamed "Jane Chinese Dissident."[68] I2P developers, likewise, work to make their technology easy for the "average dissident" to use.[69] They express concerns that I2P be able to protect the "dissident or threat to the government," which is a tough task because these technologies must withstand the analysis and infiltration of a "dedicated state-level adversary."[70] As one developer argues, I2P development is "a necessary first step … to facilitate the applications we may later need to overcome tyranny and oppression."[71]

In terms of a symbolic economy of legitimacy, these projects engage in a double move. First, they appropriate the figure of the Chinese or Saudi dissident to bolster their claims of protecting democratic discourse against overbearing state violence. For the network builders, the actual activities of dissidents (in whatever context) is not important; rather, the possibility that such dissidents might use Freenet, Tor, or I2P is justification for the development of anonymizing networks. Network builders also delegitimate governments who engage in censorship and oppression, such as China and Saudi Arabia, as a way to bolster their own claims to legitimacy. For the network builders, the stakes are high: if an oppressive government is able to defeat their network, then they believe dissidents will die. Because the Dark Web systems are largely developed in the West, especially in the United States, the

arguments that Freenet, Tor, and I2P undermine non-Western governments by supporting dissidents is a means to justify the existence of Dark Web sites to developers' own governments.

But the network builders often argue that Western governments are also engaged in censorship and surveillance, especially in the wake of 9/11 and the Global War on Terror. For example, as one Freenet developer argues, Freenet is "not only for 'dissidents in china where Freenet will be outlawed anyway', it's also for our 'beloved' democratic governments which see no problems in muffling people up and tries to suppress information, often under the veil of 'national security'."[72] Thus, Freenet, Tor, and I2P present their anonymizing technologies as a means to circumvent state practices of surveillance and censorship toward the ideal of completely free political debate, wherever those practices occur. Perhaps the strongest example of this is the "militant anarchist" statement by I2P developer jrandom:

> Without exception, the right to unimpeded, uncensorable, and anonymous communication is fundamental to a free society—a society for which we strive. The so called governments of the world cannot be allowed to limit that freedom, and neither can the corporations who run their economies. Each and every one of us must be empowered with the means to assert our autonomy and secure our right to free speech. The monitoring of communication services, the censoring of published information, the exposure of individuals to the danger of retribution by breaking their anonymity, and the simple chilling effect caused by the threat of such attacks perpetrated by governments, corporations, and malicious individuals cannot be allowed to continue.[73]

Most developers don't go so far as jrandom, but their use of the "Chinese dissident" as a synecdoche for dissenters everywhere who need absolute anonymity to allow for absolute free speech—including dissenters in Western states—is a key aspect of the Dark

Web's trial of legitimacy in terms of its role in states' claims to violent power.

The state's rejoinder to the challenge made by network builders is to point to illegitimate (i.e., non-state-sanctioned) violent and exploitative content that can get shared on Tor, Freenet, or I2P. Anarchist literature, terrorist propaganda, and child exploitation images are key classes of content that states point to. As delegitimated users of violent force, terrorists are an especially important threat.[74] For example, the former FBI director James Comey argues for the state's ability to monitor online communications. If that capacity is gone, terrorists will freely use networks to operate:

> When the government's ability—with appropriate predication and court oversight—to see an individual's stuff goes away, it will affect public safety. That tension is vividly illustrated by the current ISIL threat, which involves ISIL operators in Syria recruiting and tasking dozens of troubled Americans to kill people, a process that increasingly takes part through mobile messaging apps that are end-to-end encrypted, communications that may not be intercepted, despite judicial orders under the Fourth Amendment.[75]

Comey is speaking about encryption in general, such as end-to-end encryption in mobile apps like WhatsApp. Increasingly, security researchers, such as Beatrice Berton of the European Union Institute for Security Studies, see encrypted and anonymizing Dark Web technologies as especially capable of hiding terrorist threats and activities:

> EuroGuns is [a Tor-based] online marketplace which deals in all kinds of weapons and sends them via regular mail. AK-47s—the type of assault rifle used by the Kouachi brothers in the Charlie Hebdo attacks—are sold for $550 each on EuroArms, one of the largest online black markets for purchasing weapons. In the spirit of Anwar al-Awlaki's brand of 'self-help' terrorism, several texts such as the *Terrorist's Handbook* and the *Explosives Guide* can also be purchased on AlphaBay [a now-defunct Tor-based market].[76]

In this sense, the association of particular forms of content—a listing for an assault rifle, a terrorist handbook—with illegitimate (read: non-state-sanctioned) violence is the justification for state-based surveillance of these networks, leading to the arrest, imprisonment, or execution of the propagators of that content.[77] States delegitimate the violence and the communications of terrorists in states' renewal of their claim to the legitimate monopoly on violent force as well as the right to monitor online communications. All this is done in the name of state protection of citizens.

This leads back to the initial justifications offered by network builders. First, states are engaged in surveillance of networked communication, which may aid in catching terrorists but also may lead to invasions of privacy of noncriminal citizens. Second, network builders often challenge the state's very association of particular classes of content with violence. One person's terrorists and anarchists, the network builders argue, is another's freedom fighters and revolutionaries—that is, dissidents. Third, the network builders argue, preventing people's access to information such as the *Terrorist's Handbook* does little to protect people from the physical acts of terrorists.

This cycle of technical/network development and political condemnation is often described in terms of violence: the Crypto Wars, the War for Internet Freedom, arms races, information security, attacks against the network, Anonymous hacker "operations," defense against the adversary. Multiple social groups

use this language; for example, see jrandom's standard for I2P "militant grade" anonymity in the quotation above. The adversary could be anywhere, as I2P developer zzz notes, "Where could an evil [attacker] be? They could be anywhere. They could be outside our network. They could be inside our network."[78] Compare this to statements by government officials: the terrorists could be anywhere. They could be outside the country. They could be here, now, your neighbors. They could be using computer networks right now.

As in any conflict, contradictions abound: the "state," for example, is not homogenous. For example, Nathalie Maréchal has shown that the U.S. government has taken multiple positions regarding Tor, from the Naval Research Lab's funding of it, to the NSA's attempts to break its encryption, to the State Department's promotion of it externally as part of the "Internet Freedom Agenda," and finally to the U.S. government's continuing financial support of the Tor Project.[79] This is thus not a simple networks-versus-state tension. Similarly, network builders are not all militant anarchists dedicated to the destruction of the state. For example, jrandom's free speech absolutist statement was rejected by other developers of I2P, notably IIP founder Lance James, who felt that it was too overtly anti-American.[80]

Nonetheless, struggles over the uses of anonymizing, encrypted technologies often take a stark state-versus-networks shape, and the science of making anonymizing networks becomes ossified into what Peter Galison might call a dualistic "Manichaean science," pitting good against evil.[81] The network builders thus have a difficult task: to legitimate their networks, they must claim that their networks protect their users' communications from state monitoring and thus from state violence. Even the existence of child exploitation images on these networks is used by some network builders as evidence that their networks work. As several Freenet developers argue, "There is no way to deny [anonymity] to the 'bad guys' without also denying freedom to the 'good guys'—civil rights activists, minority religious groups, or ordinary citizens who simply

wish to keep their affairs private."[82] Thus, any state effort at all to deanonymize users—"good" or "bad"—is taken to be adversarial, the actions of an adversary that can be anywhere. But with this framing, Freenet, Tor, and I2P are often condemned as antistate and thus illegitimate, meaning they must be monitored, infiltrated, or shut down. For the state, the network and its builders become reduced to the adversary. There is no end in sight for this tension.

Propriety

The network builders not only have to operate within the specific contours of state legitimacy; they also must seek legitimacy as propriety, in both senses—as proper, respectable, law-abiding organizations, and as proprietors, able to justify their abilities to capture and control resources. For these anonymizing networks, legitimacy as propriety occurs in three key ways: claiming nonprofit status, organizing labor in the open-source production model, and public presentation.

Both Freenet and Tor are registered in the United States as 501(c)(3) nonprofits; to gain such a status, the developers had to draft legally binding documents establishing their corporate structures and missions. Doing so has placed them in the long tradition of formalized U.S. civil society, in which a wide range of disparate entities—from religious charities to reproductive rights organizations to political think tanks—agree not to compete with businesses, attest that they are not formal organs of the state, and operate with donations from private entities.[83] Freenet's 2014 tax forms show that the organization's purpose is to "support freedom of speech through Internet technology and public education," and that its yearly expenditure was around $10,000.[84] The project counts Google and Electronic Frontier Foundation (EFF) founder John Gilmore among its major sponsors.

Tor has also used its nonprofit status to seek donations. It notably partnered early in its history with the EFF, which offered web hosting and financial support. Additional funds come from various foundation grants and individual donations. Its biggest source of

funds, however, has traditionally been U.S. government agencies, including the Naval Research Lab; the Defense Advanced Research Projects Agency (DARPA); and the State Department's Bureau of Democracy, Human Rights, and Labor (DRL), "though the organization is actively trying to differentiate its funding streams" by attracting non-government funders.[85] The Tor Project currently calls for donations from journalists, businesspeople, bloggers, IT professionals, and "normal people"—alongside law enforcement and military users.[86] Tor's budget is significantly larger than Freenet's, with total expenditures over $2.5 million in 2014.[87]

I2P has become a different sort of nonprofit. In contrast to Freenet and Tor, which were founded by published academics (Ian Clarke and Roger Dingledine) who put their names on their projects, most of I2P's early developers have maintained their anonymity, using pseudonyms, meeting via IRC or e-mail rather than face-to-face, and even going so far as to anonymize contributions to I2P's code base. In addition, jrandom and his colleagues purposely refrained from promoting I2P to the general public, with the idea that they had to perfect its anonymizing capacities before allowing masses of users to rely on it.[88] All of this has had direct bearing on their organization: I2P is not registered as 501(c)(3) nor as a nonprofit in any other national context. Yet, despite not being a formal nonprofit, and despite a relative lack of large corporate donations (the biggest being $5,000 from DuckDuckGo), I2P is still an organized project, with leaders, regular meetings, and what appears to be an open budget.[89] The use of anonymity among all contributors to I2P indicates an idealistic adherence to the purpose of the project: if the goal is to protect the anonymity of users, the project has to find ways to protect the anonymity of its contributors, even to the degree of not revealing developers' identities for the purposes of filing a nonprofit registration form. This is an example of the software engineering practice of "eating your own dog food"—using the very tools one has developed.[90] Thus, I2P may be best described as an anonymous nonprofit. This anonymity has had drawbacks, however. As I2P

developer zzz noted in an interview, “It’s hard to get paid or be supported by big corporations when you’re anonymous. People want to know who they’re dealing with; people want you to be a 501(c)(3), and all that requires real identities.”[91] As I show in chapter 7, I2P’s organizational structure may have been a liability with an Internet standards organization.

In all three cases, Freenet, Tor, and I2P are making claims that their organizations are not businesses nor parts of any state. Instead, they are more altruistic, beholden not to the demands of shareholders, owners, or governments, but to a global community of privacy-conscious people. As such, their claims of propriety—respectability and control of resources—hinge on this community’s perception that they live up to idealistic goals, whether those organizational goals are expressed through official nonprofit status or as an anonymous nonprofit. This is why Tor’s U.S. government funding is a perpetual issue: if Tor is funded by the same government that runs the National Security Agency, how can it possibly be independent?[92] The Tor Project finds itself perennially defending against allegations that Tor has backdoors allowing government surveillance. Freenet and I2P excite far less speculation, likely because of their lack of U.S. government funding. Ultimately, however, nonprofit status helps all three projects by associating them with the respectable traditions of legitimate, civic-minded organizations.

In addition to funding, these projects seek another key resource: labor. All three projects have organized as open-source software projects. Open-source software production is an organizational form that allows volunteer contributors to work on parts of an overall software package. In addition to hiring workers, open-source projects recruit volunteers. Instead of payment for such contributions, volunteers receive credit (a form of legitimacy exchange) and thanks. In exchange, the resulting software is shared freely with anyone who wants to use it, which means that contributors are providing their labor not just for the organization’s benefit, but for the benefit of all users (including themselves).

Open-source software production has a decades-long history; as such, Freenet, Tor, and I2P are inheriting some of the previous legitimacies of that mode of production.[93] They mark their status as open-source projects by using copyleft or open licenses, code repositories (which allow for many contributors to add code and review code additions), and relatively open communications systems, which anyone can participate in (e-mail lists chief among them). Moreover, developers involved with all three projects argue that open-source software is more secure because it can be audited for security flaws by anyone who cares to look. By using this production model, these projects can command labor and gain further legitimacy as respectable organizations building secure software that meets a public need, offered for free rather than for profit.

Similarly, all three projects seek propriety to attract volunteers, who provide computational power. Freenet's distributed data storage system relies on each user's computer hard drive; a portion of the drive is set aside to store files for the network. Moreover, each Freenet installation is a peer in the network, shunting data to and fro. Tor relies on volunteers to provide bandwidth to the network, setting aside a portion of their personal upload and download speeds to move Tor traffic. It also seeks volunteers to run "exit nodes," the outer edges of the Tor network, where traffic exits the network onto the Clear Web. Exit nodes are essential for Tor users who want to browse the Clear Web anonymously (which is by far the largest use of Tor software). As for I2P, because it is a peer-to-peer system, every user's computer in the I2P network supplies bandwidth for network tunnels. Without these volunteer computational resources, none of these networks would function.

Finally—and certainly not least important—all three projects have spent time and resources on their public-facing web presences. I2P's early history as the Invisible IRC Project is instructive here: early in the project's history, Lance James argued that their website was too dark: "I'm really wanting to go for a brighter look … something more professional … because if we get attention by press the

darkness will give way to the 'media hacker' term."[94] Indeed, the original IIP site was redesigned from its black background to a bright yellow one, and the contemporary I2P site includes primary colors on a pale yellow background. Likewise, the Tor Project and Freenet have gone through extensive site redesigns over their histories, with Freenet developers seeking "something more welcoming and less dark," and the Tor Project using white backgrounds with green accents.[95] All three projects also developed logos: Freenet has an outline of a rabbit ("Leap over censorship"), I2P has Ignatious Toopie (a cartoon person with a yellow mask, shortened to I. Toopie), and Tor has a purple and green onion. All three logos are somewhat bright and cartoonish, which is to say they are far cries from the typical iconography associated with the Dark Web (green text on black background; faceless hooded men typing on glowing keyboards). The projects even sell t-shirts and hats with their logos. Certainly, these details are somewhat banal, and it might be surprising to see how much time developers spend on them in relation to coding, but the attention the projects pay to websites, logos, and marketing highlights their desire to be considered legitimate organizations.

Authenticity

If there is any conflict between Freenet, Tor, or I2P—if there is any sort of rivalry—it is at the register of the legit, the legitimacy of authenticity, which calls for adjudicating who's in, who's out, who belongs, and who should be excluded. As Pierre Bourdieu has argued, practitioners in fields of production struggle with questions of this form of legitimacy.[96] These struggles always hinge on criteria endogenous to the field, as practitioners develop special languages and technical standards by which participants are judged. These struggles are readily apparent among the Dark Web network builders, especially as they compete among each other in contests of technical skill. From this perspective, building an anonymizing network and an organization that can defend a user against a state-funded adversary is not just a challenge to the state's claims to

power. It is also a difficult—and therefore intoxicating—technical challenge to solve, and those who can solve it (or more precisely, parts of it) are considered legit practitioners of their craft.

Both Freenet and Tor began in a specific field of cultural production—academic computer science, with specialization in cryptography and network topologies. The cultural artifacts of this field include presentations at conferences, academic publications, awards, and appointments to prestigious graduate and faculty positions. The field also includes lengthy, intense debates over highly technical details, often in vocabularies that only members of the field can understand, and with no small amount of snarkiness.

I2P has its roots in a different field: hacking. Lance James notes that in contrast to Tor, which was an academic project, I2P is "kinda more like street coders."[97] In response to a question about defending I2P against hackers, jrandom quipped, "we are the hackers ;)."[98] Indeed, "hacker" is a common self-reference among I2P developers in their mailing list. Much like academics, however, hackers traffic in cultural artifacts, such as presentations at conferences, and reputation is a key currency. They also engage in heated, highly technical, jargon-laden debates—and they can be just as snarky. Moreover, Tor and Freenet developers, academic or otherwise, often refer to themselves as hackers as well. Above all, academic computer scientist or hacker, the ultimate object—the ultimate marker of skill and proficiency—is running code. If one can build software to the lofty expectations of the anonymity community of practice, one is legit.

But judging if the code *really* runs—if it really protects user identity and encrypts communications—is difficult. Within this community of practice, running code is the object of many interproject debates. Whether academic or hacker, in mailing lists, IRC logs, or developer forums, contributors not only argue over the technical details of their respective projects, but also critique the other projects: Freenet developers participate in debates in the Tor Project's mailing lists, and Tor developers comment in the I2P forum, and so on. Common objects of criticism include choices of

encryption algorithms, coding languages, and application interfaces, as well as network latencies, theories of anonymity, numbers of hops between nodes, and documentation quality.

For example, Roger Dingledine, during his time working on Free Haven, repeatedly and publicly criticized Freenet:

> [Freenet] really does seem optimized for distributing mp3's and porn. Which has its uses. But this is why there are other projects out there too.[99]

And:

> Freenet will be fine as long as nobody really big [e.g., a state] tries to break it. At that point, who knows.[100]

Dingledine questions the usefulness and effectiveness of Freenet—it may be good for sharing porn, because it emphasizes "popular" files, but can it live up to the loftier goals of protecting dissidents and preventing censorship? Can it do more than facilitate MP3 sharing? And would it withstand attacks from state-level adversaries?

Ian Clarke posted his own critique of Dingledine's Free Haven project on the Free Haven mailing list:

> Free Haven [is] an interesting project with similar aims to Freenet (but which doesn't seem to pay much regard to efficiency) … Perhaps there is scope for an ultra-secure (but ultra-slow) version of Freenet. … Just don't expect me to use it![101]

For Clarke, Free Haven is too inefficient, too slow to be of use.

Dingledine also critiqued I2P (and, for good measure, Freenet):

> The I2P design subscribes to same design approach as Freenet: "add complexity until it's secure." This is a different mentality than Tor's "simplify until you know what you have" approach.[102]

Dingledine's critique echoes the "Unix philosophy," a key hacker mantra: build a tool that does one thing and does it well.[103] "Complexity" is both functionally and aesthetically distasteful, and, in the case of anonymizing networks, insecure.

I2P developer zzz recalls a time when Tor developer Jacob Appelbaum delivered a scathing critique of I2P:

> Appelbaum said "You guys suck; your documentation sucks. Nobody believes you because your documentation is outdated or wrong and it's a disaster on the Web site. Until your documentation is right, nobody will trust you, nobody will believe you. You're a joke until you say at least what it is you're doing."[104]

Like the Unix philosophy, good documentation is a key ideal held by open-source advocates. Good documentation of protocols, encryption algorithms, and network topologies is necessary for contributors and auditors of the code.

But I2P developers have not held back in critiquing Tor. As zzz notes,

> We think we do hidden services much better than Tor, because it's all we do.[105]

In addition, on zzz's stats.i2p eepsite registration page, he tells prospective eepsite hosts, "Do not reuse your onion address from Tor. I2P is not Tor. Pick a real hostname," implying that Tor's use of 16-character alphanumeric URLs is not a "real" naming service.[106] Again, this echoes the Unix philosophy: I2P's hidden services—its Dark Web implementation—is superior because I2P pays so much attention to it, including providing a "real" naming service, while Tor tries to do too many other things.

These critiques may start on one network's mailing list and migrate to another, becoming what is called, in Internet parlance, "flame wars." One key flame war occurred between I2P and Freenet developers on the I2P mailing list in 2005, when Freenet developer Toad and I2P developer jrandom sparred over the stakes of their

projects. Jrandom repeatedly asked Toad, "How many dead users is OK with you?," implying that Freenet's lack of security would result in dead dissidents.[107] Toad replied, "If there was some way to build a perfect system from the ground up, and if getting busted meant hundreds of thousands of people being tortured, imprisoned for long periods etc., I might lend some weight to your arguments."[108] Here, Toad argues that an imperfect, experimental anonymizing system is far better than a "perfect one" that can never be built, and that, moreover, jrandom's question about "dead users" is hyperbolic in the extreme.[109]

Their debate covered much technical ground, as do the other debates I've excerpted, but I highlight these less technical moments as evidence for larger struggles over the legit among computer scientists and hackers concerned with building anonymizing networks. As project developers implement their designs in running code and active networks, other project developers question their choices, ultimately arguing that poor encryption algorithms, badly designed network topologies, or a poor choice of programming languages undermines their efforts to build a real, working anonymizing network. And there is more at stake than anonymity (or even jrandom's "dead users"): *the developers' reputations within their specific community of practice are on the line.* As I2P developer zzz aptly puts it, "Losing our reputation may be one of the biggest existential risks to the project."[110] To expand on Appelbaum's critique of I2P, if an anonymizing network is not considered legit—if it sucks, if it's bullshit, if it isn't for real—no one will trust it, and it will not attract enough users and contributors. Instead, users and contributors might take their resources to a different network.

On this note of reputation, developers believed to be able to solve the seductive technical puzzle of making anonymizing networks can become legit celebrities. Former Tor developer Jacob Appelbaum is a case in point. As the *Guardian*'s Anna Catherine Loll describes him,

> In 2004, he started volunteering as a developer for the Tor Project, the prestigious organisation behind the anonymity tool regarded as one of the crown jewels of the information security community. He soon became a prolific public speaker, his profile soaring in 2010 when he stood in for Julian Assange as the keynote speaker at the Hackers on Planet Earth (Hope) conference in New York.[111]

Appelbaum has graced magazine covers, given lengthy interviews, and regularly gone on speaking tours. He was—and for some, still is—the very model of a legit hacker, a person equally skilled at computer coding and representing the cause of liberation technology. For over a decade, he was associated with Tor, which in Loll's words is a "prestigious organisation." But he was removed from the Tor Project in 2016 as the result of accusations that he regularly sexually abused and bullied many people. I discuss Appelbaum—and his formerly legit reputation—further in chapter 7.

Another example illustrates a moment of legitimacy exchange. A 2013 photograph of the NSA whistleblower Edward Snowden, taken after his flight to Russia, appeared in the *Washington Post*.[112] Snowden is sitting with a laptop computer open, and on the back of the laptop is a sticker: the Tor onion logo. This points to the benefits of organizational practices such as logo design and marketing—the possibility of reputation enhancement through celebrity endorsement. In this legitimacy exchange, the association of the NSA whistleblower and Internet folk hero Edward Snowden with the Tor Project reinforced the reputations of both among the anonymizing community of practice. If Snowden uses Tor, it must be legit.

Thus, the legit—authenticity—is just as important to these projects as their relationship to the state or their status as organizations. The interproject debates are, in part, performances of cultural competency, where participants show their command of symbols such as encryption algorithms, software engineering practices, or network topologies. Contributors to these projects and the projects themselves must demonstrate these competencies as

they all compete within the field of anonymizing network technology production. The systems must also withstand the trials of security researchers, who constantly probe them for weaknesses. Researchers who discover flaws can build their own reputations by pointing out the flaws in public. Winners of these struggles may even achieve some fame, have their projects endorsed by celebrities, or receive lucrative government jobs or defense contracts. And of course, success in the realm of the legit can influence success in the organizational and state-related spheres, since a legit anonymous network will attract more coders, sponsors, and users, who in turn can support the project if it is challenged by a state.

Conclusion

In this chapter I have focused solely on the network builders—the computer scientists, hackers, and open-source software developers who gather around an intriguing technical problem: how to make networks that can hide the identity of readers as well as publishers of information. I traced how these network builders engaged in symbolic economies to negotiate with state violence, to cohere as organizations that command respect and resources, and to establish social rules of authentic anonymizing software development. All three registers of legitimacy are important to the survival of these networks and are thus intimately intertwined. The network builders recruit volunteers to contribute running code that can defend users against state surveillance and appeal to information security communities.

Growing as these projects did in the wake of the World Wide Web's explosion in popularity, the network builders unsurprisingly developed web publishing capacities early on in their histories. The early web, which began at the Organisation européenne pour la recherche nucléaire (CERN), was primarily used for publishing and reading technical data, but it quickly grew beyond technical matters and became a popular media phenomenon. This led to an unpredictable range of content, from the profound to the profane. Likewise, early web publishing on the Dark Web may have dealt largely with technical subjects (such as tc.i2p, a developer forum, or the Hidden Wiki, which started as a means for Tor to document technical issues), but of course Dark Web content has taken on a wild range of forms. To explore this, the next three chapters turn to three types of Dark Web sites: markets, search engines, and social networking. These chapters will also focus on each type of legitimacy in turn. I explore the relationship between state violence and Dark Web markets in the next chapter; the development of propriety among Dark Web search engines in chapter 5; and the

adjudication of who's in and who's out in Dark Web social media in chapter 6.

Notes

1. Ian Clarke, "A Distributed Decentralised Information Storage and Retrieval System" (master's thesis, University of Edinburgh, 1999), http://www.decuslib.com/DECUS/vmslt00a/net/freenet.pdf.

2. Ian Clarke, "[Freenet-dev] Fuzzy search," Freenet-dev mailing list archives, May 14, 2000, https://web.archive.org/web/20141117114016/https://emu.freenetproject.org/pipermail/devl/2000-May/001681.html.

3. Clarke, "Distributed Decentralised Information," 9.

4. Ibid.

5. "A Distributed Decentralised Information Storage and Retrieval System," Freenet Development Page, October 13, 1999, https://web.archive.org/web/19991013120144/http://freenet.on.openprojects.net/.

6. Ian Clarke et al., "Protecting Free Expression Online with Freenet," *IEEE Internet Computing* 6, no. 1 (2002): 40–49; "Publicity," Free Network Project, June 6, 2001, https://web.archive.org/web/20010606211622/http://freenetproject.org/index.php?page=publicity; Gary Trudeau, "Electronic Town Hall," *Doonesbury*, May 28, 2001, https://web.archive.org/web/20010609015529/http://www.doonesbury.com/strip/dailydose/index20010528.htm.

7. Duncan J. Watts and Steven H. Strogatz, "Collective Dynamics of 'Small-World' Networks," *Nature* 393, no. 6684 (June 4, 1998): 440–442, doi:10.1038/30918.

8. This six-character alphanumeric example is a bit too simple. Freenet keys are often much longer. For example, the key for Enzo's Index, an index of freesites, is USK@XJZAi25dd5y7lrxE3cHMmM-xZ-c-hlPpKLYeLC0YG5I,8XTbR1bd9RBXlX6j-OZNednsJ8Cl6EAeBBebC3jtMFU,AQACAAE/index/711/ [Freenet].

9. Mr. Bad, "Get in on the Ground Floor of FREEDOM," *Pigdog Journal* (blog), February 24, 2000, http://www.pigdog.org/auto/liberty/link/1264.html. For an example of this quotation in Freenet software, see "Read Me (Fred/Freenet 5.0)," GitHub, December 9, 2007, https://github.com/freenet/legacy/blob/stable/README.

10. Jon M. Kleinberg, "Navigation in a Small World," *Nature* 406, no. 6798 (2000): 845.

11. John Markoff, "Cyberspace Programmers Confront Copyright Laws," *New York Times*, May 10, 2000, sec. A.

12. Ian Clarke, "Creating Websites in Freenet," Freenet Project, December 14, 2000, https://web.archive.org/web/20001214054400/http://freenetproject.org/index.php?page=authoring.

13. Theodore Hong, "Freenet Keys for Testing," May 11, 2000, https://web.archive.org/web/20000511004840/http://longitude.doc.ic.ac.uk/keyindex.

14. "Welcome to FreeWeb," FreeWeb, April 28, 2001, https://web.archive.org/web/20010428125346/http://freeweb.sourceforge.net/main.html.

15. Bombe, "JSite," Freenet Wiki, September 1, 2006, https://old-wiki.freenetproject.org/FreenetJsite?time=2006-09-01+18%3A08%3A42.

16. Enzo's crawler statistics are available on Freenet at USK@XJZAi25dd5y7lrxE3cHMmM-xZ-c-hlPpKLYeLC0YG5I,8XTbR1bd9RBXlX6j-OZNednsJ8Cl6EAeBBebC3jtMFU,AQACAAE/index/711/statistics.html [Freenet].

17. Roger R. Dingledine, "The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven" (master's thesis, Massachusetts Institute of Technology, 2000), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.3453&rep=rep1&type=pdf; Roger Dingledine, Michael J. Freedman, and David Molnar, "The Free Haven Project: Distributed Anonymous Storage Service," in *Designing Privacy Enhancing Technologies*, ed. Hannes Federrath, vol. 2009 of Lecture Notes in Computer Science (Berlin: Springer, 2001), 67, http://link.springer.com/chapter/10.1007/3-540-44702-4_5.

18. Dingledine, Freedman, and Molnar, "The Free Haven Project," 67.

19. Ibid.

20. David L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM* 24, no. 2 (1981): 84–90; Andreas Pfitzmann, Birgit Pfitzmann, and Michael Waidner, "ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead," in *Kommunikation in verteilten Systemen*, ed. Wolfgang Effelsberg, Hans W. Meuer, and Günter Müller (Berlin: Springer, 1991), 451–463, http://link.springer.com/chapter/10.1007/978-3-642-76462-2_32.

21. Dingledine, Freedman, and Molnar, "The Free Haven Project."

22. Roger Dingledine, Nick Mathewson, and Paul Syverson, "Reputation in P2P Anonymity Systems," (paper presented at

Workshop on Economics of Peer-to-Peer Systems, Berkeley, CA, 2003), http://mail.freehaven.net/anonbib/cache/rep-anon.pdf.

23. Roger Dingledine, "[Freehaven-dev] Initial musings on the next Free Haven (part one of two)," Freehaven-dev mailing list archives, April 15, 2001, http://archives.seul.org/freehaven/dev/Apr-2001/msg00007.html.

24. "The Free Haven Project," Free Haven, April 9, 2003, https://web.archive.org/web/20030409042914/http://www.freehaven.net/.

25. David M. Goldschlag, Michael G. Reed, and Paul F. Syverson, "Hiding Routing Information," in *Information Hiding*, ed. Ross Anderson (Berlin: Springer, 1996), 137–150, http://link.springer.com/10.1007/3-540-61996-8_37.

26. Roger Dingledine and Paul Syverson, "Reliable MIX Cascade Networks through Reputation," in *Financial Cryptography*, ed. Matt Blaze (Berlin: Springer, 2002), 253–268, http://link.springer.com/chapter/10.1007/3-540-36504-4_18.

27. Matej Pfajfar, "Onion Routing" (Thesis, Cambridge University, UK, 2002); Roger Dingledine, "Pre-alpha: run an onion proxy now!," Freehaven.net or-dev mailing list archives, September 20, 2002, http://archives.seul.org/or/dev/Sep-2002/msg00019.html.

28. Roger Dingledine, "Remove faq and hacking files too. they're now in doc," Tor's Source Code, March 18, 2003, https://gitweb.torproject.org/tor.git/commit/?id=f9c541bfcf886248e809d198b19fb1e2e97b924e.

29. Roger Dingledine, "Name change: or -> tor," Freehaven.net or-dev mailing list archives, February 3, 2002, http://archives.seul.org/or/dev/Sep-2002/msg00009.html; Roger Dingledine, "[Or-cvs] Our program is now called 'tor', not

'or,'" Freehaven.net or-cvs mailing list archives, September 3, 2002, http://archives.seul.org/or/cvs/Sep-2002/msg00011.html.

30. Roger Dingledine, "(FWD) [or-cvs] a new TODO file with more details," Freehaven.net or-dev mailing list archives, February 13, 2003, http://archives.seul.org/or/dev/Feb-2003/msg00009.html; Nick Mathewson, "Add first draft of rendezvous point document," Tor's Source Code, June 12, 2003, https://gitweb.torproject.org/tor.git/commit/?id=3d538f6d702937c23bec33b3bdd62ff9fba9d2a3.

31. The Tor Project has recently experimented with rebranding hidden services as "onion services." As of this writing, however, their specifications files still refer to "hidden services," and most people still refer to them as such.

32. "Tor Rendezvous Specification," Tor's Protocol Specifications, October 12, 2016, https://gitweb.torproject.org/torspec.git/tree/rend-spec.txt; Paul Syverson and Griffin Boyce, "Bake in .onion for Tear-Free and Stronger Website Authentication," *IEEE Security and Privacy* 14, no. 2 (March 2016): 15, doi:10.1109/MSP.2016.33.

33. Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no. 1 (January 2, 2016): 18, doi:10.1080/00396338.2016.1142085.

34. Eternity was another data haven, similar to Free Haven. Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: Next-Generation Onion Routing" (poster presented at CodeCon, San Francisco, 2004), 4, https://web.archive.org/web/20041204074542/http://tor.freehaven.net/slides-codecon04/.

35. Roger Dingledine, "Hidden-ssh, irc, ftp, etc etc via socat," Freehaven.net or-dev mailing list archives, April 16, 2004, http://archives.seul.org/or/dev/Apr-2004/msg00013.html; "The Onion Router Wiki," Noreply Wiki, August 10, 2004,

https://web.archive.org/web/20040810102122/http://wiki.noreply.org/wiki/TheOnionRouter.

36. Lance James, "About," IIP—Invisible IRC Project, November 21, 2001, https://web.archive.org/web/20011121032730fw_/http://bovine.artificial-stupidity.net/~nop/iip/about.html; Rick Hayes, "Interview with zzz and Lance James," February 12, 2012, in *InfoSec Daily Podcast*, episode 596, MP3 audio.

37. This podcast is no longer produced, and its archives are offline. Contact the author for an MP3 file.

38. Esther Weltevrede, Anne Helmond, and Carolin Gerlitz, "The Politics of Real-Time: A Device Perspective on Social Media Platforms and Search Engines," *Theory, Culture and Society* 31, no. 6 (June 20, 2014): 143, doi:10.1177/0263276414537318.

39. Ibid.

40. The Principality of Sealand home page (2007), http://127.0.0.1:8888/USK@EwuiekEqCT4hHMzs8OpYFQbkfawSRY7sMqvRebmyZ~c,i3RauV~532OotoMheJNH~~IlHBBkmy~ZNVbOfCYZNtA,AQACAAE/sealand/5/ [Freenet].

41. Freenet developers did address this with forum software, such as Frost and later FMS. Today, Freenet has a relatively active microblogging system called Sone that is certainly faster than the early Freenet James encountered.

42. Lance James, "IIPv1 White Paper Revision 1.1.1," December 2002, https://web.archive.org/web/20020110185425fw_/http://bovine.artificial-stupidity.net/~nop/iip/IIPabout.htm.

43. Lance James, "Invisible IRC Project" (presentation at CodeCon, San Francisco, February 16, 2002), http://invisibleip.sourceforge.net/iip/resources/iip_transcript.txt.

44. Ibid.; 0x90 [Lance James] and DC, “Media > DC Interview Part 1,” Invisible IRC Project, July 26, 2002, https://web.archive.org/web/20021006073454/http://www.invisiblenet.net/iip/mediaDCInterview1.php.

45. “Stable Release—IIP v1.1.0,” Invisible IRC Project, April 17, 2003, https://web.archive.org/web/20030417093445/http://www.invisiblenet.net/iip/downloadMain.php.

46. 0x90 [Lance James] and DC, “Media > DC Interview Part 1.”

47. “I2P Development Meeting 47,” I2P: The Invisible Internet Project, July 1, 2003, https://geti2p.net/en/meetings/47.

48. The mailing list archive was hosted at Gmane (http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/), but as of this writing is only available via NNTP download. The new hosts of Gmane have indicated that the old archives will be available via the web sometime in the future, so I have included the web URLs if I have them. Jrandom, “Sample Java Api,” Gmane mailing list archive, July 15, 2003, http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/280.

49. Jrandom, “Some Light Reading,” Gmane mailing list archive, July 7, 2003, http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/269.

50. I have no record of jrandom’s gender self-identification; other developers refer to jrandom as “he.” Most of the developer meeting logs are available on the I2P site, “Logs of Past I2P Meetings,” https://geti2p.net/en/meetings.See also jrandom, “Two Quick Things to Consider before Tonights Meeting,” Gmane mailing list archive, July 8, 2003, http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/271.

51. Jrandom, “Sample Java Api”; jrandom, “Java Version + Signatures (Fwd: I2P Implementation Questions),” Gmane mailing list archive, August 1, 2003, http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/315.

52. See the Internet Archive snapshot “Index of /i2p” at https://web.archive.org/web/20040413131023/http://dev.i2p.net/i2p/.

53. Lance James, “Public Peer Review Request!,” gmane.comp.security.invisiblenet.iip.devel mailing list archives, September 3, 2003.

54. “I2P Development Meeting 65,” I2P: The Invisible Internet Project, November 18, 2003, https://geti2p.net/en/meetings/65; TC, “Hosts.txt v 1.1,” I2p.Net, December 15, 2003, https://web.archive.org/web/20040413131233/http://dev.i2p.net/i2p/hosts.txt.

55. “I2P Development Meeting 68,” I2P: The Invisible Internet Project, December 9, 2003, https://geti2p.net/en/meetings/68.

56. See “Tunnel Implementation,” I2P: The Invisible Internet Project, October 2010, https://geti2p.net/en/docs/tunnels/implementation, for the latest I2P tunnel specification.

57. TC, “Hosts.Txt v 1.1.”

58. This number does not include all eepsites currently running. As of this writing, I2P’s eepsites can be located using a 52-character alphanumeric base32 key. For example: http://udhdrtrcetjm5sxzskjyr5ztpeszydbh4dpl3pl4utgqqw2v4jna.b32.i2p/ [I2P]. To make these addresses human-readable, however, several I2P developers offer custom hosts.txt files that associate “pet names” with those keys. Using these files, I have collected 1,700 I2P URLs. Nonetheless, even those URLs are not

necessarily active. For example, to this day, tc.i2p, which may have been the first eepsite, is listed in default hosts.txt files, but TC's site has not been available for quite some time. Moreover, additional I2P sites do not use "pet names" and are found via the full 52-character keys. I do not have a good count of those sites.

59. Michael Herrmann and Christian Grothoff, "Privacy-Implications of Performance-Based Peer Selection by Onion-Routers: A Real-World Case Study Using I2P" (presentation at the International Symposium on Privacy Enhancing Technologies, Waterloo, Ontario, July 29, 2011), http://grothoff.org/christian/teaching/2011/2194/i2p.odp.

60. Hayes, "Interview with zzz and Lance James."

61. Jrandom, "0.6.1.30 Release," I2P: The Invisible Internet Project, October 7, 2010, https://geti2p.net/en/blog/post/2007/10/07/0.6.1.30-Release; Jrandom, "Jrandom's Announcement," I2P: The Invisible Internet Project, November 2007, https://geti2p.net/en/misc/jrandom-awol.

62. "I2PCon Day 1: Growing the Network, Spreading the Word (August 15, 2015)," presented by zzz, YouTube video, 57:40, posted by KYTV at I2P, August 27, 2015, https://www.youtube.com/watch?v=2KbqgR3avqw. As zzz notes, jrandom's sudden, near-disastrous abandonment of the project was an organizational point of centralization and failure, contrasting with the project's topology of decentralization. This reveals how centralization and decentralization can exist side-by-side in the same sociotechnical system.

63. See "I2P Project Members," I2P: The Invisible Internet Project, January 2016, https://geti2p.net/en/about/team.

64. "I2PCon 2015," I2P: The Invisible Internet Project, accessed September 15, 2016, https://geti2p.net/pt/about/i2pcon/2015.

65. David T-G, “[Freenet-chat] Wireless,” March 26, 2002, Freenet chat mailing list, https://emu.freenetproject.org/pipermail/chat/2002-March/000978.html.

66. Furgalj at lakeviewtech.com, “[Freenet-chat] Re: [Freenet-support] Showdown at the Freenode Coral,” Freenet-chat mailing list, August 7, 2004, https://emu.freenetproject.org/pipermail/chat/2004-August/001250.html.

67. Michael Holstein, “Paid performance-tor option?,” Tor-talk mailing list, August 18, 2008, https://lists.torproject.org/pipermail/tor-talk/2008-August/002283.html.

68. Ringo, “SoC Project: Improving Hidden Service Security and Usability,” Tor-talk mailing list, May 25, 2009, https://lists.torproject.org/pipermail/tor-talk/2009-May/014094.html; Marc Abel, “TorPark mirrors and China,” Tor-talk mailing list, September 26, 2005, https://lists.torproject.org/pipermail/tor-talk/2005-September/017938.html.

69. Jrandom, “Re: /. [How Chinese Evade Government’s Web Controls],” gmane.network.i2p mailing list archives, November 27, 2005.

70. Connelly Barnes, “Chinese Firewall Circumvention,” gmane.i2p.dev mailing list archives, October 6, 2005; Jrandom, “Re: I2P Conspiracy Theories Flamewar,” gmane.network.i2p mailing list archives, October 5, 2005.

71. Polecat, “Re: I2P Conspiracy Theories Flamewar,” gmane.network.i2p mailing list archives, October 12, 2005.

72. Newsbyte, “[Freenet-chat] [Freenet-dev] Censorship,” Freenet-chat and Freenet-dev mailing lists, May 14, 2004,

https://emu.freenetproject.org/pipermail/chat/2004-May/001267.html.

73. Jrandom, "I2p Project Overview Doc for the SDK," Gmane mailing list archive, August 8, 2003, http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/344; Jrandom, "I2p Project Overview Doc for the SDK." The language here echoes a famous document, John Parry Barlow's "Declaration of the Independence of Cyberspace," first published in 1996. See the declaration at the Electronic Frontier Foundation, February 8, 1996, https://www.eff.org/cyberspace-independence.

74. See Naomi Sussmann, "Can Just War Theory Delegitimate Terrorism?," *European Journal of Political Theory* 12, no. 4 (October 1, 2013): 425–446, doi:10.1177/1474885112464478 4, for a discussion of theories of legitimate and illegitimate violence and how these theories are used to define terrorism.

75. James Comey, "Encryption, Public Safety, and 'Going Dark,'" *Lawfare* (blog), July 6, 2015, http://www.lawfareblog.com/encryption-public-safety-and-going-dark.

76. Beatrice Berton, *The Dark Side of the Web: ISIL's One-Stop Shop?* (EUISS Alert, Paris: European Union Institute for Security Studies, June 2015), 2, http://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf.

77. We do need to distinguish between the listing of the weapon and the acts of ordering, paying for, shipping, and receiving the weapon. The relationship between the listing of an object for sale and the actual purchase and delivery of the object is hard to analyze, and we cannot assume the latter from the former. As researchers and court records have shown, the latter can happen, but given the sheer amount of scams on the Dark Web, it doesn't

often go smoothly. The prevailing wisdom on Dark Web forums is that all gun sales on the Dark Web are scams or law enforcement traps, and that a potential gun buyer would be better off buying off the street. Despite this, using a listing to support an argument for increased policing of the Dark Web can be effective. See for example the discussion of Dark Web gun listings, scams, and the need to assume every listing is a potential gun in the hands of terrorists in Giacomo Persi Paoli et al., "Behind the Curtain" (Santa Monica, CA: RAND, 2017), https://www.rand.org/pubs/research_reports/RR2091.html.

78. "I2PCon Day 1."

79. Nathalie Maréchal, "'Use Signal, Use Tor?': The Political Economy of Circumvention Technology" (PhD diss. in progress, University of Southern California).

80. Hayes, "Interview with zzz and Lance James."

81. Peter Galison, "The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision," *Critical Inquiry* 21 (Autumn 1994): 228–266.

82. Ian Clarke et al., "Protecting Free Expression Online with Freenet," *IEEE Internet Computing* 6, no. 1 (2002): 41, http://ieeexplore.ieee.org/document/978368/?reload=true.

83. For a history of the U.S. nonprofit sector, see Dobkin Hall, "Inventing the Non-Profit Sector, 1950–1990," in *The Nature of the Nonprofit Sector*, ed. J. Steven Ott (Boulder, CO: Westview Press, 2001), 112–125.

84. Freenet Form 990EZ, accessed October 24, 2016, http://990s.foundationcenter.org/990_pdf_archive/954/954864038/954864038_201412_990EZ.pdf.

85. Maréchal, "Defying Censorship, Evading Surveillance," 9.

86. See "Who Uses Tor?," Tor Project, accessed May 31, 2017, https://www.torproject.org/about/torusers.html.en.

87. IRS 990 Form and audit report for fiscal year 2014, Tor Project (2015), https://www.torproject.org/about/findoc/2014-TorProject-combined-Form990_PC_Audit_Results.pdf.

88. "I2PCon Day 1."

89. Yegg, "2014 FOSS Donations," DuckDuckGo Community Platform (blog), March 12, 2014, https://duck.co/blog/post/72/foss2014; "Hall of Fame," I2P: The Invisible Internet Project, September 1, 2016, https://geti2p.net/en/about/hall-of-fame.

90. Scott Rosenberg, *Dreaming in Code: Two Dozen Programmers, Three Years, 4,732 Bugs, and One Quest for Transcendent Software*, 1st ed (New York: Crown, 2007).

91. Hayes, "Interview with zzz and Lance James."

92. For the most detailed examples of the allegation that the Tor Project is a front for U.S. government surveillance, see Yasha Levine, "Almost Everyone Involved in Developing Tor Was (or Is) Funded by the US Government," *Pando*, July 16, 2014, https://pando.com/2014/07/16/tor-spooks/. For an analysis of the complex relationship between the Tor Project and the U.S. government, see Maréchal, "Defying Censorship, Evading Surveillance."

93. Steven Weber, *The Success of Open Source* (Cambridge, MA: Harvard University Press, 2004). Indeed, we can read Weber's history and analysis of the open-source mode of production in terms of trials of legitimacy, with concepts such as "property-as-distribution" and "impossible public goods" being contested.

94. "I2P Development Meeting 2," I2P: The Invisible Internet Project, May 29, 2002, https://geti2p.net/en/meetings/2.

95. Simon Porter, "[Freenet-dev] Freenet website redesign—Feedback, ideas and help wanted," Freenet-dev mailing list archives, December 15, 2002, https://web.archive.org/web/20141117122740/https://emu.freenetproject.org/pipermail/devl/2002-December/022664.html.

96. See in particular chapter 1 of Pierre Bourdieu, *The Field of Cultural Production: Essays on Art and Literature* (New York: Columbia University Press, 1993).

97. Hayes, "Interview with zzz and Lance James."

98. "I2P Development Meeting 153," I2P: The Invisible Internet Project, October 25, 2005, https://geti2p.net/en/meetings/153.

99. Roger Dingledine, "Re: [Freehaven-dev] Re: [Freenet-chat] MojoNation," Freehaven-dev mailing list archives, August 10, 2000, http://archives.seul.org//freehaven/dev/Aug-2000/msg00018.html.

100. Roger Dingledine, "Re: [Freehaven-dev] re: chapters done—moving forward options," Freehaven-dev mailing list archives, December 14, 2000, http://archives.seul.org//freehaven/dev/Dec-2000/msg00009.html.

101. Ian Clarke, "[Freehaven-dev] [Freenet-chat] Interesting commentary on Freenet from Freehaven," Freenet-dev and Freenet-chat mailing list archives, September 27, 2000, http://archives.seul.org//freehaven/dev/Sep-2000/msg00010.html.

102. Roger Dingledine, "Re: I2P (was Re: Psiphon (Was: Bootstraping Tor manually to get past the Great Firewall))," or-talk mailing list archives, December 4, 2006, http://archives.seul.org/or/talk/Dec-2006/msg00050.html.

103. O. M. Ritchie and Ken Thompson, "The UNIX Time-Sharing System," *Bell System Technical Journal* 57, no. 6 (1978): 1905–

1929.

104. "I2PCon Day 1." To be fair, zzz also noted that Appelbaum was right and that the I2P documentation did need to be improved.

105. Ibid.

106. See zzz's eepsite registration page, accessed August 31, 2017, http://stats.i2p/i2p/addkey.html [I2P].

107. Jrandom, "Re: I2P Conspiracy Theories Flamewar."

108. Matthew Toseland, "Re: [Jrandom-Po2eaMWI3R0@public.Gmane.Org: Re: [Tech] Re: I2P Conspiracy Theories Flamewar]," gmane.network.i2p mailing list archives, October 6, 2005.

109. In fact, jrandom was so concerned about perfecting I2P that he refused to promote it beyond a small circle of users. See "I2PCon Day 1."

110. Ibid.

111. Anna Catherine Loll, "Power, Secrecy and Cypherpunks: How Jacob Appelbaum Ripped Tor Apart," *Guardian*, October 11, 2016, sec. Technology, https://www.theguardian.com/technology/2016/oct/11/jacob-appelbaum-tor-project-sexual-assault-allegations.

112. "New Photos of Edward Snowden," *Washington Post*, December 23, 2013, https://www.washingtonpost.com/world/national-security/edward-snowden-says-his-missions-already-accomplished/2013/12/23/764e37fc-6c4c-11e3-aecc-85cb037b7236_gallery.html.

4 From Agorism to OPSEC: Dark Web Markets and a Shifting Relationship to the State

> "Everywhere I looked I saw the State."
> —Dread Pirate Roberts

Perhaps the most infamous Dark Web site was the original Silk Road drug market, hosted as a Tor hidden service. From its beginning in early 2011 to its seizure by law enforcement in late 2013, the Silk Road was arguably more than a market. Its founder, Ross Ulbricht, conceptualized Silk Road as a sociotechnical implementation of agorism, a radical market libertarian philosophy. Echoing Weberian theories of state legitimacy (as discussed in chapter 2), agorism holds that the state is indeed the sole source of coercion and violence in contemporary society. Rather than accepting this dominance as "legitimate," however, agorists argue that the state is *illegitimate* precisely because of its monopoly on violence. For agorists, free markets offer a new model for social organizing that does not rely on coercion, violence, or state power, where exchanges, not law enforcement, could be the glue that holds society together. Ulbricht argued that every sale on Silk Road was not just a means for drug dealers to satisfy the desires of drug consumers but a blow to the concept of the state itself.

Of course, the state hasn't been destroyed by Dark Web drug sales. The Silk Road has been shut down by U.S. law enforcement, and Ulbricht has been sentenced to life in prison without the chance of parole. As a consequence, the prevalence of agorist and libertarian political discussion has receded on Dark Web market forums. In comparison to Silk Road, the new markets on the Dark Web are less overtly about libertarian ideology and far more concerned with

security. Such security practices are referred to as operational security, or OPSEC, a term appropriated from the military. This conceptualization reinforces theories of communication as acts of war, violence, and defense. The new post–Silk Road Dark Web markets have moved from an idealistic agorist poststate philosophy to a "proactively paranoid" one, where scams, police raids, fraud, and weaponized communication are the costs of doing business.

In this chapter, I avoid dismissing OPSEC as simply the paranoid mindset of vendors who fear arrest, or as the overly suspicious attitude of buyers who fear being scammed. Instead, I suggest that operational security has replaced agorism as the predominant politics of Dark Web markets, and that OPSEC represents a new relationship to the state. Whereas agorism holds that the state is illegitimate, OPSEC is an appropriation of a state practice born of violent conflict. In this sense, both agorism and OPSEC are directly related to the state's claim to a monopoly on violent power; the former delegitimates this claim, and the latter attempts to appropriate it. Thus, unlike the previous chapters, this chapter (and the two to follow) focuses on only one of the meanings of legitimacy. By considering the shifting relationship between Dark Web markets and state violence, we can better understand the move from delegitimation of state practices among the agorists to appropriation of state practices among the OPSEC minded.

Drawing on market forum archives, participant observation in Tor and I2P market forums, and a growing body of journalistic and academic coverage of Dark Web markets, I first provide an overview of the sociotechnical ingredients that go into Dark Web markets. I follow this with a summary of agorism, drawn from the work of that philosophy's founder, Samuel Edward Konkin III, which sets the stage for discussion of Silk Road's relationship to agorism. Then, I turn to the new politics of the Dark Web markets, OPSEC, exploring its history as part of the U.S. war in Vietnam and its particular inflection in Dark Web market forums. I argue that OPSEC is a legitimate offspring of agorist thinking, inheriting the latter's interest in security while rebelling against its community-from-markets way of thinking in favor of paranoid sociality.

I ultimately suggest that, unlike Ulbricht's Silk Road, the post–Silk Road markets reinforce, rather than challenge, the power of the state by further associating communication with violence. Since the legitimated monopoly on violence is the core defining feature of the state, the continual expansion of violence into communicative acts expands the state's purview and further justifies increasing surveillance and securitization of communications. Postagorist Dark Web markets will breed and feed on new wars and new warriors, new policing and new securitizations, as Dark Web operations clash with law enforcement operations.

Dark Web Markets Overview

As of this writing, at least thirty markets have sites on the Dark Web, with the majority hosted as Tor hidden services. The range of markets includes multivendor sites, which are similar to Clear Web markets like eBay in that vendors can enter and leave the markets as they wish, and single-vendor stores, which are more akin to small businesses owned and operated by a single proprietor. Some markets specialize in drugs, others in stolen data, and others in weapons.[1]

Many sociotechnical ingredients go into contemporary Dark Web markets. In the following sections, I summarize several of these ingredients before turning to the main focus of this chapter: the political and social theory produced by Dark Web market participants.

Anonymizing Networks

A key technological ingredient that supports contemporary Dark Web markets is anonymizing technology, developed by the network builders I describe in chapter 3. Anonymizing networks dissociate real-world identifying information from network traffic, thus allowing administrators, buyers, and sellers to meet in conditions of strong anonymity. Currently, Tor's hidden services system is the preferred anonymizing network for Dark Web markets. Tor combines low latency, support for standard web-hosting software packages and modules (e.g., Apache, MySQL, PHP), and Edward Snowden's endorsement. Moreover, Tor's hidden services enjoy strong network effects; they are more popular than eepsites or freesites, and this popularity attracts more traffic, reinforcing Tor's dominance. Dark Web markets have also been deployed or mirrored on the I2P network, including the Marketplace and Silk Road Reloaded, both now defunct, as well as current cryptocurrency exchanges. Freenet has not, to my knowledge, hosted a Dark Web

market, likely because of its more static structure, although individual vendors have set up freesites there to promote themselves.

PGP Encryption

PGP is a keypair-based encryption scheme that enables a person to encrypt a message so that only the holder of a private key can decrypt it. Dark Web market exchanges are often facilitated by PGP in three ways. For one, market participants use PGP to encrypt messages so that only the recipient can decode them. Users also verify their (pseudonymous) identities with PGP signatures. For example, a vendor may habitually include a PGP signature in his forum posts to demonstrate that all the posts are coming from someone who controls the same private PGP key. This is especially important as vendors use the same pseudonyms across multiple markets. Finally—especially in the wake of the Silk Road bust—market participants use PGP to demonstrate technical competence. For example, in one market forum I participated in, the site administrators examined my PGP signature to make sure I was using what they considered to be the best encryption algorithm (RSA) and a large key size (4,096 bits). I was not allowed access to this particular forum until I could demonstrate this.

Cryptocurrencies

Rather than use currencies backed by the power of the state, Dark Web markets rely on new cryptocurrencies, such as Bitcoin, Ethereum, Dash, or Monero. As Vasilis Kostakis and Chris Giotitsas describe them, "Cryptocoins ... are based on cryptographic technologies, and are therefore (partly) anonymous and decentralized in production and circulation. It is not easy for someone to suppress their activity due to their peer architecture."[2] Cryptocurrencies are produced by individuals, not states, and rely on computational development and accounting, rather than banks, to put them into and keep them in circulation. Their value arises in

part from their perceived role as universal equivalents in network economies.

Because Bitcoin has such a large market share, and because Bitcoin exchanges are not inherently anonymous, buyers use "tumbling" services to dissociate Bitcoins from identification information. In tumblers, Bitcoins used to sell or purchase illegal items are mixed together with Bitcoins used for other purposes, obfuscating whose coin purchased what good.[3] More recent cryptocurrencies, such as Monero, seek to improve on this situation by providing anonymous accounting of exchanges.

Market Software

Dark Web market software tends to start with preexisting open-source packages, such as Apache or NGINX, for web-based serving and receiving of files. Similarly, they use open-source packages for transaction databases and user interfaces. These packages are heavily modified by market administrators in an effort to increase their security. They are client-server network topologies, which allows for centralized administration of the software but also introduces a point of failure if the market's servers are infiltrated or seized by law enforcement, or if the administrators decide to shut down the market. Contemporary markets are even offering "bug bounties," similar to those of mainstream software firms, to penetration testers who might find vulnerabilities in the software.[4]

In addition, forum posts across Tor and I2P discuss future implementations of decentralized, peer-to-peer market software, built on OpenBazaar, an open-source software package that uses distributed hash tables and blockchain technology to avoid the centralization problem traditional Dark web markets face. To my knowledge, there are no implementations of OpenBazaar on the Dark Web, but I expect to see one soon.[5]

Clear Web Coverage

Although Dark Web markets are hosted on the Dark Web, they are heavily reliant on Clear Web coverage to promote them. Currently, the two main sources of Dark Web market coverage come from *Deep Dot Web*, an online magazine, and the DarkNetMarkets subreddit on Reddit. The former includes interviews with drug market admins; how-to guides for using Bitcoin, Tor, I2P, or virtual private networks (VPNs); and most important, an updated list of the latest markets, including ratings and reviews. The subreddit includes vendor reviews, security discussions, and a "Markets Superlist" with links to markets, Bitcoin tumblers, e-mail services, and forums. Both *Deep Dot Web* and the subreddit are therefore important gateways into the Dark Web, rivaling other ways of navigating these networks (including search engines, a point I return to in chapter 5).

Global Delivery Systems

Dark Web exchanges that involve goods such as drugs, weapons, counterfeit cash, credit card skimmers, or fake identity documents require delivery of packages. Vendors rely on global delivery networks, such as state-based postal networks or commercial couriers, to deliver their products to buyers. As is well-documented, vendors must develop sophisticated "stealth" packaging techniques to get their goods through customs and delivery network surveillance technologies.[6] This involves using scent-blocking packaging, hiding illegal items inside legal items, or breaking up a product into smaller parts and shipping them piecemeal.

Forum Software

Many of the Dark Web markets include a corresponding forum. These forums enable market administrators, vendors, and sellers to exchange ideas about market practices. Administrators use them to make announcements and to provide basic buying and selling guides. Vendors use them to promote themselves and their products as well as to address customer concerns. Customers use them to review vendors and products, lodge complaints, or provide tips to

one another about how to use the market. In addition, as I explore in detail below, the market forums are used by participants to discuss larger political issues, such as prohibitions on drug use, the power of the state, and the political potentials of black markets.

Political and Social Theory

In addition to the above sociotechnical ingredients that go into the making of Dark Web markets, another ingredient is political and social theory. The remainder of this chapter is dedicated to tracing two such theories, considering how market participants conceptualize their relationship to the state and its claims to the monopoly on violence. First is agorism, a radical libertarian theory holding that society should be organized by market exchanges. The second is OPSEC, an appropriation of a state practice dedicated to reducing the amount of information shared with others.

Agorism

"We are coerced by our fellow human beings."[7] So begins the *New Libertarian Manifesto*, written by radical economist Samuel Edward Konkin III (often referred to as SEK3) in the early 1980s. Coercion, he argues, is happening all the time: your neighbors are preying on you right now. And it's time to fight back.

To fight back, we must smash the state. The state is the

> Mob of mobs, Gang of Gangs, Conspiracy of conspiracies. It has murdered more people in a few recent years than all the deaths of history before that time; it has stolen in a few recent years more than all the wealth produced in history to that time; it has deluded—for its survival—more minds in a few recent years than all the irrationality of history to that time. Our Enemy, The State.[8]

The state is the mechanism by which your neighbors prey on you. Konkin's logic is as follows: the state's monopoly on the use of violent power—in other words, its particular form of legitimacy—allows for it to dictate to us what we can do, think, and say. Through laws and policing, the state compels us to behave. And by paying taxes to it—taxes that are coerced from us via the violent power of the state—your neighbors are feeding this monstrous state the nourishment it needs: ill-begotten wealth. Wealth appropriated via taxes is used to fund the military and police that the state needs to maintain its power.

Thus, for Konkin, the state is the essential source of all coercion, the root of our lack of freedom. He elaborates this point in his *Agorist Primer*:

> Free means the absence of coercion. Coercion is threatening violence upon someone in order to make him surrender something. In a strictly value-free sense, then, coercive human action offers to create greater *disvalue* to you if you do not yield up your lesser value. You gain nothing but lose less.[9]

The state's coercive capacities, its ability to compel us to pay taxes and prohibit us from any activity we may want to pursue (say, use of recreational drugs, making claims to advertise a product, or driving at extremely high speeds) thus makes it libertarianism's number one enemy.

Konkin sees opposition to the state in the agora, or the free market. The agora looms so large that he coined a name for his specific program of libertarian ideology: agorism. Agorism is a radical philosophy that finds the highest expression of human freedom in markets. Markets are spaces in which voluntary, uncoerced exchanges are made. Drawing on the libertarian economist Robert LeFevre, Konkin argues that in a market-based society, "all relations between people are voluntary exchanges—a free market. No one will injure another or trespass in any way."[10] This society would have no prohibition on what we exchange, because there would be no state to impose such restrictions. Likewise, there would be no restriction on what we do or say, so long as our actions do not coerce others. Instead, our actions and ideas would be disciplined by market forces. Order would emerge through market mechanisms: the aggregation of billions of voluntary exchanges would produce a peaceful nonhierarchical social order. A society would emerge through the pursuit of individual gain and profit. Your neighbors would no longer prey on you by supporting the coercive state: they would become your trading partners.

So, how do we starve the beast, the state, and bring about the free market agora? Konkin rejects other libertarian approaches, including formalized party politics (such as the Libertarian Party, recently headed by Gary Johnson in the U.S. presidential election of 2016).[11] The Libertarian Party is a contradiction in terms, Konkin

argues: using a state-sanctioned political practice to take the reins of the state in order to eradicate the state is incoherent.[12] His feelings about voting are similar: voting in government elections is a tacit acceptance of the state's claims to legitimacy. In addition, given the premise that coercive violence is illegitimate, Konkin rejects violent revolution: violence cannot morally overcome violence.[13]

Thus, if party politics (or "partyarchy") and violent revolution are both simply playing the state's game, Konkin sees only one way toward agora: "counter-economics," a form of market anarchy. Starting with the premise that the number and complexity of the state's prohibitions have reached a point where any given trade could be found to violate a law, Konkin argues that much of our economy is composed of "black market" or "gray market" activity. The former is trade in illegal goods. The latter is trade in legal goods by illegal methods (for example, paying a neighborhood kid in cash to mow one's lawn without filing the requisite tax forms). These activities make up the counter-economy. If much of our economic activity is borderline illegal or outright illegal, and if we agree that the state is the root of all violence and that it requires tax revenue to survive, Konkin argues that we ought to consciously move all our economic activities away from state-sanctioned spaces into the counter-economy. And, as more and more of us do so, we will see how social organization can arise outside state sanction.

As the counter-economy grows, it achieves two things: it starves the state of its needed tax revenues, and it develops alternatives to state forms of justice. Certainly, Konkin acknowledges, there may be thieves in such a system, but the market would respond with security and protection products and practices, including locks, insurance policies, and contracts:

> If there were only a few “private thieves” and they were usually apprehended and forced to make restitution, something very close to a free market would exist. People would have locks, fences, alarms, and insurance policies and protection-agent policies, but would act otherwise on the assumption that they were free to give up their property to those of their choice and accept from others who gave freely to them. They could not plan on people changing their minds, but they could make contracts (exchanging a good here and now for one to be given later) so that if others changed their minds, some compensation would result.[14]

A great deal of agorist literature discusses ways to replace government judges with private arbitration firms, hired by market participants to adjudicate contractual disputes.[15]

The literature also discusses justice for those who would engage in antivoluntary, coercive crimes:

> Consistent libertarians see no place for criminals, even to fight other criminals. They believe free-market (all-voluntary) methods will take care of the few criminals; finding them (investigation), arresting them (delegated protection), trying them (arbitration), and restoring lost value to the victim from the aggressors (restitution). The means of accomplishing this vary from communal power to highly technological, competitive business agencies and others in between, such as neighborhood block associations.[16]

Of course, each of these methods would be provided by market means: insurance companies would have investigators in their employ; there would be protection agencies for hire; and arbitrators would ply their trade among parties entering into contracts. If at any point along this process a criminal resists, then and only then would violence be authorized by the agorist society. But Konkin predicts it would rarely come to violence, arguing that there would be no incentive for a person to attack another in the market society, including for an accused criminal to attack a private security force.

After all, once investigations are over and criminals are punished, they would have to re-enter market society and trade with others in order to survive. Thus, to protect their reputations, criminals would acquiesce to punishment.

Put in terms of the symbolic economy of legitimacy I outlined in chapter 2, Konkin and agorism are engaged in the *delegitimation* of the state's claims to a monopoly on violence. Notably, the theory of the state put forward by agorism is congruent with Weberian theories of the state: that it is currently the only social entity with the legitimated monopoly on violence. The agorists, however, would simply argue that the state's monopoly on violence is *illegitimate,* and that the twin institutions of state violence, the police and the military, are engaged in unproductive coercion that inhibits human freedom. Agorism is, thus, a market-based means to dissolve the state's capacity for violence by finding market means for security. The tools and practices of violence would thus be distributed through market mechanisms.

Samuel Konkin's agorist philosophy, developed in the post-countercultural context of the United States in the 1970s, inspired by economists such as Ludwig von Mises, Murray Rothbard, and Robert LeFevre, and disseminated through Konkin's edited publications *New Libertarian Notes*, *New Libertarian Weekly,* and *New Libertarian* until 1990, offered a seductively simple answer to the burning question of libertarianism: What is to be done about the state? Konkin's answer: make markets that are outside state control. But this seductively simple approach has remained largely marginal in larger debates about economy and society. Part of this can be attributed to Konkin's call for "revisionist history," which he felt would help uncover previously hidden agorist practices.[17] Unfortunately, this call associated Konkin with Nazi Holocaust deniers (i.e., revisionist historians who dispute the extent of Nazi death camps).[18] But beyond this troubling association, Konkin's agorism is also likely marginal because he refused, out of principle, to speak at or hold positions in state-based institutions such as universities. Rather than publishing his work in mainstream

economic journals and teaching students at university, Konkin held forth in the living rooms of agorist communal homes and published his work on the Internet.

Nonetheless, while Konkin's and agorism's effect on mainstream economics has been minimal, they have had a presence on the Dark Web, including major influence on the most famous Dark Web site of all, the Silk Road drug market.

Agorism on the Dark Web

Recall that one of the key justifications network builders offer for anonymizing networks such as Freenet, Tor, and I2P is that these networks prevent states from censoring speech, including prohibited political speech. Indeed, the Dark Web has many sites where anonymous users gather and discuss radical politics, including communism, anarchy, and fascism. With agorism's emphasis on building community outside state control via market exchanges, it is quite amenable to the Dark Web. In many spaces on the Dark Web, users have declared their allegiance to agorism with the rallying cry "Agora! Anarchy! Action!"

For example, Freenet users build and maintain a mirror of the Clear Web site Agorism.info, a clearinghouse for agorist writings, including Konkin's works and interviews with contemporary agorists.[19] As a mirror of the Clear Web site, the Agorism.info freesite ensures that the HTML, CSS, PDF, and audio files associated with the original site are distributed across the Freenet network. Recall that Freenet's structure is decentralized; whereas an ISP could block access to the Agorism.info World Wide Web page, Freenet's structure prevents any central authority from blocking access to files. In fact, the Freenet version of Agorism.info has files that are no longer available on the Clear Web version.[20] Another freesite is dedicated to Harry Browne, a libertarian economist who was influential on the author J. Neil Schulman, a friend of Konkin's who wrote the science fiction book *Alongside Night*, about the rise of an agorist society in America.[21] Beyond these freesites, agorism debates and discussion regularly break out on the Freenet forum FMS, particularly on the Politics board.

There have also been eepsites on I2P dedicated to agorism, including secondrealm.i2p (appearing online in 2011; now defunct) and Anarplex (hosted on I2P and mirrored on Tor and the Clear Web). Anarplex is host to the #agora Internet Relay Chat server, a

network inspired “by some leftovers of the Invisible IRC Project,” the precursor to I2P.[22]

But by far, the site that has done the most to bring Konkin’s agorist philosophy to the Dark Web is the original Silk Road marketplace, hosted as a hidden service on the Tor network.

Agorism on Silk Road

Silk Road, one of the first Dark Web markets and its most famous, came to public attention thanks to a *Gawker* story in June 2011.[23] At that point, Silk Road had been online for about five months.[24] The *Gawker* story introduced many tropes about Silk Road that would reappear again and again throughout subsequent journalistic coverage:

- It uses a "sophisticated user-feedback system" to rate vendors on their sales and service.
- It is an "Amazon" or "eBay" for drugs with a wide range of offerings.
- It requires technical skill to access (i.e., one needs to route one's browser through Tor and be able to use the 16-character URL ianxz6zefk72ulzz.onion).
- Its location is "utterly obscured" thanks to its location on the Tor network.
- Its use of the cryptocurrency Bitcoin makes its transactions impossible to trace (a false claim).[25]
- The site is legit—that is, not a scam: one could truly get authentic recreational drugs via a web browser. "It was legit," one customer whom *Gawker* interviewed said. "It was better than anything I've seen."

Along with these tropes, the *Gawker* story also included another: that the site's administrator positioned it not just as a drug market, but as a sociotechnical implementation of agorism:

> "The state is the primary source of violence, oppression, theft and all forms of coercion," Silk Road wrote to [*Gawker*]. "Stop funding the state with your tax dollars and direct your productive energies into the black market."[26]

Indeed, this direct echo of the philosophy of Samuel Edward Konkin III was not accidental—the founder of Silk Road insisted that this political message be included in the *Gawker* story.[27] The *Gawker* piece was the first major media coverage of Silk Road, and it is notable that the spokesperson stressed those agorist ideas.

As Alexia Maddox and colleagues argue, "We need to understand how Silk Road operated not just as a drug-trading market but as a political act and environment."[28] Thanks to the pioneering journalistic work of Eileen Ormsby, the archival work of Branwen and colleagues, and several academic studies, the political aspects of Silk Road are well documented, archived, and available for the analysis Maddox and coauthors call for and engage in.[29] The founder of Silk Road (and very likely the one who responded to *Gawker*), initially referred to by the pseudonym silkroad, later Dread Pirate Roberts (DPR), and now known to be Ross Ulbricht, is widely recognized as espousing agorist philosophy. For example, in a note to site visitors, DPR explained that the site was named for the original Silk Road, the ancient trade route, which "played a huge role in connecting the economies and cultures of [Asia, Africa, and Europe] and promoted peace and prosperity through trade agreements."[30] In a forum post, DPR builds on the idea of trade as a means for peace without states:

> Anything you do that is outside the control of the state is agorist, so in some sense we are all agorists whether we know it or not. Some people just take those actions because of the personal gain they can obtain, which is perfectly fine, but some do it as a conscientious objection and act of rebellion against the state as well.
>
> I'm out to turn unconscious agorists into conscious active ones.:)[31]

DPR's agorist philosophy is further illustrated in his argument *against* lifting legal prohibitions on the use and sale of recreational drugs:

> I keep hearing this argument come up when people talk about drug prohibition: legalize, regulate and tax it. On the surface it sounds like a good idea. No more drug war, more tax revenue, government regulators can make sure it is safe. Makes sense, right?
>
> I can't help but think something is wrong though. Feels like the bastards that have been screwing everyone over all this time still win in this scenario. Now all that money can go to the state and to their cronies, right?
>
> Here's the rub: the drug war is an acute symptom of a deeper problem, and that problem is the state. If they "legalize, regulate and tax" it, it's just one more part of society under their thumb, another productive sector that they can leech off of.[32]

This illustrates the difference between an agorist and, say, a "partyarchist" libertarian who runs for public office. The latter would use the state to relax restrictions; the former simply wants to abolish the state through the use of markets.

Perhaps the single most cited example of DPR's agorist thinking is "DPR's Book Club," a reading group held on the Silk Road forums, where Silk Road users could discuss books and movies that

> focus on agorism, counter-economics, anarchocapitalism, Austrian economics, political philosophy, freedom issues and related topics. My hope is that through this, we will discover what we stand for and foster a culture of peace, prosperity, justice and freedom.[33]

In addition to DPR, multiple participants in the Silk Road forums discussed agorism and the need to shed the state by using markets. Writing about the inevitability of any state engaging in violence, anarcho47 writes,

> Look, the fact of the matter is there are universal, quanifiable [*sic*] facts to life. If you don't eat, you will starve to death. If you don't drink water, you will die of dehydration. If you enact a state, eventually mass violence and mass murder will be a part of life.[34]

In a thread in homage to Dread Pirate Roberts, collapses writes,

> The thing that has always given me confidence in DPR and the mission of this site is this guy's ethics. Here is someone who eloquently preaches market anarchism and wholesale rejection of the putrid, enslaving state. And of all people to man this site it happened to be someone of my own obscure ideological persuasion. He has made agorists of us all. Hero.[35]

And finally, JohnGMcKinley praises the Silk Road:

> When I first heard of the website, I sort of dismissed it. "Well, ok, people are selling drugs on the internet, whatever."
>
> Then I read about the Dread Pirate and realized how big of a thing this is. This is amazing, I daresay revolutionary.
>
> The bulwark against a new age of informational panopticon of statist tyranny.
>
> This idea gives me hope, for the first time in a long time, real tangible hope about the development of a free society out from under the greedy eyes of those who would seek to compartmentalize our lives in order for us as good obedient tax cows on the hamster wheel of the fascist corporate state.
>
> Agorism, I kept hearing the idea talked about but never having a method to go about doing so. This is brilliant.[36]

Certainly, there were many other topics of discussion on the Silk Road forums, including drug safety, vendor reviews, and computer and network security, but multiple scholars and commentators have noted the unusual force of agorist discourse on Silk Road.

As Maddox and her coauthors argue, Silk Road was an example of constructive activism, of prefigurative politics to build "a new

society in the shell of the old."[37] In other words, the ideal of Silk Road was that every trade conducted there would chip away at the state and bring about an entirely market-based society. The prefigurative politics of Silk Road has genealogical roots in the prefigurative politics of agorism, which holds that already-existing entities such as black and gray markets are models for broader social organization. In both cases, *delegitimation* of the overarching social order, a social order perceived to be determined entirely by the needs and violent capacities of a thing called "the state," drives adherents to seek out spaces beyond the state: black markets, where new, nonviolent social organizations can arise. In other words, for both black/gray markets in general and Silk Road in particular, the agorist philosophy holds that it is possible to move beyond the legitimated violence of the state and to build a community centered on mutual exchanges. In the ideal form, agorism undermines the state's monopoly on violence by distributing practices of violence and security according to market logics. Indeed, researchers have found that participants in Dark Web drug markets report that their exchanges are safer than street-based sales and purchases of drugs.[38]

Nonetheless, Silk Road's seizure and the arrest and conviction of Ross Ulbricht radically changed the dominant politics of Dark Web markets.

The Fall of Silk Road and the Decline of Dark Web Agorism

The story of Silk Road's rise is of a particular relationship to state violence, a relationship best understood through the philosophical lens of agorism. But of course, the state (predominantly the U.S. government) ultimately asserted itself, dedicating several years to investigating the Silk Road operation and then using the state's legitimated power to put Ulbricht in prison for the rest of his life. As Judge Katherine B. Forrest stated during Ulbricht's sentencing, "There must be no doubt that lawlessness will not be tolerated. There must be no doubt that no one is above the law—no matter one's education or privileges. All stand equal before the law."[39]

The arrest of Ulbricht, the seizure of Silk Road, and above all the allegations that Ulbricht sought to hire hitmen to kill blackmailers all undermined the agorist messages he was promoting.[40] Indeed, as Dark Web scholars Rasmus Munksgaard and Jakob Demant have argued, discussion of libertarianism on Dark Web market forums has radically decreased since the seizure of Silk Road: "The libertarian political discourse has historically been prevalent on cryptomarket forums. The closure of Silk Road has affected the prevalence of libertarian discourse suggesting that while the closure did not succeed in curtailing the cryptomarket economy, it dampened political sentiments."[41] While Munksgaard and Demant note a decline in libertarian political discussions on Dark Web market forums, they and many other researchers have noted that the seizure of Silk Road did not disrupt Dark Web market activities; if anything, there is more commerce on the Dark Web than ever, spreading across the Tor network and also to the I2P network. Dark Web market forums are also spreading across the Dark Web, from Tor to I2P to Freenet.

The implication of Munksgaard and Demant's argument is that post–Silk Road market forums are solely dedicated to straightforward commercial discussions and thus no longer have an

explicit politics. I would argue, however, that Dark Web market forums do engage in new political discussions, that they have in fact reacted to the U.S. government's seizure of Silk Road with the politics of operations security, or OPSEC, a politics centering on extreme individualism, paranoid securitization, and above all, an appropriation—rather than a delegitimation—of state/military logics.

OPSEC: Operations Security

For security purposes, Dark Web forum participants often avoid linking to Clear Web sites. They make exceptions, however, for information they believe is valuable. A notable exception is a link to a 2012 YouTube video, a presentation by a man with the handle "The Grugq." This video is shared by many Dark Web market forum users, who recommend it to new users hoping to avoid being arrested. As one Dark Web forum poster notes, "I normally would not recommend Youtube videos, but this one is an exception. The Grugq knows his shit."

The Grugq: "Shut the Fuck Up"

In "OPSEC: Because Jail Is for Wuftpd," a presentation given at the 2012 Malaysia Hack In The Box convention, the Grugq lays out techniques for "freedom fighters" (Hack In The Box code for "hackers") to avoid drawing the attention of state agencies.[42] "What the fuck is OPSEC?" he asks. "OPSEC, in a nutshell, is keep your mouth shut. Don't say it. The less you say, the harder it is for people to figure out what you're doing. … In short, shut the fuck up."

The Grugq notes that OPSEC is not a matter of technology, but an issue of mentalities, practices, and our relationships with those around us. Central to OPSEC is a radical distrust of everyone a person associates with. Drawing on a theory of OPSEC from the rapper Biggie Smalls, the Grugq argues:

> Never trust anyone. This particularly goes for people you are operating with. They are not your friends; they are criminal co-defendants. … There is a high likelihood that they [will get busted] because they are dumb, because they are doing what they are doing.

"It hurts to get fucked," he intones, meaning it hurts to go to jail. And because of this pain, "No one is going to go to jail for you. …

Your friends will betray you."

Above all, the Grugq argues for the "freedom fighter" to live in a state of constant paranoia: one needs to be "proactively paranoid [because] you can't be paranoid" in hindsight.[43] Quoting the HBO show *The Wire*, he notes "You only got to fuck up once." To illustrate this point, he details the cases of hackers who failed to be sufficiently, proactively paranoid.

The Grugq also offers specific OPSEC techniques, including

- establishing multiple personas with "legitimate" backstories
- only engaging in "freedom fighting" outside one's home
- avoiding the use of code names for targets and people because "the clever codes you come up with to talk about stuff are terrible"
- constructing network "plumbing" that keeps the multiple personas distinct and separate from one another
- only breaking one law at a time (i.e., if one is transporting drugs in a car, be sure not to break traffic laws)
- never talking to the police

Notably, the Grugq's presentation includes something quite different from agorist thinking: multiple favorable references to the agencies of state power, including the military. Several of his slides feature World War II German military posters with the caption "Feind Hört Mit" (the enemy listens in). Similarly, he includes the World War II U.S. Women's Army Corps poster with the slogan "Silence Means Security." Later, he quotes a U.S. military slogan: "The more you sweat in peace, the less you bleed in war." Thus, in promoting OPSEC to "freedom fighters," the Grugq is promoting an *appropriated* state practice, one developed in the state's continual quest for the monopoly on legitimated violence. Rather than seek to shed the state via markets, an OPSEC orientation is one of homage to the state, even working with the state. In fact, one of the Grugq's

previous occupations was brokering the sales of software exploits to governments around the world; he was a mercenary hacker.[44]

OPSEC's Military Roots

OPSEC is, after all, a military invention, and the rules of OPSEC that the Grugq lays out are not significantly different from those discussed in military theory. According to a heavily redacted, formerly top secret U.S. National Security Agency (NSA) research report, OPSEC has its origins in the United States' war in Vietnam.[45] Between 1965 and 1966, U.S. bombing raids were producing poor results, with low casualties and little damage to Viet Cong or North Vietnamese Army (VC/NVA) equipment. Military leaders were faced with several possible reasons for these failures: (1) their intelligence about enemy locations was faulty; (2) the U.S. command had been infiltrated by spies who were able to warn the VC/NVA about imminent attacks; (3) the VC/NVA had defeated the United States' most sophisticated encryption ciphers; or (4) the enemy had some other means to anticipate attacks and avoid being targeted. The first three seemed unlikely, so the military formed a special research team, Purple Dragon, which reviewed bombing operations from conception to execution to consider the last possibility.

The Purple Dragon team found many methods the VC/NVA could use to anticipate U.S. bombing raids that had nothing to do with breaking U.S. encryption ciphers or infiltrating top-level commands. The team focused on the mundane ways an enemy could gather information: monitoring Voice of America or BBC broadcasts, listening to tactical radio broadcasts and paying attention to military call signs, or reading nonclassified documentation, such as requests for food for specific regions. None of these provided specific information about impending attacks, but as a whole they provided many small details that could be associated by VC/NVA intelligence officers, who could warn their comrades about upcoming attacks. To put it in the Grugq's terms, the U.S. military was not "shutting the fuck up" but was open with its nonclassified information. By training commanders and soldiers to avoid talking about seemingly

insignificant details via “open source” (i.e., nonencrypted or classified) channels, the Purple Dragon team was able to reduce VC/NVA forewarning of bombing attacks from eight hours in 1966 to under thirty minutes in 1968.

Based on the success of Purple Dragon, the value of OPSEC was championed by the NSA, who set up a training course in OPSEC in the 1980s. Thousands of government workers had taken the course by the end of that decade, and OPSEC theory was further standardized.[46] By the end of the decade, President Ronald Reagan signed an executive order instructing all U.S. government agencies and, importantly, contractors to engage in OPSEC training for their employees.[47] The director of the NSA was put in charge of oversight of these efforts; thus OPSEC has become “the third major component, along with signals intelligence and information systems security, of the National Security Agency's mission.”[48] Later, in the 2000s, OPSEC became a big point of contention during the second Iraq War, with concerns about soldiers’ “milblogs” providing too much information about operations. It continues to be a concern as more soldiers use social media.[49] Moreover, OPSEC is a keyword for corporate organizations seeking to defend their intellectual property. A full genealogy of how OPSEC moves from B-52 raids on Vietnam to the boardrooms of transnational corporations is beyond the scope of this chapter, but here I turn to the specific ways OPSEC appears as the new politics of Dark Web markets.

OPSEC on Dark Web Markets

As Angus Bancroft and Peter Scott Reid have documented, Dark Web market participants hold OPSEC in high esteem, mixing technical practices (encryption, Bitcoin tumbling) and "socio-legal deniability" to protect themselves.[50] Yet, academics tend to treat OPSEC as merely a set of tactics and practices for criminals to evade law enforcement agents. I contend that operational security is just as much a political philosophy as agorism by first exploring some basic Dark Web OPSEC practices and discussions, followed by an argument for seeing OPSEC as a political philosophy.

Silk Road Postmortems

The fall of Silk Road inspired lengthy discussions on other market forums about what went wrong. The Hub, a Tor-based forum dedicated to general drug market discussion, has several such postmortems, and the consensus is that Ross Ulbricht engaged in poor OPSEC.

First, the OPSEC-minded analysts argue that Ulbricht did not do enough work to separate his various online identities, pointing to his use of a Gmail account (rossulbricht@gmail.com) as he recruited developers to help build Silk Road in early 2011.[51] Moreover, Ulbricht kept a journal of his activities in building Silk Road. In the Grugq's parlance, Ulbricht failed to create the "plumbing" that would keep his online identities from being cross-contaminated.

Several also note that Ulbricht failed to consistently use PGP—keypair-based encryption used to encrypt e-mails, private messages, and files. As one analyst put it,

> One of the pitfalls of Silk Road 1, is that some of the administrators, including Ross himself did not always communicate using PGP encryption. Once Ross was busted, they had access to his servers and his computers and anything that wasn't encrypted was wide open for them to look at.[52]

In other words, vendor data stored on Ulbricht's computer was in "plain text," rather than in encrypted form, which could have prevented law enforcement from accessing it.

Compounding this problem, Ulbricht refused to require PGP of Silk Road vendors:

> [A vendor was] urging Ross to enforce the use of PGP, to protect the [private messages] and the address information—this matches advice he was given by *many* other people. Ross didn't listen … he was a cementhead (in addition to being an incompetent fool), and now there is very likely going to be another person spending the rest of his life in jail.
>
> I find myself wondering just how many other people are going to be spending their lives in jail, all because they trusted Ross Ulbricht.[53]

Indeed, in the Silk Road forums, DPR argued that to compel the use of PGP would violate a principle of agorism: that all actions arise voluntarily.[54] As Eileen Ormsby has noted, this stance was frustrating to the multiple Silk Road participants who were "security conscious."[55] In other words, security was certainly a concern of many Silk Road participants, but their prescriptions were often ignored in favor of actions more in line with voluntaristic, agorist thinking. As an OPSEC-minded forum poster noted in a postmortem of Silk Road, "Ross relied far too much on voluntarism, in other words, more of that Agorist Libertarian bullshit—just look where the fuck it got us—busts are still being made based on information in the Silk Road databases."[56] To put this in the Grugq's terms, Ulbricht failed to "shut the fuck up," posting messages "in the clear," where people beyond the intended recipient could read them.

Moreover, he failed to require others—including vendors, who would have the names and addresses of customers—to avoid doing the same.

These OPSEC-minded people delegitimated the previously respected Ulbricht by engaging in these postmortems, which in turn legitimated them as security conscious. The lessons Dark Web market forum participants take from the fall of Silk Road are thus framed as OPSEC lessons.

OPSEC Guides

In the period following the arrest of Ulbricht, forums posted guides to OPSEC, and the concept is increasingly seen as fundamental for authentic Dark Web market participation. As a result, a now-standard feature of any Dark Web market forum is an OPSEC tutorial. For example, Outlaw Market's OPSEC guide echoes the Grugq's advice: "When dealing through darknetmarkets OPSEC is always a major issue, this means keep your mouth shut." "Jolly Roger's Security Thread for Beginners" is a lengthy set of forum posts on the Hub, covering everything from PGP basics to examples of OPSEC failures, all to teach new Dark Web market users the proper techniques. The now-defunct AlphaBay Market forum hosted a "Noobs Ask Anything Thread," where seasoned market participants tutor "noobs" in OPSEC skills.[57] Finally, a lengthy set of posts on the now-defunct Darknet Counterfeit Forum, titled "How to Spend Counterfeit 100s," offers guides in passing fake money at major retailers. The techniques and tips are couched in terms of OPSEC, including suggestions that bill passers spend their money far from home and keep their operation a secret from friends and family.

Beyond LEO: OPSEC against Scammers

So far, the implied adversary of Dark Web market administrators, vendors, and buyers is law enforcement; "shutting the fuck up" is a basic means to avoid giving law enforcement any advantage. As the Grugq argues, "Law enforcement is the apex predator" on the

Internet.[58] Yet, starting with Silk Road and continuing on markets today, another major adversary must be overcome: other market participants.

Scammers abound on Dark Web markets; this includes not only vendors, but also administrators. For example, Jonathan Pace's analysis of the court documents from Ross Ulbricht's trial reveals that scams were a constant problem on Silk Road.[59] Likewise, as Ormsby writes of Silk Road 2.0 toward its latter days,

> The discussion forums stopped being a lively, intelligent home of self-styled revolutionaries united in their fight against the war on drugs. Infighting and division became the norm and the site's management became increasingly less visible and engaged, emerging only to provide the occasional update reassuring those who were left that all was fine. Reports of scamming sellers became increasingly frequent, with many accusing the administration of aiding and abetting the scammers.[60]

The short history of Dark Web markets includes multiple incidents of major scams, including the 2015 Evolution market "exit scam," in which the Evolution market administrators absconded with millions of dollars' worth of Bitcoins being held in the market's escrow system. Accounts of smaller scams perpetrated by vendors and sellers frequently appear on forums. Vendors threaten to blackmail buyers by revealing their personal details to law enforcement (thus using the coercive power of the state as a threat). Sellers threaten buyers with bad reviews, and buyers order products, receive them, claim they never arrived, and refuse to pay. As a result, anxiety among market participants is high. For example, the popular Tor- and I2P-based Hidden Answers site now has a "Legit or Sh!t?" section, where anxious would-be buyers ask if various vendors or markets are for real or scams.

In terms of OPSEC, this reveals the wisdom of the radical lack of trust and "proactive paranoia" that the Grugq espouses. Even beyond the observation that anyone arrested in relation to Dark

Web markets would likely betray his or her associates to the police, the ubiquitous scamming that has occurred on Dark Web markets results in Dark Web market participants not trusting one another. For example, common advice to new buyers is to never reveal their addresses to vendors, who can use this information to blackmail buyers by threatening to turn it in to the police. Instead, the OPSEC-minded buyer finds a "drop point"—say, a vacant home in the neighborhood—to receive the shipment. As many scholars of illicit markets point out, there are no courts in which a Dark Web market participant could sue another for fraud or prosecute a blackmailer. The only defense is self-defense. The Grugq argues that a goal of OPSEC is to avoid being put in a position of vulnerability to another person. Similarly, in Dark Web forums, OPSEC is presented as a tool to avoid both law enforcement *and* the possibility of being made vulnerable via blackmail or scams.

Markets for Bad Security

In addition to using OPSEC principles to avoid both law enforcement and potential scammers, OPSEC orients Dark Web market participants to the profit potentials of the world of poorly secured information, including credit card fraud, PayPal and Amazon scams, and the theft and sales of "fullz" (full identification of people, including social security number, addresses, and date of birth). These activities, often referred to as "carding," have a long history that precedes the Dark Web, but Dark Web markets for them have grown over the past few years.[61] As journalistic coverage of the Dark Web shows, there are markets for black-hat hacker services as well.

Carding and black-hat hacking activities reveal the flip side of Dark Web OPSEC: whereas legit Dark Web carders or hackers would protect themselves with OPSEC principles and avoid leaking identifying information, their victims clearly fail to protect their own information and thus become vulnerable and exploitable. In this sense, markets for poorly secured information are a direct result of the increasing pressure to move more and more of our

personal information into digital databases, from our social connections, shopping habits, and credit histories to our state-sanctioned legal documentation.

Although breaking into databases seems like the most effective route to gain such identity information, key practices of obtaining this information exploit "bad OPSEC" practices of victims through social engineering. This can involve using personal persuasion to gain small pieces of information about someone, such as a pet name or birthplace, which can be used to defeat password verification systems. In most cases, such social engineering is effective because most people are trustworthy and helpful.[62] The OPSEC minded, who know to maintain tight control over their own information, seek to gather up the information of those who aren't as paranoid, who simply trust their fellow humans too much.

Dark Web OPSEC Politics

Thus, everything in Dark Web markets is subjected to the intense, proactively paranoid skepticism of the OPSEC minded: from the infrastructural level (Is Tor compromised? Is this market's web software secure?) to the administrative (Are the people running this market law enforcement agents?) to fellow market participants (Is this vendor going to steal my Bitcoins? Am I selling to a cop?) to the larger flows of information (Is this bank routing information secure, and if not, can I take advantage of it?).[63] Above all, this skepticism operates in a larger cultural context of state surveillance: "The increased surveillance of the population noted by a number of writers … has been one of the conditions of possibility … for paranoia—which is not to deny that individuals before this time might have been suspicious."[64] The "proactive paranoia" of Dark Web OPSEC is thus a reflection of larger power dynamics playing out among market participants in relation to one another, to the profit motives of capitalism, and to the state's legitimated monopoly on violence.

All of this sounds as if I'm suggesting that Dark Web market participants are suffering from a pathological condition of debilitating paranoia. I am not. First of all, as David Harper argues, "There is no singular and coherent cultural image of paranoia."[65] Certainly, we can speak of pathological paranoias or conspiracy theories, both of them pejorative labels that bring with them burdens of social stigmatization and delegitimation. But, as Stef Aupers has argued, paranoia has "evolved over the last decades from a deviant, exotic phenomenon to a mainstream narrative that has spread through the media and is increasingly normalized, institutionalized and commercialized."[66] Following the work of Harper, Aupers, and Suzanne Wedow, I argue that we should think of OPSEC's proactive paranoia not as a pathology, but as a rational means to structure relationships and, from there, conceive of a

social order. It is a new Dark Web market politics brought about by exposure of the limits of the agorist ideal.

As Suzanne Wedow has shown in her ethnographic work on drug users in the 1970s, paranoia is a perfectly viable means to structure functioning social relationships and thus build a society.[67] Here, I argue that OPSEC's proactive paranoia provides heuristics for market participants as they relate to the state (an institution that seeks their arrest), to their market colleagues (who could be scammers or easy prey for scams), and to the broader information society (which can be a rich source of data to be stolen and sold). In this view, OPSEC as politics has the goal of social ordering that emerges through radical self-regulation and individualism. It is the legitimate politics of Dark Web markets, appropriated from a state practice: the extreme paranoia of the military regarding information, especially as information leakage reduces the military's ability to kill enemies.

First, OPSEC politics is a means for authentic (i.e., legit) participation in markets, and skill in OPSEC can translate into social and technical power in the markets. This is similar to what Suzanne Wedow observed among drug users in the 1970s: those who could use "anticipatory paranoia" as a storehouse of knowledge to protect themselves and others from law enforcement gain "cool" status as well as social power.[68] In Dark Web forums, OPSEC advice is constantly judged by others, and those who offer advice consecrated as legit gain social capital as being security aware. Such persons can even rise in the organizational structure of the markets, becoming admins and thus gaining administrative power over nonadmin users. A key example is the Guide Review Board (GRB) of the now-defunct AlphaBay Market. The GRB had a similar function to academic peer review, in which experts assess the quality of academic work before it is published. In the case of the GRB, the publications were guides to fraud, including guides on PayPal or Amazon scams. Because anyone can claim to have expert knowledge of such practices, put together a PDF, and sell it for Bitcoins, AlphaBay implemented the GRB to cut down on redundant, poorly

written, or outright incorrect guides. The GRB staff was composed of AlphaBay vendors recognized by the AlphaBay admin for their security and frauding skills; they received first-read privileges on fraud manuals on the site (giving them, as many non-GRB members pointed out, a huge advantage in learning new fraud techniques). Thus, those who are skilled at OPSEC politics—the politics of proactive paranoia—can rise in social stature to administrative roles.

Next, OPSEC politics can be understood in terms of larger political shifts in the Western world. OPSEC politics is the politics of "you're on your own." It should thus be a familiar—if extreme—variety on the politics many in the West are increasingly subjected to: a retrenchment of collective organization (from federal governments on down to neighborhood associations) in favor of the bunker mentality of neoliberalism. In a world where "there is no society, just individuals," as Margaret Thatcher famously put it, the social emerges through highly individualized interactions, rather than through a sense of the collective as such. While this individualistic theory assumes the good will of other individuals, it also warns us that we are on our own as we confront others who might do us harm. All social interaction is guided by caveat emptor. Suspicion and paranoia are rational responses to this: "In most paranoid discourse, the Other has malevolent intent, the result is not only anxiety but self-regulation and suspicion."[69] On Dark Web market forums, new members are advised to "self-regulate" by learning from seasoned, legit, security-aware participants. They are also taught that, in the end, they are solely responsible for their own safety and security. As one participant put it in the Hub,

> Big things are coming … are you prepared to Learn how to protect yourselves?Don't end up like fuckwad Vendors that do not take their Safety and their clients Safety seriously …Learn and progress. … do not stifle yourselves and Fail.

Similarly, the AlphaBay FAQ warned users, "We take no responsibility if you get caught, so protecting yourself is your responsibility."

In this sense, then, Dark Web OPSEC politics is a continuation of agorism. In the agorist theory of Konkin, security practices should shift from state based to market based as entrepreneurs seek ways to reduce the risks they are taking. OPSEC reflects this shift: Dark Web market participants seek to secure themselves against their fellows and the state itself. So far, they are arguably successful: despite scams, fraud, and arrests, sales still happen, deals are made, and money changes hands. There are more Dark Web markets today than ever, and they provide order and discipline through the mechanism of exchange.

Even as OPSEC politics and agorism intersect at the level of caveat emptor, however, the two are distinct. OPSEC reveals the logical outcome of agorism's worship of the self-interested entrepreneur. Despite agorism's insistence that markets can be based on noncoercive principles, markets themselves are predatory institutions. Political economists Samuel Bowles, Herbert Gintis, and Robert Rider have argued that all market exchanges are "contested exchanges" hinging on power relations, predation, and coercion—practices the agorists attribute solely to the state.[70] For Bowles, Gintis, and Rider, the drive for individual profit at another's expense is a fundamental aspect of market exchanges, and exploitation of others logically follows. The only remedy is self-defense, including OPSEC techniques. In agorist theory, the state provides a violent force opposing market exploitation, but it has gone too far in monopolizing violent power.[71] Agorists thus argue it is morally imperative to struggle against, outwit, and exploit the state. But in Dark Web markets, where the state's presence is far less felt on a daily basis, exploitation shifts from the state to fellow market participants, who become possible targets to defraud. As Whitney Phillips aptly puts it, "the idea that a person has the right, and perhaps an obligation, to take advantage of others for their own personal gain is the American dream at its ugliest."[72] Jonathan Pace has taken up this line of analysis in his work on Silk Road, arguing that the "salient principle of economic relationality on Silk Road was not cooperation and freedom but deception and intimidation."[73]

To be fair, agorists would decry these activities as counter to agorism's noncoercion principle, but at the same time, agorism calls for individuals to seek profit above all else.

Thus, put in the terms of Konkin's *New Libertarian Manifesto*, in the social order emerging on Dark Web markets, your neighbors are no longer preying on you by feeding the state; instead they are preying on you by seeking some way to profit at your expense. OPSEC politics is agorism's legitimate offspring, but it rebels against its progenitor by embracing predatory state-developed practices rather than trying to shed them. OPSEC politics is postagorist Dark Web politics, inheriting agorism's hyperindividualism, while shearing away any illusion of community so that all that is left is to exploit or be exploited.

And unlike the rabidly antistatist agorism, as appropriations of a state practice, Dark Web OPSEC practices can be, in turn, reappropriated by the state. One such practice that has developed over the past few decades is government agencies' hiring of or contracting with hackers. As mentioned above, OPSEC expert the Grugq is one such example, formerly brokering deals between hackers and government intelligence agencies who sought to purchase legit hacking services in the service of legitimated violence. Highly skilled Dark Web market OPSEC specialists could parlay these skills into government jobs, and perhaps some already have.

But beyond this immediate appropriation, Dark Web market participants, by engaging with the politics of OPSEC, reinforce rather than undermine the state's claims that communication and information can be weapons. The appropriation of state language regarding communication, including terms such as OPSEC, justifies state claims that information and communication can be "weaponized" and are thus subject to state regulation, what Jack Bratich might call "communications warfare."[74] Examples of this include politicians who declare a "war" on social problems and thus invoke militaristic language and thinking, whether it be a "war on drugs" or a "war on hackers."

Sean Lawson has written extensively about the dangers of linking "cyber" (i.e., communications mediated by computer networks) to "warfare," specifically in the context of arguing that practices such as DDOS attacks or hacking are acts of war. As he notes,

> Arguments in favor of expanding the definition of "war" to encompass "bloodless" cyber actions are … the result of political and military leaders, news media, and others focusing first and foremost on the instruments of cyber conflict rather than their effects or intent of their use. Many different types of actions carried out in/through cyberspace for very different reasons are conflated because they tend to rely upon the same instruments, which are seen as new and unprecedented. Unfortunately, the term under which they have been conflated is "war."[75]

Likewise, journalist Joseph Cox argues that policymakers and journalists metaphorically link software exploits and hacking to weapons, such as missiles and bombs.

> With these analogies there is a danger that debates can become warped or confused. Topics such as whether deploying exploits is proportionate, or whether using exploits can act as tools of deterrence in conflict cannot be tackled without a proper understanding of what exactly a[n] exploit is, and inaccurate comparisons are not going to further the discussion. In place of nuance we are left with hype and potential fearmongering.[76]

The association of "cyber" with "war" is not limited to the rhetoric of (U.S.) political and military leaders or news media outlets; hacker collectives also use the language of war to describe their actions.[77] Likewise, the appropriation of military language—OPSEC—by Dark Web market participants further presents communication as a Manichaean battle. In this way, Dark Web markets have moved from delegitimating the state's coercive power to appropriating the language—if not the *actual* practice—of state violence to understand how to relate to one another. This will further fuel the expansion of

military and police action into spaces of communication, continuing to make communication itself a theater of war, the legitimated sphere of the state.

Thus, we have seen a shift in the politics of Dark Web markets. Based on their delegitimation of state violence, Silk Road agorists fixated on developing freedom through markets. In their view, freedom would emerge through a narrow mechanism of exchanges, new market communities would arise, and the state would wither away. All members would thrive because of course completely free markets liberate all who participate. This short-lived but powerful political ideology was shorn away when Silk Road was seized, revealing the underlying core of paranoia and exploitation that accompany market logics. The new market politics, OPSEC politics, has a more pragmatic relationship to the state, appropriating state practices and transforming them for the Dark Web environment. For OPSEC politics, freedom will emerge not from exchange, but through attrition, as market participants self-regulate their informational practices with the goal of simply outlasting one another as scams and arrests thin their ranks.

Postscript: OPSEC Politics after AlphaBay and Hansa

On July 20, 2017, the head of the U.S. Department of Justice, Jeff Sessions, joined by the acting director of the FBI, Andrew McCabe, and Europol's executive director, Robert Mark Wainwright, announced the seizure of AlphaBay and Hansa markets. Founded around a year after the Silk Road seizure, AlphaBay had become the largest Dark Web market, with sales of drugs, fraud guides, and stolen information that dwarfed the size of Silk Road in its prime. Hansa was not as large but was estimated to be at least the third largest on the Tor network. In Sessions's comments to the press, he announced,

> The dark net is not a place to hide. The Department will continue to find, arrest, prosecute, convict, and incarcerate criminals, drug traffickers and their enablers wherever they are. We will use every tool we have to stop criminals from exploiting vulnerable people and sending so many Americans to an early grave. I believe that because of this operation, the American people are safer—safer from the threat of identity fraud and malware, and safer from deadly drugs.[78]

Wainwright added, "The dark web is not a safe area for criminals."[79]

The press release and associated documents describe a complex operation, in which U.S. agencies—the FBI, Drug Enforcement Agency, Department of Homeland Security, Immigrations and Customs Enforcement, and Internal Revenue Service—coordinated with one another and cooperated with the "Royal Thai Police, Dutch National Police, Lithuanian Criminal Police Bureau (LCPB), Royal Canadian Mounted Police, United Kingdom's National Crime Agency, Europol, and French National Police."[80] Given that Hansa Market was seized by the Dutch police and operated by them for four weeks, all while AlphaBay was seized by Canadian authorities and its alleged founder was arrested in Thailand, this was

undoubtedly a well-coordinated operation—with a high degree of operational security to avoid alerting the administrators, vendors, or users of these markets.

The Department of Justice, as part of its announcement, released a copy of the civil forfeiture complaint filed against the alleged AlphaBay founder, Alexandre Cazes, arguing he was in charge of the site, adding "Cazes was ultimately responsible for [AlphaBay's] operational security and technology updates."[81] Cazes, the alleged operational leader of AlphaBay, was outdone by a complex, sustained, global law enforcement operation.

Just as in the Silk Road bust of 2013, this announcement started a frenzy of discussion on forums dedicated to Dark Web markets, including the Hub, Darknet Market Avengers, and a variety of subreddit threads. Much like the days after the fall of Silk Road, there was much confusion and speculation about how this happened—and a great deal of OPSEC postmortems. For example, on the DarkNetMarkets subreddit, a thread that attracted a great deal of attention is titled "How Alphabay was taken down due to a simple OPSEC mistake." As the original poster explains,

> Guys, You should read the criminal complaint regarding the asset seizure of Alexandre Cazes … here's the juicy bit of how they caught the guy: **They found out that his personal email was included in the header of the welcome email sent out to new users.** The email address was "Pimp_Alex_91@hotmail.com." They subpoenaed information about it, and of course they investigated him closely from there.
>
> They discovered that he had millions of dollars in assets that could not be traced to a legitimate source of income.
>
> Just think about it: He made one mistake, and got fucked. Of course he made a bunch of other mistakes too—like accumulating too many real world assets without a legitimate job or business to back them up.[82]

Immediately, commenters noted the similarity to how Ross Ulbricht was found: bad OPSEC involving an e-mail, including using the

same e-mail address for Dark Web and Clear Web activities. The parallel between Cazes and Ulbricht was so striking it beggared belief: as one commenter wrote, "I can barely believe he would be that stupid that he'd include his personal hotmail in *welcome emails* I mean wtf." But later, the same commenter added,

> after reading the legal case I have to say it all sounds pretty legit. He left traces back in 2008, using his hotmail and nicks [nicknames] all over the place. Cops just pieced it all together and it required little skill.

As the Grugq argues, "you only got to fuck up once."

Unlike Ulbricht, however, Cazes, a Canadian citizen living in Thailand, will face no courtroom or prison time. Before these charges were made public and he could be extradited to the United States, he committed suicide in a Thailand jail cell at the age of twenty-six.

Within hours of Sessions's press conference and the revelations of the global law enforcement operation, the post–AlphaBay Dark Web market communities were once again reiterating the need for better OPSEC, which means they are reiterating the need for proactive paranoia and radical distrust of one another channeled through an online marketplace. They call for a new market administrator who can engage in new economies of legitimacy: balancing the appearance of "legitimate" businesses (to have a reason to have cash and cryptocurrencies) with a market secure enough to fend off the state, the legitimated holder of the monopoly of violence. Such a market would allow for legit vendors and buyers to meet and thus new ways of being authentic within the constraints of OPSEC politics. Once again, they call for the continuation of the adversarial relationship with the state, where market operators face off with state operators in the Manichaean struggle, where communication and information continue to be weaponized.

Despite the state's demonstrated power over life, the speculation is that new markets will rise, with stronger security than before. As one Redditor put it, "despite all the drama i'm a little excited to see

what comes next. The [Dark Web Markets] are so young and at a pivotal point in their development, its great to sit back and watch them evolve over the years."[83] In this view, the OPSEC view, the loss of AlphaBay, Hansa, and Cazes is simply the cost of doing business.

Notes

1. Jonathan Pace, "Exchange Relations on the Dark Web," *Critical Studies in Media Communication* 34, no. 1 (January 1, 2017): 1–13, doi:10.1080/15295036.2016.1243249.

2. Vasilis Kostakis and Chris Giotitsas, "The (A)Political Economy of Bitcoin," *TripleC: Communication, Capitalism and Critique* 12, no. 2 (2014): 433.

3. Alois Afilipoaie and Patrick Shortis, *From Dealer to Doorstep—How Drugs Are Sold on the Dark Net* (GDPO Situation Analysis, Wales: Swansea University, Global Drugs Policy Observatory, 2015), 4, http://www.swansea.ac.uk/media/Dealer%20to%20Doorstep%20FINAL%20SA.pdf.

4. Benjamin Vitáris, "Dark Net Markets Launching Bug Bounty Programs," *Deep Dot Web*, February 22, 2017, https://www.deepdotweb.com/2017/02/22/dark-net-markets-launching-bug-bounty-programs/; "Alphabay statement on PMs bug (fixed now)," Pastebin, January 23, 2017, http://pastebin.com/9whZbnVi.

5. I base this prediction on the fact that distributed peer-to-peer search engines (built on Yacy) and federated social networking (built on diaspora* and GNU social) have been implemented on the Tor and I2P networks. I2P's network topology lends itself to distributed systems; it is known for its support of BitTorrent. Hence, I believe that we will see an OpenBazaar implementation on I2P in the future. Whether that market attracts enough traffic or is competently administered is another matter.

6. James Martin, "Lost on the Silk Road: Online Drug Distribution and the 'Cryptomarket,'" *Criminology and Criminal Justice* 14, no. 3 (2014): 358, doi:10.1177/1748895813505234.

7. Samuel Edward Konkin III, *New Libertarian Manifesto* (Los Angeles: Koman Publishing, 1983), 6, http://agorism.info/docs/NewLibertarianManifesto.pdf.

8. Ibid.

9. Samuel Edward Konkin III, *An Agorist Primer* (Huntington Beach, CA: KoPubCo, 2008), 25. Here, Konkin is using a concept from Austrian economics, *wertfrei*, or "value-free." This is basically an argument for objectivity, rather than subjectivity, in economic thinking. It is a claim that the economic thinking of scholars such as Ludwig von Mises is more scientific than other economic schools of thought (especially Marxian), which (in this view) suffer from the imposition of subjective values. In a wertfrei view, alternative values—say, the value of security provided by the state—are ignored in favor of a strictly marginal value theory, where value is solely measured by one's own perception that the object of the value judgment could reduce one's discomfort. In other words, to be wertfrei in the Austrian economic sense is to be objective about the subjectivity of value.

10. Konkin, *New Libertarian Manifesto*, 11.

11. When discussing the politics of Silk Road, academic literature tends to use the term "libertarianism." I suggest that more specificity is required, since there are many subtle flavors of libertarianism, just as there are many flavors of liberalism, socialism, and fascism. Hence my emphasis on agorism, specifically, and its particular instantiation on Dark Web markets.

12. "Samuel Edward Konkin III (SEK3)—The Founder of Agorism," debate at Dagny's Freedom Festival, Los Angeles, California, 1985, YouTube video, 47:32, posted by David Martin, March 17,

2013, https://www.youtube.com/watch?v=qpoMib89cVk; Samuel Edward Konkin III, "The Last, Whole Introduction to Agorism," *Agorist Quarterly* 1, no. 1 (1995): 3–10.

13. Konkin, *An Agorist Primer*, 56.

14. Ibid., 26.

15. For example, see Brad Spangler's presentation on market-based law beyond the state: "Stateless Law & Counter Economics," a talk by Brad Spangler, March 17, 2011, YouTube video, 31:42, posted by SecularNumanist, March 28, 2011, https://www.youtube.com/watch?v=sWYIIiqPL0Y.

16. Konkin, *An Agorist Primer*, 55.

17. Konkin, *New Libertarian Manifesto*, 7.

18. Ulrike Heider, *Anarchism: Left, Right, and Green* (San Francisco: City Lights Books, 1994).

19. Agorism: Revolutionary Market Anarchism, a freesite based on www.agorism.info, December 20, 2016, http://127.0.0.1:8888/USK@fIkEtTMu6F3f7Y48dB4mmZiyFbB-iddMGBvtruSE3Vc,sFg1GrDfJ-k6BE8VmqqQjw~iOgOKu-aws8law90GeY8,AQACAAE/agorism/13/ [Freenet].

20. These files include an interview with Samuel Konkin in which he draws on science fiction to imagine society without the state: "If the State had been abolished a century ago, we'd all have robots and summer homes in the Asteroid belt." See Samuel Edward Konkin III, "Interview with Samuel Edward Konkin III," interview by _wlo:dek and michal, 2002, http://127.0.0.1:8888/freenet:USK@fIkEtTMu6F3f7Y48dB4mmZiyFbB-iddMGBvtruSE3Vc,sFg1GrDfJ-k6BE8VmqqQjw~iOgOKu-aws8law90GeY8,AQACAAE/agorism/42/docs/konkin-interview.pdf [Freenet].

21. Harry Browne archive, December 20, 2016, http://127.0.0.1:8888/USK@aySB1hz04ZehrSIJ3BiFCoTzAoxDFI5RmHwLJzCcw~I,Tf7Ee~tdmwTUuL7qq4M6JevHj71463p0cLyueU7iQjY,AQACAAE/HarryBrowne/11/ [Freenet]; J. Neil Schulman, *Alongside Night* (New York: Avon, 1987).

22. "#Agora IRC Server," Anarplex, last updated 2013, https://anarplex.net/agorairc/.

23. Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable," *Gawker*, June 1, 2011, http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

24. "SR/DPR-Timeline," accessed February 8, 2017, http://shadowlife.cc/wp-content/uploads/2013/10/SR-Timeline.html.

25. In an update to the story, *Gawker* included comments from Bitcoin developer Jeff Garzik, who dispelled the idea that Bitcoin transactions are anonymous. Despite this, much subsequent media coverage of Silk Road, Tor, and Bitcoin presented all three as anonymizing technologies.

26. Chen, "Underground Website."

27. Eileen Ormsby, *Silk Road* (Sydney: Macmillan Australia, 2014), Kindle.

28. Alexia Maddox et al., "Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital 'Demimonde,'" *Information, Communication and Society* 19, no. 1 (October 15, 2015): 3, doi:10.1080/1369118X.2015.1093531.

29. Ormsby, *Silk Road*; Gwern Branwen et al., "Darknet Market Archives (2013–2015)," Gwern.Net, December 1, 2013, https://www.gwern.net/DNM-archives; Rasmus Munksgaard Andersen, "Intersections of Drug Dealing and Politics—A Macroanalysis of Cryptomarket Discourse" (master's thesis,

Copenhagen University, 2015), https://diskurs.kb.dk/item/diskurs:96023:1/component/diskurs:96022/DiskursVersion.pdf; Rasmus Munksgaard and Jakob Demant, "Mixing Politics and Crime—The Prevalence and Decline of Political Discourse on the Cryptomarket," *International Journal of Drug Policy* 35 (September 2016): 77–83, doi:10.1016/j.drugpo.2016.04.021; Amy Phelps and Allan Watt, "I Shop Online—Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia," *Digital Investigation* 11, no. 4 (2014): 261–272, doi:10.1016/j.diin.2014.08.001; Maddox et al., "Constructive Activism in the Dark Web"; Pace, "Exchange Relations on the Dark Web."

30. Quoted in Ormsby, *Silk Road*, chap. "A Word from the Dread Pirate Roberts."

31. Quoted ibid, chap. "Enter Dread Pirate Roberts."

32. Dread Pirate Roberts, "If Prohibition Is Lifted," Silk Road forums, Darknet market archives, April 29, 2012. https://www.gwern.net/DNM-archives.

33. Dread Pirate Roberts, "***DPR's Book Club***," Silk Road forums, Darknet market archives, August 14, 2012, https://www.gwern.net/DNM-archives.

34. anarcho47, "What Is the Goal of Silk Road?," Silk Road forums, Darknet market archives, September 5, 2011, https://www.gwern.net/DNM-archives.

35. collapses, "To Dread Pirate Roberts," Silk Road forums, Darknet market archives, May 4, 2013, https://www.gwern.net/DNM-archives.

36. JohnGMcKinley, "What Do You See as the Future Implications of the Silk Road and Cypherpunk?," Silk Road forums, Darknet market archives, August 18, 2013, https://www.gwern.net/DNM-archives.

37. Maddox et al., "Constructive Activism in the Dark Web," 4.

38. Monica J. Barratt, Jason A. Ferris, and Adam R. Winstock, "Safer Scoring? Cryptomarkets, Social Supply and Drug Market Violence," *International Journal of Drug Policy* 35 (September 2016): 24–31, doi:10.1016/j.drugpo.2016.04.019.

39. U.S. Attorney's Office, Southern District of New York, "Ross Ulbricht, aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison," press release, Federal Bureau of Investigation New York Field Office, May 29, 2015, https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison.

40. Eileen Ormsby has done excellent work documenting Silk Road users' reactions to the arrest of Ulbricht, as well as the allegation that he hired hitmen and that he controlled Silk Road in a highly authoritarian manner. Ormsby, *Silk Road*.

41. Munksgaard and Demant, "Mixing Politics and Crime," 77.

42. "OPSEC: Because Jail Is for Wuftpd," presentation by The Grugq, YouTube video, 1:04:24, posted by Hack In The Box Security Conference, May 21, 2012, https://www.youtube.com/watch?v=9XaYdCdwiWU.

43. Writing about marijuana use among U.S. college students in the early 1970s, Suzanne Wedow uses a similar phrase: "anticipatory paranoia." Suzanne Wedow, "Feeling Paranoid: The Organization of an Ideology About Drug Use," *Urban Life* 8, no. 1 (1979): 72–93.

44. Andy Greenberg, "Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)," *Forbes*, March 21, 2012, http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-

the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/.

45. Redacted, *Purple Dragon: The Origin and Development of the United States OPSEC Program* (United States Cryptologic History, Fort Meade, MD: National Security Agency, 1993), https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/purple_dragon.pdf.

46. Ibid., 91.

47. Ronald Reagan, National Security Decision Directive No. 298 (January 22, 1988), Presidential Directives and Executive Orders, https://fas.org/irp/offdocs/nsdd298.htm.

48. Redacted, *Purple Dragon*, 92.

49. Sean Lawson, "The US Military's Social Media Civil War: Technology as Antagonism in Discourses of Information-Age Conflict," *Cambridge Review of International Affairs* 27, no. 2 (April 3, 2014): 232, doi:10.1080/09557571.2012.734787.

50. Angus Bancroft and Peter Scott Reid, "Challenging the Techno-Politics of Anonymity: The Case of Cryptomarket Users," *Information, Communication and Society* 20, no. 4 (April 3, 2017): 497–512, doi:10.1080/1369118X.2016.1187643.

51. Joe Mullin, "The Incredibly Simple Story of How the Gov't Googled Ross Ulbricht," *Ars Technica*, January 26, 2015, https://arstechnica.com/tech-policy/2015/01/the-incredibly-simple-story-of-how-the-govt-googled-ross-ulbricht/.

52. Source withheld for privacy.

53. Source withheld for privacy.

54. Doublehelix, "Admins: Make PGP Compulsory? (Please?)," Silk Road forums, Darknet market archives, November 28, 2012, https://www.gwern.net/DNM-archives; GetYourFix,

"REQUEST:Making Pgp a Requirement for a Buyer's Account?," Silk Road forums, Darknet market archives, December 9, 2012, https://www.gwern.net/DNM-archives.

55. Ormsby, *Silk Road*.

56. Source withheld for privacy.

57. AlphaBay was seized in July 2017. The emerging analysis of the end of AlphaBay is similar to the postmortems of Silk Road: an analysis of OPSEC failures on the part of AlphaBay's administrators. This discussion is happening on Reddit and the Hub.

58. "OPSEC: Because Jail Is for Wuftpd."

59. Pace, "Exchange Relations on the Dark Web."

60. Ormsby, *Silk Road*.

61. Alice Hutchings and Thomas J. Holt, "The Online Stolen Data Market: Disruption and Intervention Approaches," *Global Crime* 18, no. 1 (January 2, 2017): 11–30, doi:10.1080/17440572.2016.1197123.

62. Christopher J. Hadnagy, Mati Aharoni, and James O'Gorman, *Social Engineering Capture the Flag Results: Defcon 18* (n.p.: Social-Engineer.org, 2010), http://www.social-engineer.org/wp-content/uploads/2014/03/Social-Engineer_CTF_Report.pdf.

63. Indeed, a common tactic used by law enforcement is to seize a site and then run it for a period, pretending to be the site's administrators, all the while gathering information on site users. This happened in 2017 with the Hansa Market, where Dutch law enforcement agents seized the site and ran it for a month. Similarly, Joseph Cox reports that the FBI ran a child exploitation image site; see Joseph Cox, "DOJ, FBI Executives Approved Running a Child Porn Site," *Motherboard*, May 29,

2017, https://motherboard.vice.com/en_us/article/doj-fbi-child-pornography-sting-playpen-court-transcripts.

64. David Harper, "The Politics of Paranoia: Paranoid Positioning and Conspiratorial Narratives in the Surveillance Society," *Surveillance and Society* 5, no. 1 (2008): 4.

65. Ibid., 10.

66. Stef Aupers, "'Trust No One': Modernization, Paranoia and Conspiracy Culture," *European Journal of Communication* 27, no. 1 (2012): 24, doi:10.1177/0267323111433566.

67. Wedow, "Feeling Paranoid."

68. Ibid.

69. Harper, "The Politics of Paranoia," 6.

70. Samuel Bowles and Herbert Gintis, "Contested Exchange: New Microfoundations for the Political Economy of Capitalism," in *The Economic Nature of the Firm: A Reader*, ed. Louis Putterman and Randy Kroszner, 217–232 (Cambridge: Cambridge University Press, 1996); Robert Rider, "Conflict, the Sire of Exchange," *Journal of Economic Behavior and Organization* 40, no. 3 (November 1999): 217–232, doi:10.1016/S0167-2681(99)00065-7.

71. This is, in fact, the origin story of the state told by Konkin in *An Agorist Primer*.

72. Whitney Phillips, *This Is Why We Can't Have Nice Things: Mapping the Relationship Between Online Trolling and Mainstream* (Cambridge, MA: MIT Press, 2016), 134.

73. Pace, "Exchange Relations on the Dark Web," 2.

74. Jack Bratich, "User-Generated Discontent," *Cultural Studies* 25 (September 2011): 626, doi:10.1080/09502386.2011.600552.

75. A DDOS attack is a "distributed denial of service" attack, where a large group of computers is coordinated to visit the same website at the same time. The sheer volume of requests overwhelms the website's server, and the site goes down—hence "denial of service." Sean Lawson, "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States," *First Monday* 17, no. 7 (2012), http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270.

76. Joseph Cox, "It's Time to Stop Comparing Exploits to Physical Weapons," *Motherboard*, July 17, 2017, https://motherboard.vice.com/en_us/article/mbaxxv/its-time-to-stop-comparing-exploits-to-physical-weapons.

77. E. Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (New York: Verso, 2014). I owe credit to Katy Razzano for pointing to hackers' use of war metaphors.

78. U.S. Department of Justice, "AlphaBay, the Largest Online 'Dark Market,' Shut Down," press release, July 20, 2017, https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.

79. Ibid.

80. Ibid.

81. U.S. Department of Justice, United States of America v. Alexandre Cazes, filed July 19, 2017, 17, https://www.justice.gov/opa/press-release/file/982821/download.

82. Rimlogger, "How AlphaBay was taken down due to a simple OPSEC mistake," DarkNetMarkets (subreddit), July 20, 2017, https://www.reddit.com/r/DarkNetMarkets/comments/6ogs83/how_alphabay_was_taken_down_due_to_a_simple_opsec/.

Original emphasis. Alexandre Cazes is the alleged "Alpha02" administrator.

83. Wombat2combat, "What to do now and future tips," DarkNetMarkets (subreddit), July 20, 2017, https://www.reddit.com/r/DarkNetMarkets/comments/6ohder/what_to_do_now_and_future_tips/.

5 Searching for the Google of the Dark Web

As I discuss in the introduction, one of the definitions of the Dark Web I reject is the Deep Web characterization, which holds that it comprises everything Google hasn't indexed. This definition implies that there are layers to the Internet, each one more impenetrable than the last, where only those with elite computer networking skills can navigate. It also implies that there are no Dark Web search engines.

Actually, quite a few search engines specialize in crawling, indexing, and sorting Freenet freesites, Tor hidden services, and I2P eepsites. One of them, onion.link, even uses a Google Custom Search engine, meaning—despite all the news stories and academic articles that say otherwise—Google has crawled significant parts of the Dark Web.[1]

The concept of a "web beyond Google" might give the Dark Web a lot of mystique, the idea that there is a web beyond the web, out of reach of those of us who engage in Google searches, only vaguely aware that there is more to the network than what Google caches. It also gives the makers of Dark Web search engines a lot of motivation: What if I could beat Google to these new networks? What if my search engines becomes, to use an often repeated phrase, the Google of the Dark Web? What if it becomes a legitimate portal into the Dark Web?

This chapter takes up Dark Web search engines and considers them through the specific lens of legitimacy as propriety, or the sort of legitimacy that corporations and nonprofit organizations seek. I first elaborate on what I mean by propriety and, following that, briefly lay out a theoretical framework for the chapter. Then, drawing on interviews with Dark Web search engine operators, archival research, and participant observation (including using multiple Dark Web search engines as well as installing and running distributed search engine software), I consider how Dark Web

search engines seek propriety by aligning the interests and perceptions of various other entities, including Dark Web users and nonusers, humans and nonhuman entities. In doing so, I hope to answer the call for research on search engines that focuses on their "gatekeeping" capacities and how they technically function.[2] I also hope to highlight the importance of search engines as entry points into specialized networks, such as the Dark Web; this focus on search can illustrate a portal by which Dark Web nonusers can become users. To emphasize this, I conclude by considering how these search engines seek to gain a big inheritance: the title of "Google of the Dark Web," thus inheriting Google's legitimacy.

Propriety: Commanding Respect, Commanding Resources

Organizational and managerial communication literature reveals two facets of legitimacy. First, legitimacy is about perceptions. Second, legitimacy is about resources.

For the first facet, I return to organizational sociologist Mark Suchman's definition of legitimacy. Legitimacy is "a generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions."[3] This places organizational legitimacy firmly within the bounds of strategic communication and perception management. For example, writing about challenges to organizational legitimacy, Myria Watkins Allen and Rachel H. Caillouet argue, "Corporate actors, especially those whose legitimate right to operate is being challenged, embed self-presentation strategies in their external discourse to control perceptions within their organizational field."[4] For scholars of start-ups, such as Monica A. Zimmerman and Gerald J. Zeitz, legitimacy is so important that its acquisition should be the first goal of the new venture, even ahead of becoming profitable: "New ventures need resources from their environment, and, in the end, the motivating factor for external actors to give such resources is their *belief or feeling* that the venture is indeed competent, efficient, effective, worthy, appropriate, and/or needed."[5] In other words, if a start-up is perceived to be legitimate, it is more likely to attract venture capital.

Second, many organizational and managerial communication scholars note that organizational legitimacy has a relationship to the command of resources. To put it simply, organizations are perceived to be legitimate by dint of the fact that they have resources.[6] If organizational legitimacy is about perceptions, it stands to reason that organizations with the resources to engage in advertising, sponsorship, or lobbying enjoy increased odds of being perceived as desirable, proper, and appropriate.[7] To use a term from

the symbolic economy of legitimacy, organizations with resources can simply purchase legitimacy through ad campaigns. Furthermore, in contemporary capitalism, a firm's legitimacy is often measured in terms of its resources. In this view, a firm's profitability reflects the fact that consumers have chosen it over others when making purchasing decisions. More profits means more legitimacy. In fact, an extreme example of this resource-first-legitimacy-later approach can be seen when a previously illegal business "goes legit." As R. T. Naylor caustically notes, "Today's [criminals] ... may well be tomorrow's free-market pioneers. Someday Bogotá may well host the Pablo Escobar School of Business to vie with certain North American institutions bearing the names of notorious tobacco barons or booze smugglers."[8] Nonprofits pursue resources such as government grants not only to fund their organizations, but also as a marker of their legitimacy.[9] The more grants and donations the nonprofit can attract, the more legitimate it is.

Indeed, these two facets of legitimacy—perceptions and resources—present a causal quandary. Does the perception that an organization is legitimate give it access to more resources? Or does the command of resources give an organization the perception of legitimacy?[10] Rather than seeking the causal factor, however, I instead turn to organizational studies scholars who argue that we must attend to the relationships between social, technical, economic, and political factors as organizations take shape. My suggestion that this form of legitimacy is best understood as *propriety*, in the dual sense of something being proper as well as commanding resources and property (as in proprietorship), is meant to emphasize that we must simultaneously examine how organizations command both respect and resources. In this sense, legitimacy as propriety echoes the Weberian theory of state legitimacy, which holds that the state seeks a monopoly on the material tools of violence (weapons, militaries, police forces) *as well as* the perception that the state is the rightful master of these tools. Organizations seek something similar: command of resources

(employees, profits, property) *as well as* the perception that they are the rightful masters of these resources.

Thus, to investigate Dark Web search engines through the lens of organizational legitimacy, we have to consider how search engines simultaneously develop the "generalized perception" of their propriety as well as their capacities to command resources. Moreover, this has to be done within the specific environment of the anonymizing networks Tor, I2P, and Freenet. As Zimmerman and Zeitz argue, any new organization "will face a different set of relevant environmental forces" as it seeks to command respect and resources. "No organization can be consistent with all environments; the point is for the new venture to be clear about the particular mix of environmental factors that is important to its survival."[11] Likewise, any investigation of the legitimacy of Dark Web search engines must take into account the specific environmental factors in which they operate.

Organizing Resources and Respect

If propriety is a perception of the appropriateness of the organization as well as its ability to command resources, we are already dealing with heterogeneity. We're dealing with feelings and things. The problem is compounded when we consider the specific environment in which Dark Web search engines must operate, as well as the perceptions and resources Dark Web search engines must bring together, a list that includes

- the perception that the search engine provides accurate results
- a system to index Dark Web sites
- the values of anonymity and privacy
- network topologies, capacities, and latencies
- what individual users are searching for
- software packages that can manage search databases

Any successful Dark Web search engine must balance these and other perceptions and resources to gain status as a legitimated point of passage into the Dark Web. Again, it would be difficult to tell whether the perception of a Dark Web search engine's legitimacy would precede its command of resources, or whether resources, such as a large index of sites, would precede the perception. It is best, therefore, to think of all these elements in relation to one another.

For a framework to investigate these elements, I turn to a school of organizational studies that draws on actor-network theory and whose members include Barbara Czarniawska, Susan Leigh Star, John Law, and Michel Callon, scholars who have written extensively on how heterogeneous elements can be brought together into organizations that, to paraphrase Barbara Czarniawska and Tor Hernes, have legitimacy emerge through their organizing.[12] Callon,

a key figure in this field, has argued that organizations establish themselves as "obligatory points of passage" by naming various sets of actors with whom they want to have a relationship; defining relations between them; defining their interests; and presenting themselves as mediators between all the other actors on the network.[13] Law similarly speaks of organizations as capable of harnessing the power of other elements in a network:

> Actors (including collectivities) struggle to impose versions of reality on others which define a) the number of those others, both natural and social, that may be said to exist in the world, b) their characteristics, c) the nature of their interrelations, d) their respective sizes and e) their positions with respect to the actor attempting [to impose its version of reality].[14]

In other words, if an organization can "impose its reality" on others, it is far more likely to be legitimated. Importantly, for Callon and others in this school, "actors" includes human and nonhuman elements, discourses, and materials, any of which can be drawn on to support the legitimacy of the organization. Respect and resources must both be attended to.

Callon's observation that successful organizations present themselves as obligatory points of passage is especially important in considering Dark Web search engines. After all, a basic relationship mediated by search is between user and information. In fact, multiple relationships are mediated by search engines, a point I explore in depth below. Here, I want to point to another organizational scholar, Susan Leigh Star, who has argued that we need to pay attention to infrastructures as we do our analysis. Infrastructure, which she defines as background, connective processes, and systems, is "part of human organizing."[15] Operating in the background, infrastructural systems are taken for granted. As sociotechnical systems, however, they can shape a great deal of our daily lives. Her key question is, "What values and ethical principles do we inscribe in the inner depths of the built information environment?"[16] Star's question is an important one to keep in

mind as we analyze Dark Web search engines, since their legitimacy hinges in part on their ability to become infrastructural, essentially backgrounded parts of Dark Web interaction.

Finally, and in a related vein, this school of organizational studies reminds us to pay attention to elements that the organization hides or simplifies. John Law, Annemarie Mol, Gail T. Fairhurst, and François Cooren have all written about the relationships between presence and absence and simplification and complexity.[17] In terms of presence and absence, Fairhurst and Cooren consider how political or corporate leaders work to establish their authority and power, arguing that successful leaders are able to highlight elements that make them look favorable and suppress others that do not.[18] To put this into the terms of the symbolic economy of legitimacy, this latter practice is *delegitimation*. Yet, going so far as to hide other elements is often unnecessary; as Law argues, organizations can simply tell "ordering stories." "When we tell ordering stories we simplify and 'punctualize.'"[19] This is because

> not everything can crowd into a single place, and implosion, or, perhaps better, condensation, is impracticable. Perhaps this is a general principle, but, linked to concern with design and control, it's what the actor-network theorists point to when they tell of "punctualization." That which is complicated comes in simple packages … that can be used to make sense.[20]

In other words, instead of hiding unwanted elements, sometimes they can be hidden in plain sight by simplifying them, ordering them, or organizing them. To put this in terms of the symbolic economy of legitimacy, this can be *appropriation* (if the simplification is exploitative) or *exchange* (if the simplification is mutually beneficial).

Organizational studies scholars working in the actor-network theory tradition sound a note of caution, however, about hiding and simplification: these processes are not guaranteed. Hidden or simplified elements often resist the ordering stories and attempt to reassert themselves rather than be silenced. This is a point

hammered home in Michel Serres's book *The Parasite*, a work that has been influential on actor-network theory.[21]

Thus, if legitimacy at the organizational level is about aligning perceptions and marshaling resources, with these activities done in specific environments, the organizational studies scholars who attend to the relationships between heterogeneous elements are useful guides. All of these scholars highlight elements in organizing that can play roles in constructing an organization's command of respect and command of resources. Taking up these organizational studies scholars, I want to suggest key ideas:

- Communications and information organizations, such as search engines, are made by defining others, their relations, and their interests, and then mediating between most or all of them.
- These organizations attend to both technical and social elements and seek to become infrastructural, a taken-for-granted point of passage into the larger network.
- They also rely on hiding and simplifying others, delegitimating some elements, inheriting or appropriating from others, or exchanging with still others.
- Finally, they have to respond to challenges to their legitimacy, including challenges from elements that were previously hidden or simplified.

If a Dark Web search engine can achieve all of these goals, it can gain legitimacy as propriety. Aligning interests can aid search engine developers in achieving the perception of appropriateness. Becoming infrastructural will give them access to and influence over informational resources. Successfully dealing with elements that resist their ordering stories will further solidify their positions. The interaction between perceptions and resources can continue to strengthen the search engine in the network, to the point where Dark Web users agree that the search engine is legit. Legitimacy as propriety thus becomes a multiply caused effect of these alignments.

Dark Web Search Engines

In this section, I consider a range of Dark Web search engines (table 5.1), some still running, others no longer available.

Table 5.1 Search engines across various Dark Web networks

Name	**Network(s)**
not Evil	Tor
Direct	I2P (inactive)
elgoog	I2P, Tor (inactive)
Ahmia	Tor, I2P
MoniTOR	Tor (inactive)
Freegle	Freenet (inactive)
Grams	Tor
Enzo's Search	Freenet
Seeker	I2P
Beast	Tor
Eepsites.i2p	I2P (inactive)
Epsilon	I2P (inactive)
Onion.link	Tor
Candle	Tor

I am arguing not that any of these search engines have succeeded in legitimating themselves, but that they are (or were) engaged in a great deal of work to achieve that status. To explore this, I first consider their naming of other actors and their relations. I next consider how they mediate between various points on the network, seeking to become infrastructural. I finally consider how Dark Web search engines attempt to hide or simplify other elements in the network, even as some of those elements resist such attempts.

Naming Others, Relations, and Interests

First, to legitimate themselves, makers of these various Tor, I2P, and Freenet search engines must name relevant actors, identify relations among them, and discover their interests. Based on interviews with Dark Web search engine operators and analysis of developer mailing list archives, IRC chat logs, technical papers, archived Dark Web sites, and grant funding applications, I summarize the relevant actors and interests in table 5.2.

Table 5.2 Actors and interest relations potentially mediated by Dark Web search engines

Actor	**Interests**
The network	Maintain bandwidth and anonymizing capacities
Sites	Be found (although some sites want to hide)
Vendors	Be found; gain and maintain reputation as legit
DW users	Find sites or new content
Law enforcement	Identify sites and subjects; arrest lawbreakers and seize servers
Spiders	Access, duplicate, and store Dark Web pages
Protocols	Retain anonymity; condition access
Other search engines	Become the "Google of the Dark Web"
Network builders	Gain organizational legitimacy; maintain the viability of the network
Nonusers	Read about Dark Web in news; opine about necessity of Dark Web

Second, after establishing the relevant actors, Dark Web search engines seek to align interests by mediating between as many of these actors as possible, inserting themselves into (or even constituting) relations between these actors. I consider *users and networks, network builders and nonusers, Dark Web sites and law*

enforcement, users and law enforcement, vendors and buyers, and finally, *software and protocols*.

Users and Networks

The relationship between Dark Web users and the Tor, I2P, or Freenet networks is the controlling relationship. Search engines seek to become the main channel for this crucial pair of actors. One the one side, we have the extreme heterogeneity of users, who may seek any number of things, from music, pornography, or conspiracy theories to mental health support or cat facts.[22] Viewed through Daniel E. Rose and Danny Levinson's conceptual framework, they might be navigating (e.g., trying to find a specific web page), information seeking (e.g., researching a specific topic), or resource seeking (e.g., trying to find software or be entertained).[23] On the other side, we have an almost equally heterogeneous collection of websites hosted on Tor, I2P, or Freenet: social networks, blogs, forums, home pages, and markets, all covering a wide range of topics. Some of these sites' operators want them to be found; others seek to remain hidden.

Between these two sit a host of potential mediators, including directories, wikis, knowledgeable users who share links, Reddit subreddits, publications such as *Deep Dot Web*, myriad trails of links between sites, and search engines, my focus here.

Across a range of mailing lists and IRC chats, Dark Web users have called repeatedly for reliable search. As Matthew Toseland of Freenet noted in 2005, "Every user sooner or later asks 'why isn't freenet searchable?'"[24] When search engine operators present their work, they often argue that their engines are services that will benefit users most of all. For example, in an interview, the administrator of Tor's not Evil search engine likened a good search engine to parents: "They serve as a guide. You're supposed to be able to trust them with your questions."[25] Another Tor search engine operator argues that "the more of us who build engines, the more detailed and differing information will be available to the average user."[26] Likely because of the influence of Google, many

users expect Dark Web networks to be navigable via search engines: as Juha Nurmi (founder of the search engine Ahmia) puts it, a "Google-like search site is the most user-friendly solution" to the problem of navigating the Dark Web.[27]

In addition, search engine operators argue that the networks themselves will benefit from their engines. As Enzo argued in an interview with me, "I would say the one thing Freenet needs the most is users. Users make Freenet interesting. Some of those users will become contributors, providing new and interesting content, code, documentation, translations, bug reports, or feedback."[28] Enzo suggested that Enzo's Search would contribute to the goal of adding more users to Freenet. Given the structure of Tor, I2P, and Freenet, which relies on network traffic to obfuscate the identities of users, increasing numbers of users on these networks generally translates into stronger anonymity. More traffic could also translate into more heterogeneous content; as new users access Dark Web sites, they might decide to host their own to fill perceived gaps. Indeed, in addition to calling for search engines, users also call for more content to be hosted on Tor, I2P, or Freenet.

As one I2P developer notes, however, a poorly implemented search engine could actually discourage users and thus harm the networks: "Because if its not a service providing in depth information and a good overview about I2P content, it might actually hurt us. Someone using I2P first time might be disappointed, that the results wont keep up with google etc and assume theres actually no good content on I2P."[29] Likewise, Matthew Toseland notes that with inadequate search in place, "One obvious disadvantage is that users will search for something, won't find it, and will assume freenet is crap. :)"[30] Thus, if these networks introduce search engines, the stakes are high: they have to satisfy users' heterogeneous search queries and return "good content" or they risk their networks being perceived as "crap."

This basic relationship between users and networks, mediated by search engines, helps structure many other relationships and interests, including between the network builders and nonusers, law

enforcement and hidden website operators, users and surveillance systems (both corporate and government), vendors and buyers, and software and Dark Web protocols.

Network Builders and Nonusers

In chapter 3, I trace the practices of the group I call the network builders—the coders, developers, and promoters of Tor, I2P, and Freenet. While a great deal of that development is technical (as in the development of protocols, networking schemes, and encryption practices), a significant part of the work is social: Tor, I2P, and Freenet developers also work to construct the reputation of their projects for the general public of nonusers. By "nonusers" I mean any consumers of news stories about the Dark Web who do not use the Dark Web themselves. This is obviously a heterogeneous group, and although it does not include current Dark Web users, it nonetheless has significant influence on the viability of these projects. Nonusers can react to what Wendy Hui-Kyong Chun calls the "extramedial representation" of the Dark Web, "the representation of networked media in other media and/or its functioning in larger economic and political systems," by calling for or consenting to these projects being shut down, made illegal, or starved of funding.[31]

Networks builders' efforts to present their work as contributing to general communications welfare have been largely overshadowed by journalistic coverage of the taboo activities of Dark Web users and site operators. Tor in particular has been associated with the Silk Road drug market, Freedom Hosting's child exploitation images (CEI), and stories of hackers for hire. Freenet and I2P have had less coverage, but negative stories about both have also been published. To combat this image, the developers at the Tor Project, Invisible Internet Project, and Freenet have called for adding more mainstream services that may be recognizable to nonusers. This entreaty is directly tied to the perception of how appropriate these networks are.

To better present Dark Web networks to the general public, a central service that network builders call for is a search engine. As Freenet developer Arne Babenhauserheide argues, "For [Freenet to be] *more* socially acceptable we need more actively spidering [indexes] which only include what the creator deems acceptable."[32] In other words, to be legible to nonusers, Freenet needs more search engines (built in part through spiders that index Freenet) capable of highlighting "acceptable" content.

Perhaps the best example of a search engine mediating between network builders and nonusers is Juha Nurmi's Ahmia, which indexes Tor and I2P. Nurmi and his engine operate as ambassadors for the Tor Project. He frames his search engine as a transparency tool, bringing Tor hidden services and I2P eepsites to light. Rather than framing Ahmia as a system that makes largely taboo activities visible (as the Electronic Frontier Foundation's Jeremy Malcolm does), Nurmi uses statistical data produced through his crawler to claim that only a tiny number of Tor hidden services are dedicated to CEI or trade in illegal goods, and thus the majority of Tor services are appropriate and acceptable.[33] As Nurmi argues in a slide presentation,

> Unfortunately, many times the popular news about Tor are telling about drugs, guns and child porn … [which is] bad for Tor's reputation. In reality, there are only [a] few [of] these kind of sites. Ahmia has the real statistics:
>
> Less than 20 child porn sites
>
> Less than 10 black markets
>
> A few scamming sites.[34]

In a Knight Foundation News Challenge application, Nurmi contends,

> We are solving a key problem with hidden services. The problem is that it is hard to find content published anonymously using Tor. We are making Tor network accessible in many different ways: listing Hidden Services, gathering their descriptions and providing full text search to the content. We can also provide cached text versions of the pages. ...
>
> We are building good reputation to Tor network along with other online anonymity systems, such as Globaleaks and Tor2web, software project originally made by Aaron Swartz now maintained by Hermes Center for Transparency and Digital Human Rights. We have plans to integrate Globaleaks and Tor2web to our search engine.[35]

Here, Nurmi associates transparency and "good reputation," and he links Ahmia with other acceptable practices and sites, such as the whistleblowing site GlobaLeaks. He also invokes Aaron Swartz, the activist whose suicide came after what many in the free information community saw as brutal treatment by U.S. federal law enforcement.

Ahmia, as Nurmi told me in an interview, is meant "to support human rights, such as privacy and freedom of speech. ... It's like Google search for onion sites."[36] Nurmi best exemplifies a mediator between the Tor Project and the general (non-Dark-Web-using) public, and his rewards have included sponsorship by the Tor Project at the Google Summer of Code in 2014. This is a legitimacy exchange: as Nurmi seeks to improve the reputation of anonymizing networks, he builds his reputation as a skilled computer scientist who supplies a needed search engine service to network builders, users, and a general public largely wary of the Dark Web.

Dark Web Sites and Law Enforcement

In a story in *Digital News Asia,* Jeremy Malcolm of the Electronic Frontier Foundation argues that criminal activity moving onto the Dark Web will make crime more visible, not less:

> The advantage of criminals using hidden services is that at least it provides transparency about the problem. Often law enforcement agencies will spout made-up figures about how much crime is conducted online, which others have no way of verifying. … But with hidden services, it is possible to get a better idea of what previously happened under wraps. This is the first step towards catching and prosecuting those criminals using conventional investigation methods.[37]

This argument is echoed by Dark Web market researchers James Martin and Nicolas Christin, who note that

> in contrast to the secretive and opaque world of conventional drug markets, the online drugs trade takes place largely in the open. Protected by anonymizing technologies, online drug vendors freely advertise their products, including prices, quantities and the regions to which goods may be sent.[38]

In other words, Dark Web crime is far from hidden: it is made visible, with evidence being collected automatically as Bitcoins move from one wallet to another and as forum posts are recorded. Indeed, my analysis of the politics of Dark Web markets in chapter 4 was aided a great deal by scholars who have built archives of market activities, many of whom are keenly interested in the scale and scope of criminal activities on the Dark Web.[39]

Search engines can be part of this, creating new relationships between Dark Web sites and law enforcement. Given search engines' capacities to aggregate and organize data on websites, it is not surprising that they could be seen as tools for law enforcement investigations. The best example is the Memex search engine of the Defense Advanced Research Projects Agency (DARPA). Named after Vannevar Bush's famous 1945 thought experiment, DARPA Memex

> will not only scrape content from the millions of regular web pages that get ignored by commercial search engines but will also chronicle thousands of sites on the so-called Dark Web—such as sites like the former Silk Road drug emporium that are part of the TOR network's Hidden Services.[40]

Beyond indexing a large range of websites, including Tor hidden services, Memex is being designed to return detailed and linked results on specific search tasks. The initial task used to introduce Memex to the public was combating human trafficking:

> DARPA plans to develop Memex to address a key Defense Department mission: fighting human trafficking. Human trafficking is a factor in many types of military, law enforcement and intelligence investigations and has a significant web presence to attract customers. The use of forums, chats, advertisements, job postings, hidden services, etc., continues to enable a growing industry of modern slavery. An index curated for the counter-trafficking domain, along with configurable interfaces for search and analysis, would enable new opportunities to uncover and defeat trafficking enterprises.[41]

Thus, Dark Web search engines can be deployed as tools for law enforcement. Obviously, beyond Memex, there is no reason that law enforcement agencies cannot use any Tor, I2P, or Freenet search engines to research and track Dark Web sites and activities.

Users and Law Enforcement

Dark Web development has been driven, in part, by the perceived overreach of government agencies, including DARPA, the NSA, the UK's Government Communications Headquarters (GCHQ), and Communications Security Establishment Canada (CSEC). Government agencies monitor Clear Web users' search patterns or take warrants to corporations such as Google to gather data on users. In contrast, while search engines built for the Dark Web may

make *sites* more visible, they tend to deny law enforcement easy access to users' search records. For example, Ahmia seeks to keep law enforcement at a distance with its legal policy:

> We take your privacy seriously: we absolutely do not maintain any IP address logs. We have no information to share to any third parties regarding usage of the Ahmia service.
>
> We do not allow backdoors into our services for access by authorities or anyone else. Officials who want information for criminal investigations must contact the Ahmia Project Leader with a warrant. If this happens, we will publish the warrant and challenge it.[42]

Although other Dark Web search engines do not post such detailed legal policies, in interviews, their operators claim that their services will help protect end users against government surveillance. Given that Tor, I2P, and Freenet were developed in part to protect the anonymity of users, search engine operators are delegitimating the state's attempts to deanonymize and track user activities.

Considering the claims of the developers of DARPA Memex and the developers of Ahmia, Seeker, or Enzo's Search, broadly speaking, Dark Web search will in fact make hidden sites more accessible to all users, including law enforcement agents. But those who make these search engines are attempting to prevent *users'* search habits from being monitored.

Vendors and Buyers

A major part of the Dark Web political economy includes the sale of drugs, counterfeit goods, and stolen information, so it is not surprising that Dark Web search engines can become channels of commerce. The Tor-based Grams (now defunct) specialized in this area. Echoing previous Clear Web efforts to connect buyers and sellers (such as Google's Froogle), Grams offered Tor hidden service search specifically of markets. It also aggregated user-generated reviews of vendors from the markets as well as reviews on Reddit, offering a rating system not unlike Amazon's. Grams was not useful

for finding general Tor hidden services, but as the magazine *Deep Dot Web* proclaims, it became a hub for drug market sellers and buyers.[43] Vendors could build a stable reputation (tied to a pseudonym and a PGP key) across multiple markets by being included in the Grams database. Beyond this, Grams also offered Bitcoin tumbling services and an advertising network where markets and vendors could advertise their offerings.

Software and Protocols

Because Tor, I2P, and Freenet are anonymizing networks designed to obfuscate the IP addresses of both users and site hosts, search engine operators face technical challenges quite different from standard World Wide Web search. Dark Web search engine operators alter existing software packages, such as Yacy (a peer-to-peer search engine), Apache Lucene, or custom Perl or Python scripts, in order to crawl Tor hidden services, eepsites, or Freesites. Many of these web search packages were made for the World Wide Web, which is older, faster, has far more content and links, and has a centralized naming system (the domain name system, or DNS). Documentation for adjusting search engine software packages for Tor, I2P, or Freenet tends to be sparse or nonexistent. Nurmi, the founder of Ahmia, notes these problems in terms of searching Tor sites: "First, the linking between onion sites is thin; as a result, algorithms using the backlinks aren't working very well. Second, it takes time to crawl everything because Tor is slow. Lastly, onion sites are replacing their addresses all the time."[44] Search engine software, especially preexisting packages, must be heavily modified for these specific problems.

Even after doing so, however, Dark Web search engines must balance between crawling these networks enough to produce an up-to-date index while not overwhelming network bandwidth. Too little crawling of the network results in obsolete indexes; too much and bandwidth that would otherwise go to network users goes instead to the search engine software. This is especially tricky in Dark Web environments where hidden sites appear and disappear frequently.

As MoniTOR explains, to see if a site is available on the Tor network, a search engine could "ping" a server (essentially asking the server, "Are you available?"). Although "every ping is tiny, … if enough people use your service, it could potentially increase your bandwidth use dramatically."[45] Given that bandwidth on the Tor network is at a premium, pinging could slow down the search engine or even result in an inadvertent denial-of-service attack on another server. But, as MoniTOR explains, without pinging (or other methods to see if a server is online), new content could be hidden from the search engine: "As for server content, if a server[']s data changes, it may not be spidered for a period of time, or until it responds to the ping."[46]

Moreover, even with careful tuning, some website developers may not want part or even all of their sites indexed and may protest if their content ends up in a search index. On Tor and I2P networks, site owners can use a two-decades-old standard, the robots exclusion standard (commonly called robots.txt). By using a text file at the root of their servers, site administrators can declare whether and how they want their sites indexed by crawlers. But this standard was built for the World Wide Web, where user agent strings are commonly used. User agent strings identify the operating systems, applications, and IP addresses of visitors to a server. This works well for the World Wide Web, where a search engine can use a standard identification. Google's, for example, is "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)." In contrast, Dark Web systems obfuscate this information by default. The I2P system uses "MYOB/6.66 (AN/ON)" as a default (a series of jokes: mind your own business, the number of the beast, anonymous).[47] Search engine operators in I2P have to modify this default to provide unique identifying information; they also have to write guides for site administrators to properly configure robots.txt to work. In Freenet, the situation is worse: there is no support for robots.txt. In all of these systems, if a site administrator wants to be excluded from a search engine index, they are best off contacting

the search engine operators or hiding material behind password protections.

Finally, a special problem appears in the case of Freenet. Recall that one of the technical aspects of Freenet is the network's ability to "forget" unpopular content. If a file (HTML, PDF, MP3, JPG, or otherwise) is not accessed often enough, the network is designed to overwrite it. But this is predicated on the assumption that *humans* would be the arbiters of popularity. What about software processes? As David McNab notes in his description of his Freenet search engine, "The very act of spidering these pages will change their routing within Freenet—and will have a tendency to bring to life a lot of the more rarely-visited freesites."[48] In other words, as Freenet crawlers request freesites, they ensure that the network will not overwrite them, even if few humans actually want to visit them.

Even after all the work of tuning search engine software to operate in the unique protocological environments of Tor, I2P, or Freenet, the sheer resources required for search engines—and the purpose of Dark Web searchers—may drive search engine operators away. A key example of this is the highly successful, but now shuttered, Direct search on the I2P network. Direct search administrator I2Phreak explained why Direct was shut down:

> The router consumes too much system resources. The crawler is also written in Java and consumes the rest:) All the data we need to store (fetched pages, even compressed, search index, URLs database), in order to run the service, takes about 25 Gb of disk space. And about 90% of all search requests were about child pornography. There is no reason to spend so much resources to serve such kind of requests.[49]

Given that the searches were largely for content I2Phreak was morally opposed to, running Direct was not worth the high amounts of RAM and hard disk space required.

Thus, in addition to identifying actors (such as users, nonusers, law enforcement, vendors, buyers, and network builders) and mediating in various ways among them, Dark Web search engine

operators have to consider the problems and interests of the networks themselves: their specific protocols, topologies, and capacities. They must align the capacities of off-the-shelf search engine software with the specific Dark Web networks they seek to index. They also must consider the demands on their own equipment of search and networking. To become a legitimated point of passage and command respect and resources, Dark Web search must provide channels between software and network protocols. Finally, even after all this work, Dark Web search engine operators may consider hiding sites from their results, as the case of Direct implies.

Hiding and Simplifying

So far, I have shown how Dark Web search engine developers identify relevant actors and attempt to align these actors' interests, effectively becoming a channel between entities such as users, networks, law enforcement, and software. These developers seek to balance both senses of propriety, commanding respect (by aligning other actors' interests) and commanding resources (by channeling informational flows). But it is too simple to suggest that Dark Web search engines merely provide open channels between pairs of actors. They must also engage in *hiding* and *simplification*.

Hiding

Recall Barbenhauserheide's argument about Freenet search: "For [Freenet to be] *more* socially acceptable we need more actively spidering [indexes] which only include what the creator deems acceptable."[50] Only including "what the creator deems acceptable" is the key phrase here. A more complex description comes from George Kadianakis, who describes an ideal search engine for Tor hidden services:

> If I could automagically generate secure technologies on a whim, I would say that some kind of decentralized reputation-based fair search engine for hidden services might squarify our Zooko's triangle a bit. "decentralized" so that no entities have pure control over the results. "reputation-based" so that legit hidden services flow on top. "fair" so that no scammers with lots of boxes can game the system. Unfortunately, "fair" and "reputation-based" usually contradict each other.[51]

Here is a more complex set of design goals: a decentralized search system that would return only reputable sites and prevent scamming. Regardless of the differences in design goals, both

Babenhauserheide and Kadianakis are calling for search engines that filter results so that only an acceptable class of Dark Web sites are accessible. Another way to understand this: these developers are calling for searches that *hide* certain classes (disreputable, unacceptable) of Dark Web sites from view, thus delegitimating them.

In mainstream press coverage, all Dark Web sites are portrayed as inherently and equally hidden. In other words, popular press coverage tends to present Tor hidden services, eepsites, and freesites as equally hidden from technically inept web users. When they report on Dark Web search, they deploy the metaphor of "bringing light to the dark," implying that search engines (as well as directories) are seen as systems that can bring all hidden Dark Web sites into view. Actually, search engine operators often hide sites from their results by either deleting sites from their indexes or preventing them from being indexed. This is in addition to sites that use robots.txt or password protection to avoid being indexed at all. Thus, all Dark Web sites are not equally hidden or equally accessible. Those sites that are not visible through a Dark Web search are, in a sense, "deeper," or more hidden, a little Deep Web (in the original sense of this term) within the Dark Web, so to speak.[52]

Dark Web search engine operators do this by preventing classes of sites from being included in their indexes. For example, FreenetUser, the creator of the AFKindex, explains their "banned" criteria:

> First indexing/publishing any found freesite, i quickly got disgusted by child porn content, and added some filtering capabilities to AFKindex to completely ignore those freesites (no more crawling of those filtered keys).
>
> Unfortunately, lots of adult freesites provides links to indices or other freesites that points to child porn content after 1 or two "hops" ; this is why you shouldn't be able to find any porn here.[53]

In other words, to ban CEI, FreenetUser filtered out all pornography from AFKindex after finding that Freenet porn sites were strongly linked to CEI sites.

Enzo, a Freenet search engine operator, describes that index's selection criteria:

> My index allows you to browse Freenet without the need to worry about what links you are clicking on. I wouldn't say that I censor content, as it's still available on Freenet. It can still be reached from other index sites, which I do include in my index. I hide any freesite that contains child pornography, bestiality or hate speech.[54]

Nurmi took similar steps with Ahmia (the Tor and I2P search engine):

> If there is any images/videos where is naked children we will filter the site out. According to the law of Finland I am not obligated to filter out anything. However, I don't want to maintain public search for child porn.[55]

As should be clear, CEI sites are the single most filtered class of Dark Web sites. Through a range of practices, including using basic heuristics (i.e., pornography sites often link to child abuse image sites), soliciting reports from users, or building indexing algorithms that can distinguish between CEI and non-CEI sites, these search engine operators attempt to hide CEI sites from view, delegitimating them while legitimating the material that is returned by the engines.

I2P developer zzz refers to search engines that hide CEI (and other taboo material) as "curated."[56] Curation can involve the care of an archive (in this case, an index of hidden sites), but it also refers to the selection of artifacts from an archive for presentation. This museum metaphor is apt, since many museums keep the majority of their artifacts in archives out of public view and exhibit only a small proportion of them. Even if a Dark Web search engine "collects" all Dark Web sites in its index, the search engine operator

does not need to allow all of them to be accessible to the end user. In contrast, critics of such filtered or curated search refer to it as "censorship," suggesting that search engine operators are only showing classes of Dark Web sites they approve of. Regardless of the language, such filtered search engines do in fact hide sites from view, even as they make other hidden sites more accessible, visible, and legible to Dark Web users.

Simplifying

Although most Dark Web search engines seek to hide classes of sites—especially CEI sites—they must provide at least some degree of access to the legit (i.e., authentic) Dark Web. Otherwise, their basic relationship to the end user would break down: if a search engine does not return results that map onto the end user's perception of what the Dark Web contains, then that engine is not legit. Indeed, some of the search engine operators I've interviewed opted not to filter their search results. MoniTOR is one example:

> My personal feeling is that MoniTOR needs to stay neutral. … MoniTOR does indeed index CP [child pornography] sites and communities. It will also provide search results to those who look for it. Do I like it? No. However, my place [is not] to judge what a person thinks or feels. Further to this, MoniTOR does not cache any of the content, just the URLs; headers and subject lines/meta tags. This keeps MoniTOR legal, as it does not host any of the material it spiders.[57]

Here, MoniTOR promises access to simplified (i.e., URL, headers, and meta tag) overviews of all the Tor sites the Yacy-based search will index, regardless of the operator's judgment of the sites. Another search engine, I2P's Direct search, did as well. Note that both search engines are, as of this writing, offline.

Filtered or not, all the engines engage in *simplification*, or the reduction of complexity. Following the practices of mainstream search engines, the results from querying a Dark Web search engine tend to be composed of four technical elements:

- A site title
- A link to that site
- A small snippet of text from that site
- The time the site was last cached by the search engine

Although these elements provide a great deal of information about sites—title, content, and an indication of how "fresh" the content is—these are simplifications of the sites. They are not the sites themselves but rather metadata about the sites culled from the search engine's index. With this simplification, the engine can present Dark Web sites to users in small batches (about ten at a time). Moreover, the placement of the sites on the results page is based on the search engine's relevance algorithms. Finally, most—if not all—of the Dark Web search sites are in English; this of course "simplifies" things insofar as it presents web pages using non-English languages in an English metadata frame.

John Law's point about "ordering stories" applies to search engine simplification. Dark Web search engines tell ordering stories about Tor hidden services, I2P, or Freenet by privileging sites over others in their indexes, blocking others, and presenting a simplified interface to end users. The result of this is the introduction of the politics of search to the Dark Web: the engines promise access to the legit Dark Web, but this access is algorithmically curated. Rather than simply building a smooth and open channel, search engines introduce mediation that structures the connection between relevant actors, hiding some elements, simplifying others, and above all, laying claim to legitimacy as propriety.

Dealing with Resistance

Although Dark Web search engines attempt to hide and simplify other elements in the networks, as Michel Serres has convincingly argued, hidden or simplified elements will assert themselves, irrupting into view.[58] These elements challenge the legitimacy of search engines.

For example, a key set of actors on the Tor network are *cloners*. Tor hidden services use URLs that are 16 alphanumeric characters, followed by the pseudo-top-level domain .onion, as in Ahmia's URL on the Tor network: msydqstlz2kzerdg.onion/. Clearly, these URLs are not easily memorized by humans. A major problem on the Tor network are phishing sites that act as proxies, thus performing "man-in-the-middle" attacks. As of this writing, there are at least four clones of Ahmia:

- http://msydqjihosw2fsu3.onion/
- http://msydqci2rln5jq6v.onion
- http://msydq5ywzjnjvsdf.onion
- http://msydqgnbch2gsw3j.onion

Cloned Tor hidden services are a security risk: if a user visits a cloned site and enters a password or Bitcoin information, that information will be stolen by the cloner. Because of the non-human-readable onion URLs, accidentally going to a cloned site is very easy to do.

Tor hidden service search engines struggle with this challenge, because these cloners undermine the ordering stories their search results tell. The end user can't tell the legit site from the clone. As MoniTOR explained to me,

> Some enterprising people/sites/engines have come up with the idea of putting or omitting certain information in site headers to indicate it is the legitimate page. The main problem is that anyone can edit their headers to match. So while this may work temporarily, it's not an ideal solution.[59]

Another Tor-based search engine, not Evil, uses machine learning to label the real Tor hidden sites "official sites." This is meant as a means for searchers to distinguish between authentic and cloned onion sites. Nonetheless, cloned sites continue to be a major problem on the Tor network.[60]

Finally, even with search engine operators hiding CEI sites from their indexes, search engine users report disturbing finds, as one frustrated I2P user lamented on the now-defunct I2P forum:

> Then you browse search engine results, sieve through 80 pages flooded with a hundred variations of "11 yo *beep* pedo girls," just mindlessly mirrored content from the clearnet, dead sites, improperly configured sites, all kinds of illegal *beep*, sites in Russian or Polish and other foreign languages … to find maybe one link that is just "facts about cats" or something. … In 20 minutes, you eyeballed 800 pages of mostly disgusting *beep*, i.e. sex with children, only to spent 2 minutes on a site about cat facts, that you didn't even search for in the first place. … Again, you begin asking yourself, if there is anything relevant to be found in I2P at all. And if you shouldn't just stop looking for it.

Thus, even if search engine operators attempt to hide classes of sites—especially CEI sites—those sites find their way into search engine indexes, as this I2P user describes. Although Dark Web search engines seek to hide and simplify the topologies of anonymity, would-be hidden elements emerge: cloners and CEI purveyors work to defeat algorithms and filters, exploiting the new channel that Dark Web search engines introduce.

Conclusion: Inheriting from Google

Histories of the web often present search engines as key technologies of accessibility; engines such as Google have moved from being seen as bandwidth hogs that steal intellectual property to legitimated billion-dollar companies traded on stock markets.[61] As René König and Miriam Rasch argue, mainstream search engines such as Google and Bing have become infrastructural: "Just as we expect water running from the tap, electricity coming from the plug, and roads to drive on, we take for granted that there are search engines to give us the information we need."[62] Google especially has become part of our "collective 'techno-unconsciousness,'" invisibly structuring much of our daily lives, at least insofar as our lives are mediated by the Internet.[63] Moreover, our hindsight gives us a safe vantage point to make the argument that Google is legitimate: it commands respect. For example, when someone with the title Google engineer makes a social proclamation, it is widely reported on.[64] And Google also commands resources: billions of dollars and a global network of technologies from databases to operating systems to self-driving cars. Overall, Google's propriety is not often questioned.[65]

What this chapter on Dark Web search reminds us, however, is that search engine legitimacy is never guaranteed. Any potential source of legitimacy should be exploited. In addition to mediating all the relationships described above, and in addition to hiding and simplifying, Dark Web search engines repeatedly lay claim to an inheritance: the legitimacy of previous search engines, especially Google.

This is immediately apparent when we consider claims to becoming the "Google of the Dark Web." Chris McNaughton made this explicit for his search engine TorSearch.[66] Nurmi also explicitly likened Ahmia to Google. Similarly, multiple search engines use

visual and textual signals to stake their claim as inheritors of Google's legitimacy. Freegle, a short-lived Freenet search, echoed Google in its name, as does I2P's elgoog ("Google" spelled backward). The search engine not Evil playfully cites Google's "Don't be evil" motto and for several years used a primary color–based logo that echoed Google's. I2P search engine Seeker and Tor engine the Beast also emulate Google's stripped-down design (white background, textbox in the center of the screen). Tor's Candle does the same, but with a black background. Grams also borrowed some of Google's aesthetics, including the primary color logo on a white field, the "I'm feeling lucky" button, and the empire-building aspects of Google (including advertising networks and shopping services). Finally, Onion.link uses Google Custom Search to index Tor sites via the Tor2Web proxy.

Much as Google has done with multiple browsers and now the Android operating system, Dark Web search engines seek a prime position in relation to their respective networks: they seek to be on the networks' home pages. Some have been successful in achieving this position. Enzo's Search is included in Freenet's default settings, signaling that the Freenet Project believes that Enzo's Search is an appropriate window into the network. Others have not. I2P sought to do something similar; for a brief period, Eepsites.i2p and Epsilon were considered for the I2P Router Console page, the first page an I2P user sees.[67] But as I2P developer zzz recalls,

> We had a search box on I2P. We added it, and then immediately hid it, because we couldn't find any search site existing now that could really hide all the worst of the worst. You know, you want to give people a good impression of I2P, and it is almost all clean and wonderful, helpful stuff, so we want to put that in front of people. And if we can't find a search engine that can competently filter out the ugly stuff, we're not going to enable that.[68]

In other words, the I2P developers were willing to include a default search engine if that search engine hid "the ugly stuff" (presumably

CEI); if an engine is able to do so, it can enter into a legitimacy exchange with the I2P developers, gaining an "official" designation from the network builders and in turn providing users with a passage point into I2P. Selecting search engines as defaults provides the network builders with a tool that users often call for, and it consecrates those search engines as official.

The struggle to be the "Google of the Dark Web" is not settled, but it is telling that Dark Web search engine operators continue to make a claim to inheriting Google's legitimacy. Success would bring respect and resources. It would be a means for new Dark Web users to enter the networks and find content. It would also mean that a legit Dark Web site builder found a way to provide such a portal into these networks.

And failure might have worse consequences than shutting down and giving up: it could lead to an external search behemoth coming to the Dark Web. As Virgil Griffith, developer of Onion.link, argues,

> Respectfully, we lost [the war for Internet freedom]. However, a substantial fraction of the Tor community feels they can still win if they encircle the wagons tightly enough. And they see things like mainstream search engines as a finger by which mainstream attention and regulation will come to impact them more.[69]

In other words—setting aside the question of the war for Internet freedom—if a Dark Web user cannot build a "Google for the Dark Web," the fear is that some external entity (Google? DARPA?) will do it instead, thus bringing corporate or state surveillance to these obscure corners of the Internet. To head off such an invasion, those who build Dark Web search engines are attempting to port mainstream search engine practices and software into the unique protocols of Tor, I2P, and Freenet. These practices include indexing, simplification, silencing, hierarchization, and gatekeeping. König and Rasch's observation holds just as much for Dark Web search engines as it does for Google, Bing, and Baidu:

> Search engines function as gatekeepers, channeling information by exclusion and inclusion as well as hierarchization. Their algorithms determine what part of the web we get to see and their omnipresence fundamentally shapes our thinking and access to the world. Whatever their bias may look like, it is obvious that man-made decisions are inscribed into the algorithms, leading unavoidably to favoring certain types of information while discriminating against others.[70]

Such techniques are necessary for building a legitimate, respectable, proper Dark Web search engine. No search engine can avoid creating hierarchies, gatekeeping, or shaping our interactions with a network; in fact, to be legitimate in the sense I am exploring here, *they must do these things*. Calls for a "Google of the Dark Web," for a curated index of links and a web application with which to query it, is a call to make the Dark Web a bit more like the Clear Web, including replicating a de facto monopoly on a means for users to find content. By commanding respect and resources, such a search engine could even make the Dark Web itself legitimate.

Notes

1. In fact, one Tor-based social networking site admin reported in early 2014 that Google was indexing the site. These searches came through Clear Web to Dark Web proxies, such as Tor2Web, which had been active since 2008.

2. Michael Zimmer, "Web Search Studies: Multidisciplinary Perspectives on Web Search Engines," in *International Handbook of Internet Research*, ed. Jeremy Hunsinger, Lisbeth Klastrup, and Matthew Allen (Berlin: Springer, 2009), 507–521, http://link.springer.com/chapter/10.1007/978-1-4020-9789-8_31.

3. Mark C. Suchman, "Managing Legitimacy: Strategic and Institutional Approaches," *Academy of Management Review* 20, no. 3 (1995): 574.

4. Myria Watkins Allen and Rachel H. Caillouet, "Legitimation Endeavors: Impression Management Strategies Used by an Organization in Crisis," *Communications Monographs* 61, no. 1 (1994): 45.

5. Monica A. Zimmerman and Gerald J. Zeitz, "Beyond Survival: Achieving New Venture Growth by Building Legitimacy," *Academy of Management Review* 27, no. 3 (2002): 416. Original emphasis.

6. Ibid., 417.

7. Maribeth S. Metzler, "Responding to the Legitimacy Problems of Big Tobacco: An Analysis of the 'People of Philip Morris' Image Advertising Campaign," *Communication Quarterly* 49, no. 4 (September 1, 2001): 366–381, doi:10.1080/01463370109385636; Stephanie Decker, "Corporate Legitimacy and Advertising: British

Companies and the Rhetoric of Development in West Africa, 1950–1970," *Business History Review* 81, no. 1 (April 2007): 59–86, doi:10.1017/S0007680500036254.

8. R. T. Naylor, "Violence and Illegal Economic Activity: A Deconstruction," *Crime, Law and Social Change* 52, no. 3 (September 1, 2009): 232, doi:10.1007/s10611-009-9198-9.

9. Kwangho Jung and M. Jae Moon, "The Double-Edged Sword of Public-Resource Dependence: The Impact of Public Resources on Autonomy and Legitimacy in Korean Cultural Nonprofit Organizations," *Policy Studies Journal* 35, no. 2 (May 1, 2007): 205–226, doi:10.1111/j.1541-0072.2007.00216.x.

10. Scholars who focus on established organizations tend to treat them as legitimate because they are successful. In contrast, scholars such as Zimmerman and Zeitz and Lounsbury and Glynn, who focus on start-ups, tend to see legitimacy as a "cheap" resource a start-up can gather and then use to gain material resources such as investments. See Zimmerman and Zeitz, "Beyond Survival"; Michael Lounsbury and Mary Ann Glynn, "Cultural Entrepreneurship: Stories, Legitimacy, and the Acquisition of Resources," *Strategic Management Journal* 22, no. 6–7 (June 1, 2001): 545–564, doi:10.1002/smj.188.

11. Zimmerman and Zeitz, "Beyond Survival," 416.

12. Barbara Czarniawska and Tor Hernes, "Constructing Macro Actors According to ANT," in *Actor-Network Theory and Organizing*, ed. Barbara Czarniawska and Tor Hernes (Copenhagen: Copenhagen Business School Press, 2005), 10.

13. Michel Callon, "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay," in *Power, Action, and Belief: A New Sociology of Knowledge?*, ed. John Law (Boston: Routledge and Kegan Paul, 1986), 169–233.

14. John Law, “On Power and Its Tactics: A View from the Sociology of Science,” *Sociological Review* 34, no. 1 (1986): 6.

15. Susan Leigh Star, “The Ethnography of Infrastructure,” *American Behavioral Scientist* 43, no. 3 (1999): 380.

16. Ibid., 379.

17. John Law, *Aircraft Stories: Decentering the Object in Technoscience* (Durham, NC: Duke University Press, 2002); Annemarie Mol, “Cutting Surgeons, Walking Patients: Some Complexities Involved in Comparing,” in *Complexities: Social Studies of Knowledge Practices*, ed. John Law and Annemarie Mol (Durham NC: Duke University Press, 2002), 218–257; Gail T. Fairhurst and François Cooren, “Leadership as the Hybrid Production of Presence (S),” *Leadership* 5, no. 4 (2009): 469–490.

18. Fairhurst and Cooren, “Leadership as the Hybrid Production of Presence.”

19. John Law, *Organizing Modernity* (Cambridge, MA: Blackwell, 1994), 132.

20. John Law, “On Hidden Heterogeneities: Complexity, Formalism, and Aircraft Design,” in *Complexities: Social Studies of Knowledge Practices*, ed. John Law and Annemarie Mol (Durham NC: Duke University Press, 2002), 120.

21. Michel Serres, *The Parasite* (Baltimore: Johns Hopkins University Press, 1982).

22. For a relatively early study of a large search engine log, see Craig Silverstein et al., “Analysis of a Very Large Web Search Engine Query Log,” *SIGIR Forum* 33, no. 1 (September 1999): 6–12, doi:10.1145/331403.331405.

23. Daniel E. Rose and Danny Levinson, “Understanding User Goals in Web Search,” in *Proceedings of the 13th International*

Conference on World Wide Web (New York: ACM, 2004), 15, doi:10.1145/988672.988675.

24. Matthew Toseland, "[Freenet-dev] Searching support in 0.7.0?," Freenet-dev mailing list archives, November 14, 2005, https://web.archive.org/web/20141117104945/https://emu.freenetproject.org/pipermail/devl/2005-November/000086.html.

25. Not Evil Admin, interview by author, July 21, 2015.

26. MoniTOR, interview by author, November 26, 2015.

27. Nurmi, Juha, interview by author, August 3, 2015.

28. Enzo, interview by author, December 14, 2015.

29. Zzz, "Proposal: Simplified Console Home Page," Zzz.I2P forum, January 19, 2012, http://zzz.i2p/topics/1079 [I2P].

30. Toseland, "[Freenet-dev] Searching support in 0.7.0?"

31. Wendy Hui-Kyong Chun, *Control and Freedom: Power and Paranoia in the Age of Fiber Optics* (Cambridge, MA: MIT Press, 2006), 16.

32. Arne Babenhauserheide, "[Freenet-dev] Security Quibbles Was Re: Freenet Canary," Freenet-dev mailing list archives, November 30, 2015, https://emu.freenetproject.org/pipermail/devl/2015-November/038645.html.

33. Nurmi is countering an argument put forward by Dark Web researcher Clement Guitton that the vast majority of Tor hidden services are "unethical" and therefore the Tor Project should discontinue developing and supporting hidden services. See Clement Guitton, "A Review of the Available Content on Tor Hidden Services: The Case against Further Development," *Computers in Human Behavior* 29, no. 6 (November 2013): 2805–2815, doi:10.1016/j.chb.2013.07.031. For Jeremy Malcolm's framing, see Gabey Goh, "Unpeeling the Dark Web

with OnionCity," *Digital News Asia*, March 24, 2015, https://www.digitalnewsasia.com/digital-economy/unpeeling-the-dark-web-with-onioncity.

34. Juha Nurmi, "Tor Hidden Service (.onion) Search: Ahmia.Fi," Ahmia.fi, accessed May 21, 2016, https://ahmia.fi/static/presentation/Tor_Ecosystem2.pdf. In contrast, researchers such as Clement Guitton, Daniel Moore, and Thomas Rid have argued that the content of Tor hidden services is mostly illegal; see Guitton, "A Review of the Available Content"; Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no. 1 (January 2, 2016): 7–38, doi:10.1080/00396338.2016.1142085. All of these authors support their claims by using Web crawlers and indexers.

35. Juha Nurmi, "Ahmia.Fi—Search Engine for Anonymous Hidden Services," Knight Foundation News Challenge, March 18, 2014, https://www.newschallenge.org/challenge/2014/submissions/ahmia-fi-search-engine-for-anonymous-hidden-services.

36. Nurmi, interview by author, August 3, 2015.

37. Quoted in Goh, "Unpeeling the Dark Web."

38. James Martin and Nicolas Christin, "Ethics in Cryptomarket Research," *International Journal of Drug Policy* 35 (September 2016): 85, doi:10.1016/j.drugpo.2016.05.006.

39. For example, the following works note that, thanks to the relative ease with which records of sales could be gathered on Dark Web markets, tracing the scale of illegal trades is becoming easier: Amy Phelps and Allan Watt, "I Shop Online—Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia," *Digital Investigation* 11, no. 4 (2014): 261–272, doi:10.1016/j.diin.2014.08.001; Joe Van Buskirk et al., "Who Sells What? Country Specific Differences in Substance Availability on the Agora Cryptomarket," *International Journal of Drug Policy* 35 (September 2016): 16–23, doi:10.1016/j.drugpo.2016.07.004;

David Décary-Hétu, Masarah Paquet-Clouston, and Judith Aldridge, "Going International? Risk Taking by Cryptomarket Drug Vendors," *International Journal of Drug Policy* 35 (September 2016): 69–76, doi:10.1016/j.drugpo.2016.06.003; Monica J. Barratt and Judith Aldridge, "Everything You Always Wanted to Know about Drug Cryptomarkets* (*But Were Afraid to Ask)," *International Journal of Drug Policy* 35 (September 2016): 1–6, doi:10.1016/j.drugpo.2016.07.005; Judith Aldridge and David Décary-Hétu, "Hidden Wholesale: The Drug Diffusing Capacity of Online Drug Cryptomarkets," *International Journal of Drug Policy* 35 (September 2016): 7–15, doi:10.1016/j.drugpo.2016.04.020; Diana S. Dolliver, "Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel," *International Journal of Drug Policy* 26, no. 11 (November 2015): 1113–1123, doi:10.1016/j.drugpo.2015.01.008.

40. Vannevar Bush, "As We May Think," *Atlantic Monthly*, July 1945; Kim Zetter, "DARPA Is Developing a Search Engine for the Dark Web," *Wired*, February 10, 2015, https://www.wired.com/2015/02/darpa-memex-dark-web/.

41. Wade Shen, "Memex," Defense Advanced Research Projects Agency, 2014, http://www.darpa.mil/program/memex.

42. Ahmia legal disclaimer, 2016, https://www.ahmia.fi/legal/.

43. DeepDotWeb, "Grams: Becoming Hub for DarkNet Info & Ads (Part 1)," *Deep Dot Web*, May 31, 2014, https://www.deepdotweb.com/2014/05/31/introducing-grams-infodesk-features-part-1/.

44. Nurmi, interview by author, August 3, 2015.

45. MoniTOR, interview by author, November 26, 2015.

46. Ibid.

47. See "I2PTunnel," I2P: The Invisible Internet Project, January 2016, https://geti2p.net/en/docs/api/i2ptunnel.

48. David McNab, "[Freenet-chat] New Freenet Search Engine," Freenet-chat mailing list archives, February 23, 2003, https://emu.freenetproject.org/pipermail/chat/2003-February/000631.html.

49. I2Phreak, "Direct.i2p—New Search Engine," Forum.i2p, April 11, 2016, forum.i2p/viewtopic.php?t=10685 [I2P].

50. Babenhauserheide, "[Freenet-dev] Security Quibbles."

51. George Kadianakis, "[Tor-dev] Memorable onion addresses (was Discussion on the crypto migration plan of the identity keys of Hidden Services)," Tor-dev mailing list archives, May 19, 2013, https://lists.torproject.org/pipermail/tor-dev/2013-May/004884.html.

52. Michael K. Bergman, "The Deep Web: Surfacing Hidden Value," *Journal of Electronic Publishing* 7, no. 1 (2001), http://quod.lib.umich.edu/cgi/t/text/idx/j/jep/3336451.0007.104/--white-paper-the-deep-web-surfacing-hidden-value?rgn=main;view=fulltext.

53. FreenetUser, "About AFKindex," March 2008, http://127.0.0.1:8888/USK@2L-k2U32b3yIl2~YjBU7--QJPTtixSwJHZxYOuGjS3Ao,QJBd6zpJgEsijJGQNNcwUhsrW5vJ8VtlmNX5ka2~d [Freenet].

54. Enzo, interview by author, December 14, 2015.

55. Nurmi, interview by author, August 3, 2015. Also see Juha Nurmi, "Ahmia Search after GSoC Development," *Tor Blog*, September 14, 2014, https://blog.torproject.org/blog/ahmia-search-after-gsoc-development.

56. Zzz, "State of I2P Search Engines," Zzz.I2P forum, January 22, 2012, http://zzz.i2p/topics/1083-state-of-i2p-search-engines [I2P].

57. MoniTOR, interview by author, November 26, 2015.

58. Serres, *The Parasite*; also see Steven D. Brown, "Michel Serres: Science, Translation and the Logic of the Parasite," *Theory, Culture and Society* 19, no. 3 (2002), doi:10.1177/026327602401081503.

59. MoniTOR, interview by author, November 26, 2015.

60. Mark Stockley, "Hundreds of Dark Web Sites Cloned and 'Booby Trapped,'" *Naked Security*, July 1, 2015, https://nakedsecurity.sophos.com/2015/07/01/hundreds-of-dark-web-sites-cloned-and-booby-trapped/.

61. John Battelle, *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture* (New York: Portfolio, 2005).

62. René König and Miriam Rasch, "Reflect and Act!: Introduction to the Society of the Query Reader," in *Society of the Query Reader: Reflections on Web Search*, ed. René König and Miriam Rasch (Amsterdam: Institute of Network Cultures, 2014), 10.

63. Ibid.

64. When Google engineer Chade-Meng Tan presented a workshop on being happy at SXSW, the room was packed, and summaries of the talk were picked up by the BBC, CNN, and LifeHacker. Of course, he has also given a TED Talk.

65. Siva Vaidhyanathan, *The Googlization of Everything: (And Why We Should Worry)* (Berkeley: University of California Press, 2012).

66. Andrew Couts, "TorSearch Makes Finding the Next Silk Road a Lot Easier," *Digital Trends*, October 11, 2013, http://www.digitaltrends.com/web/torsearch-tor-network-hidden-services/.

67. Zzz, "State of I2P Search Engines." As of this writing, no search engines are presented as defaults on I2P's home page. The reason

given by zzz is that none of them do proper filtering—specifically the filtering of CEI. "I2PCon Day 1: Growing the Network, Spreading the Word (August 15, 2015)," presented by zzz, YouTube video, 57:40, posted by KYTV at I2P, August 27, 2015, https://www.youtube.com/watch?v=2KbqgR3avqw. Even if search engine operators seek to filter it, CEI seems to bubble up into results.

68. "I2PCon Day 1."

69. Virgil Griffith, interview by author, May 30, 2016. In fact, Griffith's Onion.link is arguably bringing "mainstream search engines" to the Dark Web, because it uses Google Custom Search to crawl .onion sites. Griffith's comment here is in response to a question about criticism of this practice.

70. René König and Miriam Rasch, eds., *Society of the Query Reader: Reflections on Web Search* (Amsterdam: Institute of Network Cultures, 2014), 13.

6 Being Legit on a Dark Web Social Network

There is a very rare genre of Dark Web writing, a form of writing that might appear for a few days and then be deleted, never to be seen again. It's a genre we might call the "Fuck you, I'm Shutting This Down" message. As I mention throughout this book, many Dark Web sites are ephemeral, coming and going in a matter of months. Often, they disappear for no apparent reason. They just disappear off the networks, and because they were created and run by anonymous people, there's little chance of following up with their former administrators to ask why these sites are gone.

But on occasion, the administrators of sites provide a message to their users explaining why they're shutting their sites down. On two occasions, the admins of Tor-based social networking sites did just that. Around August 2015, MultiVerse Social Network was closed down, with this message:

> This used to be the home of MultiVerse Social Network. Thanks to all of our serious users that participated in making MultiVerse a functional site. Unfortunately, all things eventually come to an end, including this site. When we launched MultiVerse around 1 year ago, it was our staff's intention to create an alternative social network to those found on the public internet. While our intents were genuine and the site was built and maintained according to our intent, we continually were faced with a very aggravating problem caused by users who are unable to appreciate the work that goes into making and maintaining a site like this one once was. Normally, when a site closes, they do so quietly. But we are not so inclined. (1.) The greater majority of the member-signups were from users that abandoned their account within an hour of creating it. Apparently they didn't get that they were getting in on the ground-floor of a new social network, and expected everything and everyone to be there to entertain them. (2.) The pedophiles, other perverts, and the LEAs [law enforcement agents] that pursue them … this group may have been the most troublesome. While the pedos were a pain, they were usually easily dealt with and would go away when banned for creating a nickname that included the word 'pedo' (when we made it quite obvious in our site-rules that this wouldn't be tolerated). The other perverts were a little more annoying, but they also seemed to know when to piss off. The LEAs that made accounts here and tried to bait some of our users … those people were the last straw. Rather than fight them, which is a losing battle anyway, there will be no more site here for them to use for that shit. We told you to fuck off, and you didn't listen. Well, now what? The site's no longer here, so fuck off![1]

In March 2016, the admin of Dark Matters, another social networking site, posted something similar:

> Apparently, we're not criminal enough to be welcome out here. Apparently, we since [*sic*] don't allow Child Porn, marketing, harassment of our users, and don't allow for appeals by those who have been banned for breaking the site's rules, apparently we must have our priorities fucked up.
>
> Tor *has been* taken over by criminals for the most part, and apparently many of them were stupid enough to believe that this site was made for them, when it absolutely wasn't, and I thought that the rules that were posted on *every single page of the site* made that clear.
>
> So, as of 10:30am today, I'm closing this site and leaving the darknet, and I'll be encouraging my friends to do the same.
>
> For those who got themselves banned here and complained about it elsewhere, trying to gain sympathy for your own fuckups, here's a big "FUCK YOU ASSHOLES" to all of them. I hope the feds shoot them in the fucking head, and I'll gladly help them do so.
>
> This page will remain online for a few days, and then the server will be wiped.[2]

These messages are no longer online, and of course, neither are their respective social networking sites.

I quote these messages in full because they encapsulate both the hopes and the frustrations of Dark Web social networking site developers. In my time on Freenet, I2P, and Tor, I've seen over a dozen different social networking sites come and go.[3] Many start optimistically: we're going to provide a chance for people to use pseudonyms, meet each other, have conversations that are only possible when we enjoy the freedom of speech associated with anonymity. We're going to be an alternative to corporate social media found on the Clear Web, especially Facebook and Twitter. We're going to show everyone that the Dark Web isn't just a network for terrorists, drug dealers, and child exploiters.

And many end bitterly, as the two "fuck you" messages show.

These two "fuck you" messages also reveal something else: a concern with cultivating a particular user base. Note the common

laments of both: MultiVerse and Dark Matters were overrun with "child pornographers," law enforcement agents, perverts, marketers, and harassers. These aren't the "serious users" the MultiVerse admin hoped for. In an interview, the MultiVerse admin told me the biggest challenge the site faced was getting "legit users" in and keeping illegitimate ones (particularly "n00bs" and law enforcement agents) out.[4] Note that, as expressed in the MultiVerse message, most users simply don't understand the amount of work it takes to build a Dark Web social networking site, nor do they realize the opportunity it affords them—they aren't "serious users." The Dark Matters message argues that criminals shouldn't expect every Dark Web site to serve their needs. Judging from these messages, these admins wanted something else from their users altogether.

This chapter is meant to illuminate what that something else might be. In other words, what sort of users belong on Dark Web social networks? How do Dark Web social network administrators and users attempt to build community norms and practices? And how are these norms enforced? What happens when users violate social norms?

In other words: Who's a legit Dark Web social networking member? Who's bullshit? And how do we tell the difference?

Hence, this chapter is focused on the legitimacy I have been calling "legit," or legitimacy as authenticity, a term that gets used on many Dark Web sites to delineate real from fake, authentic from inauthentic, belonging from not. In fact, of all three legitimacies described in this book, the legit is perhaps the most common meaning used in Dark Web interactions. To illustrate how users are judged to be legit in Dark Web social networking sites, I focus on one particular social network, Galaxy2. The two "fuck you" messages notwithstanding, there are in fact successful Dark Web social networking sites, sites that have been online for several years (which is a long time in relation to other sites), such as Visibility on the I2P network and the distributed microblog Sone on Freenet. The focus of this chapter, Galaxy2, is another enduring site, which

appeared on the Tor network in early 2014 and is still online as of this writing.

Although this chapter focuses on the third type of legitimacy, legit, or legitimacy as authenticity, the other two legitimacies, violence and propriety, are clearly in play here: consider the MultiVerse admin's lament that his site was infiltrated by LEAs (law enforcement agents).[5] For the admin, LEAs making accounts on his site and attempting to bait users interested in child exploitation images represented an unwanted intrusion of state power onto the MultiVerse social network. Consider also that, much like Dark Web search engines, social networking sites must develop command of respect and resources, particularly respect of rules and command of flows of social information. Indeed, although Dark Web social networks can be hard to find, and although they come and go, they also tend to have thousands of users—sometimes tens of thousands—who sign up within short time spans.[6] This may not sound like much in comparison to the billions of people using corporate social networking sites such as Facebook, but Dark Web social networking sites tend to be some of the most active sites on the Dark Web. As such, organizational legitimacy—propriety, or the perception that a site is properly commanding resources—is a key legitimacy here as well.

But a focused exploration of authenticity, the legit, will be incredibly fruitful. Thus, the next move for this chapter is to further elaborate on the meaning of "legit" and how the legit is tied to other slippery terms, such as authority, power, and authenticity. Then, to illustrate the legit, I focus on Galaxy2. Specifically, I focus on Galaxy2's written rules, demonstrations of command of computer technologies, unwritten rule against "self-doxing," and members' skills with pseudonymous social networking. I suggest that, by adhering to the rules (written and unwritten) and demonstrating technical knowledge and skill in social networking on an anonymous network, Galaxy2 members can be accepted as authentic. Those who break the rules, on the other hand, are banned, a form of social exclusion that can be quite controversial.

But I trouble this somewhat by focusing on another form of authenticity: the authentication that some members are asked to engage in if they self-identify as young and female. All of these practices will illustrate how one Dark Web social networking site successfully cultivates a sometimes contradictory but thriving culture of legit users.

The Legit: Legitimacy as Authenticity

As I argue in chapter 2, all three legitimacies (violence, propriety, and authenticity) include power practices. This is the single most important connective tissue across them. Specific power practices inform each legitimacy, and these power practices also act as motors that drive the symbolic economic activities that help produce legitimacy (inheritance, exchange, purchase, appropriation, and delegitimation) because these activities help reinforce power relations.

State power practices are painfully obvious: break the law and be imprisoned (as Ross Ulbricht and Alexandre Cazes found out). Engage in war and be bombed. Organizational power practices are obvious as well: most employment in organizations is marked by hierarchies. The historical and global arc of capital/labor relations is bending toward "at will" employment and even to "free agent" precarity, so the threat of firing or simply not getting a contract is always in play. In transnational capitalism, the right and proper distributors of wealth and resources are corporations; run afoul of, say, credit standards and face the consequences of being shut out of access to low-interest loans.

Chapter 2 shows that "the legit" is also marked by power practices, ones that are different from being bombed or losing a job: *inclusion* and *exclusion*, belonging or not belonging, being recognized or not, accepted or not. Although these differ from state or organizational power practices, they are nonetheless very consequential. After all, being socially excluded can bring pain and despair; they might be different from those associated with prison or being unemployed, but the pain and despair are real enough. Given these consequences, users have a stake in understanding not only what it means to be legit, but also who as the authority to define and enforce this authenticity.

Authenticity

My window into the power practices employed on social networks is through the concept of authenticity. Unfortunately, "authenticity" (like "legitimacy" or "Dark Web") is a term that is often used by scholars but rarely defined.[7] I define authenticity as

> a socially constructed, context-contingent perception that an entity belongs to a larger field of entities, and its belonging indicates that it is a true example of the field. This perception of belonging is produced in two ways: first, by identifying those entities that are not authentic and do not belong to the field; thus, we come to know the authentic by contrasting it with the inauthentic. Second, it is produced through proclamations of actors who themselves have been accepted as members of the field and who are perceived to have the legitimate authority to judge what belongs and what does not.

Key words that come along for the ride in scholarship on authenticity include *real, true, authorized, belonging, natural, original, genuine, qualified,* or *pure*. Each, of course, brings along shadows: *fake, false, unsanctioned, outside, artificial, simulated, counterfeit, unqualified,* or *polluted*.

I derive this definition after carefully considering scholarship on authenticity. This scholarship takes on wide range of objects. I hate to reduce them to a list and thus reduce the scholarship to mere citations, but I do so to indicate the breadth of objects:

- consumption practices[8]
- academic fields[9]
- leisure activities[10]
- popular music[11]
- comedic styles[12]
- film genres[13]

- social identities (e.g., racial, indigenous, ethnic, religious)[14]
- ways of speaking[15]
- homeless shelters[16]
- online identities.[17]

The scholars writing about these objects take up a wide range of indicators of authenticity, including aesthetics, symbols, rhetorics, performances, psychological states of mind, and the evaluations of critics. Often, multiple indicators must be associated in a proper mix for something to be found "authentic."

The core anxiety of these works centers on processes of deciding what is in, what is out, what's for real, and what's bullshit.[18] This decision often depends on the context and the participants: one person's authentic object is another person's worthless junk; one person's real punk band is another's corporate rock band; one person's authentic Mexican cuisine is another person's bland chain-restaurant meal. Needless to say, no matter the object of study, scholars agree that authenticity is extremely contested. While we might conclude from this that chasing authenticity is a fool's errand, I argue instead that discourses of authenticity do matter in the world, that they have effects, and above all that they indicate the importance of this sort of social and cultural sorting.[19] As Sarah Banet-Weiser argues, "The concept of authenticity remains central to how individuals organize their everyday activities and craft their very selves."[20] Deciding whether a practice, person, or object is authentic matters a great deal to those who are involved in this adjudication as a form of personal expression, and there's much at stake: social acceptance, self-respect, access to resources, and social power. As Kate Bowan notes, authenticity "has long been a battleground on which passions have raged and boiled."[21] The power practices of authenticity are just as important as those of violence and propriety, and this is not to mention the ways in which authenticity can be trafficked into other forms of legitimacy (and hence, practices of violence or propriety).[22]

I would also suggest that the central anxiety—of figuring out what's for real and what's not—is not just an anxiety of making that distinction, but the anxiety over *who* gets to make those distinctions. As Theo Van Leeuwen argues, the approach should be not to ask "'How authentic *is* this?'," but 'Who takes this as authentic and who does not?', and 'On the basis of which visible or audible cues are these judgments made?'"[23] To these questions I would add: Who has the power to decide what's authentic or not? This is where authenticity becomes associated with legitimacy.

Legit Authority

For Pierre Bourdieu, in restricted fields of production, those subjects who can invoke, produce, judge, or police the borders of authenticity are legitimate authorities. These are, to use Bourdieu's term, "consecrators." What is at stake in any field that adjudicates authenticity, Bourdieu argues, "is the monopoly of the power to consecrate producer or products."[24] This is a form of legitimacy, one that echoes—but does not completely map onto—the other forms of power I trace throughout this book: the monopolized, accepted, respected, *legitimated* power over life and death at the level of the state, or the monopolized, accepted, respected, *legitimated* power over resources at the level of organizations. Similarly, for Bourdieu, the ability to consecrate is the monopolized, accepted, respected, legitimated power over what belongs in a field of production and what does not, what is valuable and what is not, or who belongs in a field and who does not.

This power hinges on the ability to discern authenticity, and the consecrators become legitimate authorities on the authentic. They can do so by demonstrating command of a restricted set of symbolic and cultural symbols and competencies that arise out of the search for authenticity. In other words, artists, hackers, critics, and academics all can become legitimated vis-à-vis the authentic: by making authentic things, living authentic lives, or distinguishing the authentic from the inauthentic. Think of how, for example, being a hip-hop artist hinges largely on ways of acting, dressing, and

speaking. If one is judged to command those practices, one may become a legitimate authority on who else is a "real" hip-hop artist.

So the authentic is determined in part by the legitimate authorities on the authentic, the consecrators. But how does one become a consecrator? If we expand the previous quotation from Bourdieu (who is using the example of literature), we can see:

> In short, the fundamental stake in literary struggles is the monopoly of literary legitimacy, i.e., *inter alia*, the monopoly of the power to say with authority who are authorized to call themselves writers; or, to put it another way, it is the monopoly of the power to consecrate producer or products (we are dealing with a world of belief and the consecrated writer is the one who has the power to consecrate and to win assent when he or she consecrates an author or a work—with a preface, a favourable review, a prize, etc.)[25]

In other words, one becomes a consecrator because one has been consecrated after one has consecrated other things. Yes, this is exceptionally circular; it is a "circle of belief."[26] Those who track, promote, add to, and shape waves of authenticity can become legitimated as knowledgeable arbiters of authenticity, authorities on the specific subject matter and practices involved in their restricted field of production. They gain this authority through the contingencies and accidents of being recognized by others as such. They become legit by declaring other things legit, and they become legit by being recognized by others as legit: "Declaring something authentic legitimated the subject that was declared authentic, and the declaration in turn can legitimate the authenticator."[27] Or, as Bourdieu puts it,

> Every critical affirmation contains, on the one hand, a recognition of the value of the work which occasions it, which is thus designated as a worthy object of legitimate discourse (a recognition sometimes extorted by the logic of the field, as when, for example, the polemic of the dominant confers participant status on the challengers), and on the other hand an affirmation of its own legitimacy. All critics declare not only their judgement of the work but also their claim to the right to talk about it and judge it. In short, they take part in a struggle for the monopoly of legitimate discourse about the work of art, and consequently in the production of the value of the work of art.[28]

Looking back at the scholarship I cite in my reductive list above, we can see that, indeed, another word that also comes along for the ride with authenticity is legitimacy. In Vincent John Cheng's book *Inauthentic: The Anxiety over Culture and Identity,* he notes that "it is we in the Western academy, after all, who have access to the structures and institutions of speech and representation, and so we are more likely to be listened to as authenticating presences, conferring legitimacy for subaltern voices."[29] Writing about Arabic hip-hop music, Usama Kahf analyzes "authenticity claims in Palestinian hip hop to answer the research question: How do Palestinian hip hop artists establish legitimacy in relation to hip hop and in relation to their own cultural and political realities?"[30] Writing about heavy metal music fandom, Ben Hutcherson and Ross Haenfler argue,

> Not only does authenticity in music scenes have racial and class dimensions, such idealized representations are often gendered, often privileging the masculine as more authentic. In many [music] scenes, men are taken-for-granted performers and consumers of music, while women struggle for legitimacy both onstage and off.[31]

Thus, "the power to impose the dominant definition of reality, and social reality in particular," the power to judge who or what is in and who or what is out emerges through the struggles in whatever field we're considering and—this is important—solely on the terms of the field itself.[32] This is why Bourdieu argues that we cannot foist distinctions onto a field from without:

> The autonomy of a field of restricted production can be measured by its power to define its own criteria for the production and evaluation of its products. … [T]he more cultural producers form a closed field of competition for cultural legitimacy, the more the internal demarcations appear irreducible to any external factors of economic, political, or social differentiation.[33]

Instead, we have to trace how distinctions emerge from within a field on its terms and its terms alone, rather than using external criteria.

In terms of the field of production that is Dark Web network building, site hosting, and use, the term "legit" is directly tied to questions of authenticity and the power to judge. For example, when a Dark Web user calls a drug vendor legit on a drug market forum, they are doing two things. First, the user is proclaiming the vendor in question as "real," an actor or collective from whom one can *really get* drugs. The vendor is not a scammer nor a law enforcement officer. The vendor's products are not overpriced, and the drugs are of high quality. Second, the user's proclamation that the vendor is legit is simultaneously a proclamation that *the user is an authority on what's authentic,* that they are legit as well and able to judge the quality of vendors on the Dark Web.[34] These proclamations can be one-off posts, or they might be systematized into a collection of reviews of vendors, much like reviews of restaurants. To put this in terms of the symbolic economy, Bourdieu's consecration is an act of *legitimacy exchange*: I declare you to be authentic, and in my doing so, you enable me to demonstrate my own authenticity.

So here, I turn to ways to be legit on a specific Dark Web social networking site, Galaxy2. But first, a bit of history.

From Galaxy to Visibility to Galaxy2

Something that might be unique to the Dark Web is a tendency to name sites as if they're movie sequels. For example, after Silk Road shut down, Silk Road 2 took its place, and then there was Silk Road 3. Each was run by different administrators. In terms of the symbolic economy of legitimacy, the sequential Silk Roads were claiming to inherit the legitimacy of the original Silk Road.[35] This sort of naming is quite possible on anonymous networks that have little regard for copyright.

The social network Galaxy2 is in this vein. As its name implies, Galaxy2 was a sequel to Galaxy, a Tor hidden service that came online in August 2013 and disappeared abruptly in December 2014. Unlike MultiVerse or Dark Matters, the administrator of the original Galaxy left no "fuck you" message; instead, the site was simply gone. Prior to its disappearance, Galaxy had over thirty-three thousand registered users, although site members estimated that only 10 percent of them were active. Thirty-three thousand registered users and three thousand active members is small in comparison to Clear Web behemoths such as Facebook, but in terms of the Dark Web, Galaxy was a very popular site.

Galaxy was an anonymous social networking site, which is to say that users were expected to avoid revealing personal information about themselves, including names, gender identities, ages, or geographic locations.[36] Yet, because it was a social networking site, its interface and the norms of social networking shaped its uses, and its users built and maintained stable pseudonyms tied to typical social networking profiles. Over time, as often happens in online interactions, these pseudonymous users began to forge strong relationships as they shared images, liked each other's blog posts, and commented on each other's profiles.

Thus, when Galaxy suddenly disappeared, these users lost a key means of connecting and socializing with one another. But because

they had developed stable pseudonymous identities within Galaxy, a small group of users was able to reconnect: many of these users migrated to an I2P-based social networking site called Visibility, where they used their Galaxy screen names, profile pictures, and PGP keys to identify themselves to one another.[37] There, one Galaxy veteran formed a group called Galaxy Castaways, and this small group of users tried to figure out what to do next.

One of these Galaxy Castaways was Lameth, a self-described thirty-something heavy metal fan and computer network expert who had experience running and administrating Tor hidden services. Lameth volunteered to start a new Galaxy, and Galaxy2 was born in early 2015.

Galaxy2 replicated many of the features of the original Galaxy. Much of this can be attributed to the underlying software that both sites used (and Visibility currently uses), an open-source social networking system called Elgg. Elgg replicates many functions developed in sites such as Facebook and Twitter, including registration with a username and password, user profiles (with profile pictures, textual self-descriptions), likes, a social graph built on "friending," blogging, microblogging (called the Wire), user groups, commenting, and threaded discussions. Elgg is also centralized, which means that it runs in the client-server network model, with clients (users with web browsers) connecting to the central Elgg server to log in and interact with other users.[38] Elgg is built to work with a suite of open-source technologies familiar to many web developers, the LAMP (Linux, Apache, MySQL, and PHP) stack. Taken together, Elgg thus offers familiar social networking functionality to end users, while administrators have a relatively easy time installing and administering it.

But the underlying software was only part of the carryover from the previous Galaxy. In addition to using the same software, Lameth adopted many of the same rules the original Galaxy had. The original Galaxy was often praised by its users, who felt that it featured civil discourse and was populated by a friendly community. Lameth invoked these qualities in his welcome message:

> Galaxy2 is meant to be a respectful community. … I just want to keep Galaxy2 a nice and clean place that allows all to be here.

In effect, because of its sequential name, software, and rules, and because Lameth was a consistent presence on the original Galaxy and then Visibility, Galaxy2 inherited a great deal of the original Galaxy's practices, user base, and thus legitimacy. When Lameth brought Galaxy2 online in early 2015, the previous users were able to quickly understand both its functions and its community norms, and many of the Galaxy Castaways rebuilt their old Galaxy profiles and reconnected with one another.

Once on Galaxy2, the users renewed the original Galaxy's project of pseudonymous social networking within the anonymizing structures of Tor hidden services. After two years of existence, rules, standards, community norms, and practices have emerged that help members distinguish legit Galaxy2 (G2) members from the nonlegit.

Ways of Being a Legit G2 Member

1. Publicly Obey the Rules

As Jessica L. Beyer has noted in her study of various anonymous online groups, these groups are managed through a variety of means, including formal rules and informal community norms.[39] There are no set formulas, and each site varies in its mix of formal and informal regulation. With this in mind, to explore the "legit" on Galaxy2, I start with its formal rules before branching out to informal norms.

One of the first things Lameth did after launching Galaxy2 was write the rules for the site. I quote their original form in full:

1. **No child pornography**. That doesn't mean a censorship on discussing pedophilia, but [we] sure as hell censor any kind of media upload of this shit. Use your common sense, and if in doubt, ask before posting.
2. **No public commercial trade**. I don't want Galaxy2 to become a market targeted by different government agencies and police forces. Even benign legal trade will not be allowed, because what may be legal one place might not be legal another, and it's easier to just say "not allowed" than keep some complex system as to what is and isn't allowed. What happens in private conversation between members is private. But don't advertise stuff in the public areas.
3. **Be respectful**. Galaxy2 is meant to be a respectful community where ideas, philosophies, religion even, and so much else can be discussed, learned, taught, communicated, whatever. And it should all be done in a respectful manner. Trolling, flaming and simply being an ass toward others doesn't belong here. Go anywhere else for that.
4. **My word is law**. If I decide something, that's how it is. If you don't like it, let's discuss it, but just like a game master in a role playing game I maintain the right to have the last word. Now, once that is said I don't consider myself to be unfair or unapproachable, and I do not ban people just because I disagree with them. I am human and I can and properly will make mistakes, but I can admit to mistakes so if you feel unfairly treated, let's talk. I just want to keep Galaxy2 a nice and clean place that allows all to be here.

The first two rules are straightforward: to be accepted as a member of Galaxy2, users cannot post or solicit child exploitation images or offer to buy or sell any products or services. The administrators immediately ban anyone doing the former, and those who break rule 2 are often given warnings. In addition, Galaxy2

members themselves regularly warn new users who post commercial messages. The most common way is to respond to a commercial post with a variation of "Public trade is not allowed" and a link to the rules. In interviews, the admins have told me that members also regularly report violations of rule 1 if they are seen, including uses of code language ("cheese pizza," "jailbait") or avatars that feature pictures of children in new user profiles and comments. Every page and post on Galaxy2 has a "Report This" button, similar to content flags in mainstream corporate social media.

The third rule, "Be respectful," is much more difficult to enforce. Discussions of "ideas, philosophies, religion" provoke heated debates. Couple this call for discussion of controversial topics with the fact that the most active area of Galaxy2 is the Wire, a public character-limited microblogging system (similar to Twitter), and it is not surprising that ad hominem attacks and flaming can happen and are visible to all logged-in users.

For example, in late October and early November 2016—immediately before and after the U.S. presidential election, coincidentally—a weeks-long and often ugly argument between a few Galaxy2 members broke out on the Wire. Topics under discussion included pedophilia, Satanism, Hillary Clinton, online advertising, anonymous networks, porn, sex work, sexual assault, and Israel/Palestine.

These topics are obviously controversial in the most civil of settings. Yet, as contentious as these are, they are not necessarily off-topic for Galaxy2. Debates about topics such as these have occurred on Galaxy2 without participants resorting to "trolling, flaming or simply being an ass towards others." But in late 2016, the pace of the discussion was faster than the norm, with Wire posts appearing in rapid succession. This pace was fed by the ad hominem attacks users posted against each other: you're drunk, you're retarded, you're unreasonable, you're a troll. Grow the fuck up. You're white trash, you're lazy, you're illogical, you're a moron, you're uneducated. Go take some medication. And most

importantly, these flame wars were happening in the most public part of Galaxy2, where all members could see.

I've participated in Galaxy2 since its creation in early 2015, and these Wire arguments were, in fact, some of the worst I have seen. Other members agreed, and they began to point out the problems with this sort of uncivil clash. One longstanding G2 member wrote a long blog post arguing that uncivil posts can distract the administrators away from enforcing rule 1:

> Does [child pornography] exist on G2? It easily may. What makes us so distracted to identify it? "Mal-posting" Yes I just coined a term lol. Malposting, it's filling up a site with so much junk posts that it distracts the admins from focusing on what they should be looking out for. This is all MHO of course. I'd like to say it's like a DDOS, but with post.:)
>
> What to do? Do your part by not posting "junk" every five minutes, 24hrs a day. Don't let me discourage you from being here. Log in, hang out, post your thoughts, youtube vids, smart ass remarks, but don't flood the site with Malposts 24/7/365, it's a small private server, not Twitter. Most importantly if you are a G2 user then be a good steward of it. You don't have to be an admin to make it a better place. G2 is yours, it's mine.

During discussion, this member clarified:

> When I say "junk" I mean flooding the wire with mostly instigating, negative, trolling comments all day … sucking people into day long arguments because the comments are so inviting lol. It's like the playground fight in elementary. Sometimes I log in here and feel like I'm watching an out of control CNN presidential candidate discussion panel lmao!

Lameth reacted to this Wire incivility by pleading with members to stop using the Wire for anything but announcements of new blog posts:

> I would love to see the [user] groups getting the same love and attention as The Wire gets. That's what they are there for. That's their purpose; to get the level of content in any topic that would make Galaxy2 this awesome social collaboration in gaining and sharing ideas, thoughts, opinions, believes.
>
> I've half a mind to actually disabling The Wire entirely, if only for a while until the groups starts reaching their potential, and to teach you users as well as newcomers how to properly utilize them. Because they really do have great potential to build this community and take it far beyond the greatness of what it already is today. But it requires you to use it right. And having all the activity on The Wire isn't the right way to do it.
>
> The Wire is not meant for conversations as it's mainly used for now. It's not mean[t] to debate politics. It's not meant to discuss religion. It's meant to ask "Where do I find X?" or "I've just published Y."

Other members of Galaxy2, including longstanding members, supported Lameth, calling out users who engaged in ad hominem attacks on the Wire, decrying "malposting" and bad argumentation.

Nonetheless, public support of administrators is often not enough to halt incivility in the public parts of Galaxy2. At a certain point, the administrators may take a drastic measure: banning offending members by locking them out of, or even deleting, their accounts. As the Galaxy2 admin warned some members who were arguing over religion,

> Abusive dialogue has been and will be deleted. Keep it off the wire. Feel as passionately as you like about your religion, but do not assault everyone's sensibilities with it. If the battling parties persist, you will be banned.

This may seem trivial: after all, what is being "banned" is a pseudonymous account. What's to stop the banned person from starting a new one? When bans happen, however, they are treated extremely seriously by the members of the site. In the instances of banning I've observed, the friends of the banned account demand

that the banned be reinstated. Some use blog posts to write petitions, with others using comments to sign the petition. Some take to rival social networking sites to decry the ban and accuse the administrators of censorship (see the Dark Matters "Fuck You" message above). Some use the language of mourning to describe their feelings about the loss of their friend. All of this is a reflection of the power of social networking, even pseudonymous social networking, where users develop tight social relations through the mechanisms of friending, sharing, and liking. The same bonds that helped Galaxy2 emerge (via I2P's Visibility) after the end of the original Galaxy also result in these reactions to banning as a form of social exclusion, a punctualization of the practices of deciding who's in, who's out, who's legit, and who should be excluded.

These activities echo Jessica Beyer's observation that

> in spaces where users have identity over time, they will protect those online identities. Individuals will protect an online identity—even "aliases," such as user names or avatars. This protectiveness means that individuals will curtail inflammatory speech and avoid behavior that could draw censure from other users in such spaces.[40]

Thus, the "ban hammer" is the key censure administrators have to enforce social order on these Dark Web social networks. The power of the "hammer" is such that some members, who sense that they may be banned, decide to quit on their own terms rather than face the public sanction of being banned. One member who was very involved in the November Wire acrimony, and who was repeatedly warned by the administrators about violating rule 3, announced in a blog post that they were leaving, and subsequently did so. After this, the Wire largely returned to its normal, civil patterns—what Lameth might call "using it right."

The rules, the "Wire controversy," and the eventual exit of one of the more acrimonious Galaxy2 users illustrates how site rules are interpreted and violations of them enforced. The user who left was not banned—so far as I can tell, no one was banned for lack of

civility during the Wire controversy—but members and admins did police behaviors by calling out rule breakers, further establishing ways of behaving that enable Galaxy2 members to see who belongs and who does not. In this way, some members delegitimated particular practices and, inversely, legitimated themselves as arbiters of proper behavior on Galaxy2's Wire.

This leaves rule 4. In almost any meta-discussions about Galaxy2 policy, most members praise Lameth, accepting his claim that "his word is law," lauding him for creating a largely civil haven on the Dark Web. When Lameth makes decisions about the structure of the site, the rules, or how the rules are enforced, most members accept him as the most legitimate authority on the site's rules, practices, and user base. While this seems simple—if you sign up to a site, you ought to obey the administrator and the rules—it ties in with the legit at the level of legitimacy exchange. A social networking site relies on its users to contribute content; otherwise, it's merely an empty software interface. There are multiple Dark Web social networking sites (not to mention forums, chans, and chat rooms). If Dark Web users choose to develop their pseudonymous identities within the affordances and constraints of Galaxy2, they are exchanging legitimacy with Lameth: they provide content that allows Lameth to make the claim that Galaxy2 is, in fact, an authentic social networking site, and they confer on Lameth the legitimate authority to administer the site. They provide the authentic in order to produce the legit.

But while commercial activity, acrimony, and debate may not be accepted on the Wire or other public spaces, they can in fact happen on Galaxy2, and those engaged in them can still be authentic members. Elgg's affordance includes groups and private messages, and these allow outlets for practices that would otherwise be sanctioned. Another way to be legit on Galaxy2 is to shift communication to these more private channels.

2. Use Groups and Private Messages

The structure of Galaxy2 is not unlike Reddit in that members are encouraged to start interest groups (akin to subreddits). Although Lameth and the administrators consistently sanction members who engage in heated debates in the more public areas, such as the Wire, they encourage members to take up controversial topics in special-interest groups. Lameth's statement on the Wire quoted above is not the only time he called for more expansive debate and discussion to happen in groups.

While all members see the Wire and can post to it immediately, members have to join groups in order to post to them. Featured groups on Galaxy2 include CopBlock, a group dedicated to documenting police violence; New To Tor, in which members share links to other hidden services; a Bitcoin discussion group; the Cafe at the End of the Internet, a general discussion group; OPSEC, with guides on securing information; a group dedicated to the specialized Kali Linux operating system; and LGBTQ, a group for members exploring sexual and gender identities. As of this writing, Galaxy2 has nearly five hundred groups, some with hundreds of members, most with only a few or even just the lone founder as a member. Members display their group membership on their profiles, adding another layer of personalization to their personas.

If there are intense, heated debates that avoid admin sanction, they happen on group pages. An example is the group Antifa, an antifascist group. Early in 2016, the Antifa group founder grew concerned about a growing number of Galaxy2 accounts featuring swastikas, white power crosses, and anti-Muslim slogans, so he began naming and shaming Galaxy2 members who advocated for white supremacy or National Socialist ideology, posting links to their profiles in an Antifa group blog. This admin's actions were thus quite similar to current antifascist online actions. But some members whom the Antifa group labeled as racists took to the group's blog to argue. Some praised Hitler as a genius; others delighted in peppering their comments with the word "nigger"; still others accused the Antifa admin of being racist for being "antiwhite" and asked if Black Lives Matter supporters should be on the list, too. Many suggested that the existence of a group that has the

explicit goal of "making G2 hostile to racists" is a violation of rule 3, since making racists feel unwelcome is disrespectful to them.

Another example is the Tor Child Protection Agency. Like Galaxy2 itself, the group has rules: "1. Be Respectful. 2. Our main purpose is to expose Pedophiles. 3. Anyone is welcome to join who are against these scum." In between debates over the definition of pedophilia, this group's members also expressed their disgust with anyone who requested or shared child exploitation images. One member argued, "Killing them is too good—too quick—compared to the lifelong anguish and psychological problems they create and inflict on their victims. They need to be fully castrated—not just their balls—I mean it." I should note that members of this group were in fact very respectful with one another as they pondered ways to punish or hurt pedophiles.

In both of these cases, the debates and comments were more acrimonious than those in the Wire controversy. The antipedophile group openly advocated for violence, a line I did not see being crossed in the Wire controversy. While the fascists and racists who mocked the Antifa group never openly advocated violence, their repeated praise of Hitler invoked white supremacist violence, at least indirectly. But even with the acrimony, neither the group administrators nor the participants faced administrative warnings, let alone sanctions, because these debates were sequestered into private groups, and members have to opt in to these respective groups to see them and participate in them. This is different from the Wire, a more public, central social stream that all members see.

In addition, note that Lameth's rules do not prohibit *private* commercial exchanges, that they in fact suggest it. Galaxy2 also features a private messaging system with which members can send each other e-mails. Lameth has even gone so far as to provide tutorials on PGP encryption, which enables a sender to encrypt files so that only a specific recipient can open them. With such encryption, Galaxy2 members who want to make commercial exchanges can do so without Lameth or any administrators knowing. A member can send an encrypted offer to buy something to another, and the second one can encrypt a reply, with no one able

to read the messages but the recipients. Beyond Galaxy2, PGP encryption is a vital practice for nearly all Dark Web site users: countless forums, markets, and other social networks require users to be skilled with PGP, including the use of newer encryption protocols. Those who cannot work with PGP are not considered legit. Lameth and Galaxy2 reinforce this Dark Web–wide practice by encouraging members to communicate with PGP-encrypted private messages.

Thus, authentic Galaxy2 members can engage in harsher arguments, building social capital through delegitimating groups, ideas, or people they disagree with, even other Galaxy2 members. And they can engage in commercial activities as well. The main condition is that they push these practices into the more private spaces on the site, away from more public areas, such as the Wire.

Thus, the public/private divide within Galaxy2 reflects another element of the legit on the Dark Web: the recognition that Dark Web users require privacy for their communications. In other words, if Lameth had altered Galaxy2 to force *all* communications to be public, the site would not be considered legit by Dark Web users. After all, the requirement that all communications be open, public, and transparent is considered to be a vice, rather than a virtue, of the Clear Web. Lameth's instructions to members to use groups and PGP further legitimates the site and allows for legit uses, because it recognizes that authentic Dark Web practices require both opt-in systems (e.g., one must opt in to see group content) and privacy-protecting encryption.

3. Become a Technical Elite

In addition to the explicit rules (be civil in public, move debate to groups, use private messages for commercial exchanges), there are unwritten rules of authenticity on Galaxy2. A key topic of discussion is on technologies, such as networking, operating systems, and hacking. For example, checking the Wire on a typical day on Galaxy2, I saw these discussions:

- speculation about devices that can scrub air pollution

- how secure Clear Web to Tor proxies are, and how they work
- the compatibility of various software packages with different Linux distributions
- how to build wireless mesh nets

Technical discussions rely on restricted vocabularies, and thus Galaxy2 members can demonstrate their command of these vocabularies and therefore their legitimacy. This is what I have elsewhere called "techno-elitism": a command of specific technical terms and the consecrated ability to judge others on their use of this restricted vocabulary.[41]

Tracing technical discussions on the site reveals which members are consecrated as legit and which are "n00bs" (new users). For example, there is a steady influx of new users who ask a variation of "OK, I've made it to Galaxy2. Now, how do I go deeper to the Marianas Web? I need a quantum computer, right?" This question allows for the performance of technical authority by seasoned Galaxy2 members, who patiently explain that there is no "deeper" network, no Marianas Web (or its equivalent, the Closed Shell System), and that these places are Internet hoaxes. It also provides a chance for legit Galaxy2 members to explain to new users the topologies of Tor, Freenet, and I2P and how they relate to the rest of the Internet. These performances often happen in open blog posts or in the Wire, so they function as public displays of technical knowledge.

More complex discussions happen when members of the site ask about the differences between operating systems or between programming languages. These questions prompt long discussions about the distinctions between the operating systems Qubes and Tails, or OpenBSD and FreeBSD, for remaining secure while having control over one's machine, or the distinctions between scripting languages (Python versus PHP) or full programming languages (Java, C++, Visual Basic) as the best languages to learn to program. Often these discussions are in the context of questions about becoming a hacker. Unlike the Marianas Web question, "how to be a

hacker" discussions tend to be dialogues, with the new user feeling welcome to ask questions and the legit members offering advice: learn Linux. Learn how to network computers. "Avoid being [a] 'script kiddie'; it's not very respected."[42] Start to think like a programmer, like a hacker.

One exchange between a self-described new user and the legit hackers on Galaxy2 is notable. In response to the "how do I become a hacker?" question, one person wrote:

> Give up. The internet is full of more fantasy than hackers. Hacking looks nothing like movies, it requires years of dedicated study to learning basic boring things and building a system of knowledge. … If you are asking how do I become a blackhat [hacker], you have an elaborate fantasy and that simply wont sustain the years of effort, the reality of the process, and is dangerous when pared with the legal risk.

And another is more blunt: "I've two things to say to you: 1) USE FUCKING GOOGLE! 2) YOU'LL NEVER MAKE IT!"

Here, like many other moments of the legit on Galaxy2, we see the production of insiders and outsiders. The insiders are those who can pierce the veil of "fantasy," can negotiate the legal risk, and can learn on their own (by "using fucking Google"). They do not turn to sites like Galaxy2 to expose their naiveté. Outsiders are those who subscribe to the fantasy of the all-powerful hacker, as well as the fantasy of the "hacker community" that can transform n00bs into l33ts.

Arguably, these two responses violate rule 3, Be respectful. But most legit Galaxy2 members pride themselves not only on their technical skills, but also on their friendliness with new users. They will take n00b education as an opportunity to perform. To be a technical elite on this social network tends to require combining command of technical vocabulary with the willingness to explain it respectfully, which clearly gives the legit techno-elite members the chance to publicly perform their authenticity. These performances are enhanced when the techno-elites are also administrators of their

own Dark Web sites (such as blogs, forums, chat rooms). Such techno-elites can gain likes and friends through these performances and, if they run their own sites, traffic to them.

4. Demonstrate Pseudonymous Social Networking Skills

A second unwritten prohibition is against self-disclosure of personal information. Echoing the discussion of OPSEC in chapter 4, new members are often warned to not give out personal details. For example, a Galaxy2 member posted a guide to configuring the Tor browser bundle, warning, "Under no circumstances, never ever even give hints about your real name, country or any other personal details if you really want to stay anonymous. If you do so, even Tor couldn't help you to stay hidden." New users who post details about their ages or locations are often warned by veteran members to avoid doing so, often with lectures about the value of proper OPSEC. And, like the techno-elitist performances, seasoned users can demonstrate their authority by tutoring new users about the dangers of self-revelation.

But because Galaxy2 is a social networking site, the central activities of building a profile, collecting likes, declaring friendship with one another, and sharing media mean that members do build relatively stable, pseudonymous identities. These identities are, on the whole, more developed than those of Dark Web markets, where the dominant interactions center on buying and selling. Again, social networking bonds can be powerful. This was evidenced by the transition of the Galaxy Castaways from the original Galaxy to Visibility.i2p and finally to Galaxy2, where several original Galaxy members reused their pseudonyms, avatars, and PGP keys to keep their connections alive as they migrated. Some members have maintained the same pseudonym for many years.

The somewhat contradictory prohibition against personal details on a social networking site allows for long-standing members of Galaxy2 to demonstrate their skill in revealing certain details about themselves—for example, specific computer or networking skills, political or social interests—while not revealing others, such as

geographic location. For example, one member's "About Me" profile description reads:

> I will not disclose personal information unless necessary. Asking is moot and pointless. I will however, describe my background. Basic graphic designer, 3D modeler, and art historian. I made this account only to try and find information. Nothing more. If you want more information about me, I only trade knowledge for knowledge.

Another's profile includes this statement:

> I don't know who to trust here, or if anyone at all.
>
> Gender neither conifrmed [*sic*] nor denied, do not bother asking the question of gender identity for you will be given the answer of a Synthetic Human.
>
> My interests do not matter to you, nor will I give them out until time has come for me to unveil my anonymous figure to be released of vague details.
>
> I realize my display name says Jane Doe. It is but a name. It shall not, nor will it ever, reveal my gender.
>
> Discover me if you wish.
>
> But be warned; I will not trust so easily.

Members do offer e-mail addresses to contact them outside of Galaxy2, but they use e-mail services such as Sigaint, which do not require any personal information. Clear Web mail services, such as Gmail, are shunned because they are more easily traced to real-world identities. Members also share PGP public keys, which allow for others to send them encrypted messages. But again, these PGP keys are tied not to real-world identities but to throwaway Sigaint or Torbox accounts. It is rare for members to even share links to Clear Web sites, because (at least in Tor) the concern about using Tor with Clear Web sites is that exit nodes can deanonymize traffic.

But the line between social-networking-style self-revelation and the prohibition against self-disclosure is an extremely blurry one. To be an authentic member of Galaxy2 is in part to build

connections with others—quantified through public displays of numbers of friends and likes—while avoiding being seen as providing too much personal information and thus receiving warnings from other members who are constantly policing the informational security of the site. Thus, topics such as technical discussions function to allow for socializing while avoiding the need to divulge personal information. Moreover, one can become a legit Galaxy2 member—a consecrated authority on the site—by collecting large numbers of friends, likes, and comments on one's profile. Such legit members enjoy more respect when they weigh in on site discussions and debates.

Yet, there appears to be an exception to the blanket prohibition against revealing personal information.

A Contradicting Form of Authenticity: Being Young and Female on Galaxy2

For most members of Galaxy2, to be an authentic member is to be publicly civil, move any rule-breaking acrimonious or commercial exchanges to private (and often encrypted) channels, show technical skill, and avoid self-doxing. The legit demonstrate knowledge of these practices by pointing out violations of them to other users. Above all, the emphasis is on building a pseudonymous identity that does not explicitly reference the user's real-world identity and connecting it with other like-minded members. One way of thinking about this is socializing with a mask on. As Lameth put it to me in an interview, even when members refuse to share real-world details, "You still communicate, and over time you start to get a connection and feeling of each other."[43] Or, as another Galaxy2 member notes,

> I feel like nobody knows who I am, so I don't have to shield myself from some things. The deep web gets a deeper slice of my personality that I would never reveal on the surface. That "surface [shield]" is gone; I actually show some more emotions. And if it really gets too bad for me, I'll just go inactive and never be heard from again.

In other words, on Galaxy2, the "real/embodied/unmasked" person is irrelevant; what matters are the on-screen performances and social interactions of stable pseudonymous members.

But there is an exception. The rules of authenticity change as soon as a member identifies as a young woman.

As I suggested above, the line between personal revelation and too much information is a blurry one, but members tend to police it, pointing out when other members reveal too much and warning them against the practice. But when members reveal they are (a) female and (b) young, some members do the opposite: they demand *more* personal details. In these cases, other Galaxy2 members often demand that young- and female-identified users *authenticate* themselves by providing selfie images that include their pseudonyms and today's date written on sheets of paper or in marker on their bodies. Presumably, the combination of on-demand selfie image, written screen name, and date are enough to authenticate that these members are indeed young women.

It appears then that the prohibition against the revelation of personal information does not trump the homophobic or embarrassing prohibition against being catfished. "Catfishing" is a term used to describe misrepresentations in online profiles. It became part of the popular lexicon in 2013 after a prominent U.S. college football player found out that the woman he was emotionally and romantically connected to over the Internet for three years was actually a man.[44] The term was later used as the title of a movie and a reality television show on MTV exploring the consequences of such deceit.

The mere chance that some members may become emotionally involved (through likes, discussions, or sharing media, and the confessions that may arise in a pseudonymous environment) with others who are not who they appear has led some Galaxy2 members to accuse those who identify as young women of lying. In response, the women are pressured to—and sometimes agree to—post selfies to prove they are who they claim to be. One female-identified/young-identified Galaxy2 member took a selfie with her

screen name written on it, captioning it “for whenever I need to prove my existence.” Another posted a selfie with a screen name and the title “just so u know im not a 30y/o man.” Another posted a selfie with the caption, “I’m tired of being called a Liar.” Others posted selfies with the simple caption “Me.” Almost all examples of this practice I have seen are of young women.

Once their gender and age are established, these members often receive comments about their bodies: “lovely picture”; “your [sic] have the most sexiest gorgeous legs”; “I trace your body with my mouse”; “Sexy lol”; and “You have photos naked??” They receive propositions for chatting, private messaging, and image sharing from self-described “horny” Galaxy2 members. These comments appear in more private areas, such as on individual profiles, but I’ve seen them happen on public areas, such as the Wire.

Thus, it appears that in order to be accepted by other members as an authentic young woman on Galaxy2, one has to have one’s body put on display, a variation on the 4chan or Internet meme of “tits or GTFO.”[45] Here, as identifying details of gender and age emerge (either over time as members socialize or in a space such as a user profile), members call for another mode of authenticity and authentication, distinct from the practices of hiding personal details or demonstrating technical knowledge.

This approach to bodily display is not limited to self-identified young women on Galaxy2. It also occurs in groups dedicated to pornography. An example is the group titled Exposed: Female Edition. As its name implies, Exposed is a porn-sharing group. Its description reads

> This group is dedicated to females and their beautiful bodies. If you’re a woman lover and love the female form, then this group is for you. You can find pictures, post and much more in this group.

And like Galaxy2 itself, this group has rules of conduct:

> We only have one rule, **NO PICTURES OF MEN**!!!! If you like men, to each [h]is own, but please don't post none of that gay sh!t here. Now if there is a woman being f*cked by a guy, then by all means upload it. Just no plain and raw penises. Vagina, a woman's a** and tits have to be somewhere in there.

As of this writing, Exposed is Galaxy2's fourth most popular group, behind CopBlock, New To Tor: Looking for Interesting Links?, and Files and Stuff. It is more popular than the Cafe at the End of the Internet, a group that most Galaxy2 veterans recommend to new users as a way to meet other Galaxy2 members and begin the pseudonymous social networking process.

Thus, to be an authentic *female*—particularly young female—on Galaxy2 requires a different set of performances and rules. If a member claims to be a young woman, she will face pressure to authenticate herself with a signed and dated selfie, exposing her "female form" to allay fears of catfishing. And some members of this privacy-conscious community, where so many members use any image but their actual faces for their profile pictures, have no qualms about posting nude photos of women.[46] The message is that performances of femininity on Galaxy2 are conditioned by larger cultural values of objectifying women and putting their bodies ("vagina, a woman's a** and tits") on public display for masculine consumption, even when such displays violate privacy or result in sharing personal details.

That said, many of the self-identified women on Galaxy2, including those who agreed to post selfies to authenticate themselves, are very active members, and they are engaged in some wry gender politics of their own. One prolific member posts images of Palestinian women training with assault rifles, praising their military prowess in the struggle against Israeli occupation. She also engages in debates about a range of topics. Another has become a techno-elite, publicly offering thousands of words of technical advice to other members. Another member shares screenshots of private messages she has received in which other Galaxy2 members ask her for nude photographs and otherwise harass her because

she's a self-identified young woman. As she describes it, "I have a small album of screenshots publicly ridiculing the … messages I have received in the past, and that's pretty much stopped my encounters with people who ask." Her exposure of private harassment in public is a brilliant move: she contrasts one method of being legit on Galaxy2 (pushing communication into private and encrypted channels) with another (the demands on self-identified female members to be sexual objects). Her posts caused Lameth to lament, "And here I was just praising the user base of Galaxy2 … I hope you don't get too much of this?" Other members—self-identified as women or no—have made groups such as Feminism on the Dark Web to share feminist literature and philosophies with one another.

I thus do not call into question the authenticity of self-identified female members of Galaxy2, even those who violate the prohibition against self-disclosure by posting selfies. Their contributions to the site are accepted by other members as valuable. They can be just as authentic, just as legit, even if some succumb to the pressure to anchor their on-screen performances in images of their actual bodies.

Conclusions

Predominantly, to be a legit Galaxy2 member is in part to oppose the Clear Web model of social networking. Clear Web social networking, such as Facebook or Twitter, is perceived by Galaxy2 members to be recording every activity we engage in to build profiles that are tied to traditional identifying information, with the goal of selling this information to advertisers. Even Twitter users, who might use a pseudonym, reveal their Internet protocol addresses to Twitter—something Dark Web users work extremely hard to avoid. Thus, Galaxy2 as well as other Dark Web social networks (e.g., Sone on Freenet, and Visibility, Ano+, or ID3NT on I2P) were built in reaction to pervasive surveillance, commercialization of sociality, and the threats of government and corporate censorship. As scholars of authenticity rightly note, authenticity is constructed partly in relation to what is perceived to be *inauthentic*, and Dark Web social networking members believe that Clear Web social networking is not legit.

This is a direct contrast to the production of authenticity that Alice E. Marwick and danah boyd found on Twitter, where "revealing personal information is seen as a marker of authenticity."[47] At first glance, we might argue that revealing personal information is more authentic than hiding it. But if we judge authenticity and the legit on the terms of Galaxy2 (and social networking on the Dark Web more generally), rather than on some fixed, objective measure of "authenticity," we see the opposite: that hiding personal information while socializing is one means of becoming legit. Thus, Galaxy2 is a response to a lack of authenticity on the Clear Web, with Dark Web social networking members decrying what they see as fake, idealized, self-promoting, and corporate-corrupted practices on Facebook or Twitter. In contrast, from their perspective, social networking on the Dark Web offers something deeper, something

more real, more authentic, than the content made by self-branding Clear Webbers.

Thus, anti–Clear Web authenticity is marked by "the continued craving for experiences of unmediated genuineness" that are—intriguingly—produced through anonymous/pseudonymous interaction, rather than what Dark Web users perceive as fake performances for Facebook audiences.[48] As one Galaxy2 member told me in an interview,

> As I have said in many posts, I believe that is where people are at there [*sic*] most honest: when the mask goes on, many of our daily masks come off. We tend to shed layers of societal convention and become closer to who we really are. Humans are social creatures. A psychologically well-adjusted person will seek out others of his peer group. [Dark Web social networking sites] provide this watering hole for this medium. Once foddered, to extend the metaphor, he's free to range elsewhere as he chooses, knowing the herd is there to welcome him home.[49]

As another Galaxy2 member noted in a blog post, "I can't help but notice that most people on here are realists, as opposed to the self centered average joe on the clearnet. It's not that I'm surprised given where we are, it's just refreshing." And, as Lameth noted in a message to Galaxy2 users, Galaxy2 is an "experiment, proving that you don't need to sell your life to corporations in order to establish meaningful online connections with other people around the world."

Simultaneously, however, authenticity on Galaxy2 is also a response to the media ideology of the Dark Web as a place for terrorists, drug dealers, and purveyors of child exploitation images. In that same message to users, Lameth also noted, "We are not a shady den that deals in drugs, weapon[s], child pornography or terror. We are not the place that common media will have everyone else believe about the Tor projects and it's 'citizen', its users." The emphasis on civility in the public areas of Galaxy2 is in part a

reaction to the sense that anonymous communication must inevitably devolve into the worst human behaviors. While some new users of Galaxy2 may argue that terrorist speech should be allowed because all speech should be allowed, or that drug dealing should be allowed because to ban it is to limit user freedom, or that images of naked, sexualized children are only 1s and 0s and thus ought not be censored, Galaxy2 administrators and members have continually pushed these activities away from their site, delegitimating them and thus legitimating other ways of using the Dark Web. As the prohibitions against incivility during the Wire controversy and the threat of banning shows, Galaxy2 is not a free-speech free-for-all but a site with a cultivated culture that emerges through struggles over authenticity.

To be legit on Galaxy2 is to accept these limits and to experiment with the mix of freedom and constraint that emerges through the mixture of social networking software, anonymizing networks, and community norms. In this way, the meaningful term "legit" gets at questions Christine Hine asks in *Virtual Ethnography:* "What are the implications of the Internet for authenticity and authority? How are identities performed and experienced, and how is authenticity judged?"[50] The distinctions that Galaxy2 administrators and members draw between their site, Clear Web social networking, and other Dark Web practices provide the criteria to judge who is an authentic Galaxy2 member and who is not. Those members who can negotiate these distinctions, as well as demonstrate skills in pseudonymous social networking, can become legitimated authorities on what is authentic in Galaxy2. Indeed, while Galaxy2 started with only Lameth having administrative power—including the power to ban users—as the site grew, Lameth began to recruit administrators, who have taken an increasingly active role in the site as it has grown to over seventeen thousand members. The new administrators came from the stock of long-term, socially respected members who had already proved their ability to perform according to the written and unwritten rules of the site.

In this sense, the production of the legit—of accepted authority on who belongs and who does not—on Galaxy2 echoes Regina Bendix's analysis of folklore studies, which itself longed for the "ideal folk community, envisioned as pure and free from civilization's evils."[51] The authentic, Bendix argues, is an ineffable reminder of what is perceived to have been lost. In this case, the Clear Web in general and corporate social media in particular have lost their capacity for freedom, so people turn to the Dark Web and its social networking sites to recover what's lost. To be legit on Galaxy2 is to command knowledge of what has been lost as well as what is possible on the Dark Web.

But the problem of the other form of authenticity on Galaxy2 remains: the pressure on self-identified young women to authenticate themselves with pictures of their bodies, as well as the existence of groups such as Exposed: Female Edition, not to mention those members espousing fascist or racist views (as seen in the Antifa group discussion). These practices and groups may continue to marginalize potential Dark Web users seeking an alternative way into the network than through the drug markets. As many corporate social media sites, including Facebook and Twitter, struggle under the weight of hate speech, harassment, and a newly legitimated white supremacist "alt-right" movement, a Dark Web social network may appear to be a refuge. But the repeated emergence of hypermasculine practices on Galaxy2 itself can make that network seem like anything but a refuge to many people. The subtle logics of inclusion and exclusion that appear on Galaxy2 contribute to—but certainly do not entirely explain—the fears many people have about the Dark Web as an exclusive and even a frightening networking practice.

And yet, Galaxy2's experiment in building a particular form of Dark Web authenticity is clearly an experiment in progress, one that is open to being shaped in new directions. Even facing the problems of harassment of self-identified female Galaxy2 members, Lameth has abstained from writing that rare genre of Dark Web posts: the

“Fuck You, I’m Shutting This Down” message. He continues the experiment that is Galaxy2.

Postscript: Happy New Year

As I have done in the past with my writings about Galaxy2, I shared a draft of this chapter with Lameth, who in turn shared it with other site members and administrators. Lameth has been a key source of insight into the Dark Web, and we have developed a relationship through correspondence over the years. I was nervous about sharing this chapter, especially because of the criticism it levels against Galaxy2 over the recapitulation of hypermasculine practices (specifically, the harassment of self-identified women and the existence of the Exposed porn group).

I shared the chapter around New Year's Day, 2017, which also happens to be the time of Galaxy2's second anniversary. Lameth wrote a blog post celebrating this milestone, but also included some requests for members:

> There is a thing that has been called to my attention that I'd like to bring up. One that could be considered a little smudge or dent in this pedestal I keep putting the G2 community upon. It's an extension of sorts of one of my previously rants about respect, and that is how young female users are treated on Galaxy2. It seems like it has become acceptable and common practice to "demand" that users who claims to be females prove themselves by taking pictures and posting them with some sign or some way of authenticating them as females. Yet, for every other user, intent and purpose, it's preached that people should guard their privacy and anonymity.

Lameth went on to argue that

> We should respect everyone equally, and girls deserve the same right to privacy as the next guy. If people want to show their faces or provide personal information, then sure, fine, it's their decision. But we shouldn't as a community build up peer pressure to make someone feel like they have to compromise their person in order to be accepted, acknowledged and respected here.

This blog post began a discussion in the comments about these practices, with one self-identified young woman confiding,

> To think back the past year and reflecting, I was attacked the most for not proving I was female. I finally did post pictures of myself, to be harassed even more. People begging for nudes and all other kinds of things, which made me feel like dirt, because I didn't come here for that, I actually came here to get away from that. Being a Teen Girl online is hard as fuck and people don't understand that. I actually have suggestion for girls, if you don't want people knowing about you, keep all personal info out of conversation.

Here, this member performs the legit: she delegitimates harassment and legitimates the unspoken rule of Galaxy2 that members ought to avoid providing personal information. She uses her experience—and not to mention her reputation as a prodigious poster on Galaxy2—to establish herself as an authority on the site.

Other members discussed next steps: perhaps a group to ferret out members who make such requests. Perhaps a mentoring program for new users who join Galaxy2 and need to learn the site's culture, including the unwritten rule against personal self-disclosure. I'm glad to say that the discussion continues on Galaxy2 as members continue to develop norms for authentic participation in the site.[52] Time will tell if the pressure on self-identified young women will fade; given the overall culture of the Internet, I doubt it. Galaxy2 could even spin out of the control of Lameth and other administrators, as new members arrive and ignore or flaunt the community norms and rules; many other Dark Web social networks

experience this, as the “Fuck You” messages quoted above show. But for now, Lameth’s legit authority over the site and his willingness to call out harassment mark Galaxy2 as a site that defies conventional understanding of what happens on the Dark Web. The site’s longevity—contrast it with the short-lived sites described at the beginning of the chapter—is a testament to its consciously developed culture.

To be certain, this chapter has been critical of the selfie-authentication demands leveled at self-described young women on the site, but to Lameth’s and the rest of Galaxy2’s credit, the site actively struggles with problems such as this, trying to solve some of the intractable problems of the Internet. Galaxy2 is a legitimate Dark Web social network.

Notes

1. Infernal1, "MultiVerse | Closing Message," S-Map: The Social Media Alternatives Project, August 23, 2015, https://socialmediaalternatives.org/archive/items/show/164.

2. Fenris, "To the Shutdown of Dark Matters," Galaxy2, November 18, 2016, http://w363zoq3ylux5rf5.onion/blog/view/160082/to-the-shutdown-of-dark-matters [Tor].

3. To see screenshots of many of them, see S-Map: The Social Media Alternatives Project, https://socialmediaalternatives.org/archive/items/browse?tags=dark+web&page=1.

4. Infernal1, interview by author, August 21, 2015.

5. In interviews with me, the Multiverse admin preferred the "he" gender pronoun.

6. In the past three years, I have seen member counts on various social networks in excess of twenty-five thousand.

7. There are exceptions, of course: Walter Benjamin, "The Work of Art in the Age of Mechanical Reproduction," Marxists Internet Archive, February 2005, http://www.marxists.org/reference/subject/philosophy/works/ge/benjamin.htm; Brooke Erin Duffy, "Manufacturing Authenticity: The Rhetoric of 'Real' in Women's Magazines," *Communication Review* 16, no. 3 (July 1, 2013): 132–154, doi:10.1080/10714421.2013.807110; Oliver L. Haimson and Anna Lauren Hoffmann, "Constructing and Enforcing 'Authentic' Identity Online: Facebook, Real Names, and Non-Normative Identities," *First Monday* 21, no. 6 (June 10, 2016), http://firstmonday.org/ojs/index.php/fm/article/view/6791;

Theo Van Leeuwen, "What Is Authenticity?," *Discourse Studies* 3, no. 4 (2001): 392–397. My own definition draws on their work.

8. Dominik Bartmanski and Ian Woodward, "The Vinyl: The Analogue Medium in the Age of Digital Reproduction," *Journal of Consumer Culture* 15, no. 1 (March 1, 2015): 3–27, doi:10.1177/1469540513488403; Greg Dickinson, "Joe's Rhetoric: Finding Authenticity at Starbucks," *Rhetoric Society Quarterly* 32, no. 4 (2002): 5–27; Duffy, "Manufacturing Authenticity."

9. Regina Bendix, *In Search of Authenticity: The Formation of Folklore Studies* (Madison: University of Wisconsin Press, 1997); Louise Archer, "Younger Academics' Constructions of 'Authenticity,' 'Success' and Professional Identity," *Studies in Higher Education* 33, no. 4 (2008): 385–403.

10. Samantha Senda-Cook, "Rugged Practices: Embodying Authenticity in Outdoor Recreation," *Quarterly Journal of Speech* 98, no. 2 (May 2012): 129–152, doi:10.1080/00335630.2012.663500.

11. Michael Mario Albrecht, "Acting Naturally Unnaturally: The Performative Nature of Authenticity in Contemporary Popular Music," *Text and Performance Quarterly* 28, no. 4 (October 1, 2008): 379–395, doi:10.1080/10462930802351989; Sean Chadwell, "Inventing That 'Old-Timey' Style: Southern Authenticity in O Brother, Where Art Thou?," *Journal of Popular Film and Television* 32, no. 1 (2004): 2–9; Ben Hutcherson and Ross Haenfler, "Musical Genre as a Gendered Process: Authenticity in Extreme Metal," in *Studies in Symbolic Interaction*, vol. 35, ed. Norman K. Denzin (Bingley, UK: Emerald Group Publishing, 2010), 101–121, http://www.emeraldinsight.com/doi/abs/10.1108/S0163-2396(2010)0000035010; Usama Kahf, "Arabic Hip Hop: Claims of Authenticity and Identity of a New Genre," *Journal of Popular Music Studies* 19, no. 4 (2007): 359–385; Steve Redhead and John Street, "Have I the Right? Legitimacy, Authenticity and

Community in Folk's Politics," *Popular Music* 8, no. 02 (May 1989): 177–184, doi:10.1017/S0261143000003366.

12. Vincent M. Meserko, "The Pursuit of Authenticity on Marc Maron's WTF Podcast," *Continuum* 29, no. 6 (November 2, 2015): 796–810, doi:10.1080/10304312.2015.1073682.

13. Mark Jancovich, "'A Real Shocker': Authenticity, Genre and the Struggle for Distinction," *Continuum* 14, no. 1 (2000): 23–35.

14. Vincent John Cheng, *Inauthentic: The Anxiety over Culture and Identity* (Piscataway, NJ: Rutgers University Press, 2004).

15. Van Leeuwen, "What Is Authenticity?"

16. Mustafa Emirbayer and Eva M. Williams, "Bourdieu and Social Work," *Social Service Review* 79, no. 4 (2005): 689–724.

17. Haimson and Hoffmann, "Constructing and Enforcing 'Authentic' Identity Online"; Alice E. Marwick and danah boyd, "I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience," *New Media and Society*, July 7, 2010, doi:10.1177/1461444810365313.

18. Most of these scholars take this adjudication seriously, attempting to establish through close readings of texts or through sociological analysis how certain people, practices, or things are deemed to be authentic. In contrast, Sean Chadwell takes a very interesting approach: he closely reads the film *O Brother Where Art Thou?* and argues that the film is premised on ways "authenticity" is deployed by musicians and politicians to gain resources or power. See Chadwell, "Inventing That 'Old-Timey' Style: Southern Authenticity in O Brother, Where Art Thou?"

19. Bendix, *In Search of Authenticity*.

20. Sarah Banet-Weiser, *Authentic™: The Politics and Ambivalence in a Brand Culture* (New York: New York University

Press, 2012), 10.

21. Kate Bowan, "R. G. Collingwood, Historical Reenactment and the Early Music Revival," in *Historical Reenactment: From Realism to the Affective Turn*, ed. Iain McCalman and Paul Pickering (London: Palgrave Macmillan, 2010), 146.

22. Think of debates about who is a "real American" and their consequences for immigrants, Muslims, or people of color. Or think of corporate efforts to make "authentic brands" and the consequence of colonizing our ways of thinking by associating our emotional lives with particular consumer objects.

23. Van Leeuwen, "What Is Authenticity?," 396.

24. Pierre Bourdieu, *The Field of Cultural Production: Essays on Art and Literature* (New York: Columbia University Press, 1993), 42.

25. Ibid.

26. Ibid., 77.

27. Micki McGee, *Self-Help, Inc.: Makeover Culture in American Life* (New York: Oxford University Press, 2005), 7.

28. Bourdieu, *The Field of Cultural Production*, 35.

29. Cheng, *Inauthentic*, 21.

30. Kahf, "Arabic Hip Hop," 362.

31. Hutcherson and Haenfler, "Musical Genre as a Gendered Process," 102.

32. Bourdieu, *The Field of Cultural Production*, 101.

33. Ibid., 115.

34. Notably, one does not become legit by claiming oneself to be legit. In fact, doing so leads others to argue you're trying too

hard. Instead, becoming a legit Dark Web user is typically a matter of judging the authenticity of other Dark Web users, practices, and sites, and gaining a reputation as an accurate judge of them. Any time I see someone explicitly claim "I am legit" on the Dark Web, the person is usually running a scam.

35. Given that each subsequent Silk Road was largely more scam than legit market, however, subsequent "sequels" to Silk Road are now treated more like bastards than legitimate offspring. As the *Deep Dot Web* puts it, "The only reason a dark net market operator would have for naming his or her site after Silk Road is to create a false sense of credibility to attract inexperienced users and steal their money." See "Silk Road 3.1," *Deep Dot Web*, 2017 (accessed July 20, 2017), https://www.deepdotweb.com/marketplace-directory/listing/silk-road-3.

36. For a discussion of this type of social networking site, see Robert W. Gehl, "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network," *New Media and Society* (October 16, 2014): 1–17.

37. Visibility.i2p is still online and is similar to Galaxy2 in that it's been a relatively stable institution on the I2P network. It has not attracted as many users as Galaxy2, however.

38. This is distinct from a peer-to-peer system in which data are distributed across networks of devices, rather than served from a central computer. Sone, a social networking site on the Freenet network, is a peer-to-peer social network.

39. Jessica L. Beyer, *Expect Us: Online Communities and Political Mobilization* (New York: Oxford University Press, 2014).

40. Ibid., 9.

41. Gehl, "Power/Freedom on the Dark Web."

42. A “script kiddie” is someone who uses premade computer code to break into other people’s computers without understanding how the code works. This is less respected than understanding the code and writing your own.

43. Lameth, interview by author, May 19, 2015.

44. Jack Dickey and Timothy Burke, “Manti Te’o’s Dead Girlfriend, the Most Heartbreaking and Inspirational Story of the College Football Season, Is a Hoax,” *Deadspin*, January 16, 2013, http://deadspin.com/manti-teos-dead-girlfriend-the-most-heartbreaking-an-5976517.

45. Vyshali Manivannan, “Tits or GTFO: The Logics of Misogyny on 4chan’s Random - /b/,” *Fiberculture*, no. 22 (2013), http://twentytwo.fibreculturejournal.org/fcj-158-tits-or-gtfo-the-logics-of-misogyny-on-4chans-random-b/.

46. This is all the more troubling when some of the images are framed as “revenge porn” images, but revenge porn is not prevalent on Galaxy2. Instead, the images tend to be copied from porn sites.

47. Marwick and boyd, “I Tweet Honestly, I Tweet Passionately,” 127.

48. Bendix, *In Search of Authenticity*, 8.

49. Xl33t, interview by author, December 18, 2014.

50. Christine Hine, *Virtual Ethnography* (Thousand Oaks, CA: SAGE, 2000), 8.

51. Bendix, *In Search of Authenticity*, 7.

52. During the copyediting phase of publishing this book, however, Galaxy2 has gone down, replaced with a message from Lameth noting the site had database problems. He expressed hope that

the site could be revived, but as of this writing in late 2017, this has not happened.

7 Facebook and the Dark Web: A Collision

<tonious> "I2P: Who needs the IETF?"

—From jrandom's collected I2P quotations

Facebook's Tor hidden service, found at https://facebookcorewwwi.onion, is lightning in a bottle. It is at the intersection of all three legitimacies analyzed in this book: state delegation of rules and regulations to a standards body (in this case, the Internet Engineering Task Force [IETF]); corporate propriety (DigiCert, Facebook); nonprofit propriety (the Tor Project); hacker legitimacy (the [now disgraced] hacker wunderkind Jacob Appelbaum); and Dark Web authenticity (the notoriety of Silk Road). Thus, Facebook on Tor is an association of state-delegated power, respect of resources, and authenticity. It is also a symbol of the blurred lines between the Dark Web and the Clear Web, a collision of legitimation and delegitimation.

This is a story of triumph for at least one of the Dark Web systems discussed in this book. As journalists have argued, Facebook's presence on Tor legitimates that Dark Web system, making it a bit more like the Clear Web, but, of course, with a security- and privacy-conscious spin. Facebook's ability to get an Extended Validation (EV) certificate from DigiCert only furthered this narrative. Not only can we connect to Facebook via Tor and avoid ISP surveillance or government blockage of our use of that social network, we can also do so and see the little HTTPS lock icon in our Tor-enabled browsers. Facebook's entry into Tor hidden services happened in October 2014—only one year after the Silk Road bust, months after the Freedom Hosting child exploitation bust, and in the middle of Silk Road founder Ross Ulbricht's highly publicized trial. Rather than focus on the morally "dark" aspects of Tor hidden services, journalists covering Facebook's hidden service could instead focus for a while on the world's largest social network, a

multibillion-dollar company, helping to connect the "social graph" more securely. Facebook's https://facebookcorewwwi.onion Tor hidden service helped hammer home the point that Tor's value lies in part in helping "the dissident" (as discussed in chapter 3) communicate without fear of government reprisal.

Moreover, thanks to Facebook's help, a year later, the Tor Project received a major benefit: the designation of .onion (Tor hidden service's pseudo-top-level domain [TLD]) as a special-use top-level domain (SUTLD) by the IETF and that domain's subsequent registration with the Internet Assigned Names Authority (IANA). After a six-month process, the Internet-Drafts (I-D) process, Facebook's Alec Muffett and the Tor Project's Jacob Appelbaum were able to publish an IETF standard, RFC 7686, "The '.onion' Special-Use Domain Name." This standard placed .onion into the Internet Corporation for Assigned Names and Numbers (ICANN) Special-Use Domain Name list, alongside only seven others. The goal of this designation was to instruct non-Tor-equipped browsers not to send requests for .onion sites to the public domain name system. This would protect user privacy: a request for an .onion site sent to the public DNS would reveal that the user intended to visit that site. And recognition of Tor hidden services by Internet standards bodies furthered the idea that Tor hidden services were integrating into the "legitimate" Internet.

And yet, while this can be a story of the legitimation of Tor hidden services, a legitimation achieved through state-supported practices of standards production and identity verification, corporate and nonprofit propriety, and hacker legitimacy, this can also be a story of disappointment, frustration, and conflict, especially if told from the perspective of another Dark Web network described in this book: the Invisible Internet Project (I2P). The rapid process by which the IETF granted .onion SUTLD status came after years of debate over a different I-D, Christian Grothoff and colleague's "Special-Use Domain Names of Peer-to-Peer Systems." This proposed standard would have granted SUTLD status to six pseudo-TLDs: .gnu and .zkey (both used by GNUnet); .bit (used by Namecoin); and, most relevant to this book, .i2p (used by I2P

eepsites), as well as .exit and .onion (both used by Tor). Thus, the Grothoff et al. I-D, first proposed a year before Facebook's Tor hidden service was launched, would have provided SUTLD status not only to the Tor Project, but also to GNUnet, Namecoin, and I2P. In fact, representatives from I2P, GNU, and Tor all worked together to draft that now-failed standard. In turn, all these organizations may have then been eligible for special rules for Extended Validation certificates, allowing recognizable Internet companies to mirror their content on these respective networks.

Nonetheless, Grothoff and his co-drafters failed in this task.

This chapter is thus a mix of triumph and failure, told through analysis of infrastructural—which is to say, boring—documents and discourses of standards bodies.[1] It is the story of how Tor hidden services were able to benefit from an economy of legitimacy while I2P's eepsites failed to do so. And it is about Facebook's relationship to the Dark Web: collisions between mainstream Internet governance and Dark Web legitimacy, between perceptions of the Clear and Dark Webs. It is the story of how practices we commonly associate with the Dark Web (drug sales, delegitimated violence, and child exploitation) appear across the Internet, while practices we associate with the Clear Web (authentication of identities, centralized authority) have begun to appear on a Dark Web system.

Special-Use Domain Names: The IETF's RFC 6761

The story starts in the highly technical, backgrounded, infrastructural processes central to the modern Internet: the production of Internet standards, especially those set by the Internet Engineering Task Force (IETF). The IETF is charged with setting standards for the protocols that enable the Internet to work. Despite their boring nature, Internet standards have profound influences on how we communicate today.[2] And they have direct bearing on the structure and legitimacy of the Dark Web.

The IETF's Request for Comments (RFC) process is the system task force members use to hammer out standards and protocols for Internet functionality. One such RFC is particularly important to the Dark Web: RFC 6761, titled "Special-Use Domain Names."

RFC 6761 was written by two Apple employees, Marc Krochmal and Stuart Cheshire.[3] Approved by the IETF and published in mid-February 2013, Krochmal and Cheshire's RFC 6761 formalizes a process by which the IETF could set aside certain top-level domain names as "special use," preventing their being registered with another Internet governance body, ICANN, the corporation that normally oversees allocation of TLDs.

RFC 6761 set aside a small group of TLDs as special use: .localhost, .test, .invalid, variations on "example," and various longer strings ending in .arpa. These names had been traditionally used for testing purposes, local networking, and as example domains. They had been recognized for these purposes since 1999. In other words, these names were reserved to preserve these technical uses, and thus Internet users are not allowed to get domain names that involved them—say, for example, weavingthedarkweb.test or robertwgehl.example.

In 2011, however, ICANN voted to allow an expansion of generic top-level domain names (gTLDs) from the historical six (.com, .edu, .org., .net, .gov, .mil) to an eventual thousands. This meant that

corporations could apply for branded TLDs (such as .apple) or speculative terms (such as .bank). The danger, then, was "name collision," where a TLD used for one purpose (say, in a local private network) could be registered for use on the public Internet. Such a collision would confuse web browsers and other software as they attempted to load requested files. It would be a collision between previously existing specialized networking protocols and the larger Internet.

This is exactly why Krochmal and Cheshire proposed RFC 6761. As Apple employees, they were interested in a SUTLD name registry because of Apple's own arguably special-use domain: .local. This domain was part of Apple's Bonjour local networking system, often used in people's homes to connect computers, printers, and media devices to one another. Because the domain had been in use for over a decade, millions of devices were potentially relying on it. If ICANN were to inadvertently allow a corporation to register .local for use on the public Internet, the smaller, private Bonjour networks would likely break down as a result of name collisions, as computers would not be able to distinguish between local-area-network .local devices and wide-area-network .local sites.

Krochmal and Cheshire's RFC 6761 created a process to set aside special domains to avoid this sort of problem. Thus, less than a week after receiving IETF approval for RFC 6761, they immediately used it to establish .local as a SUTLD in RFC 6762.[4] With that, no one could register .local to the public Internet; the potential collision between the broader Internet and Apple's specialized local network software would be avoided.

While it benefited Apple's Bonjour system, RFC 6761 also revealed a way for systems using domain name–like structures (e.g., mycomputer.domain), yet not seeking to use public DNS, to apply for their pseudo-TLDs to be recognized by Internet governance authorities. This had great appeal to the makers of Dark Web systems, such as Tor and I2P. Recall from chapter 3 that both Tor and I2P had established their respective pseudo-TLDs, .onion and .i2p, in 2003, using them as TLDs for their Dark Web sites. Tor

hidden services end in .onion (e.g., 347k6hepharlncwb.onion), and I2P eepsites end in .i2p (e.g., legitimate.i2p). ICANN's opening up of gTLDs in 2011 introduced the danger that some entity other than Tor and I2P could register .onion or .i2p and cause massive problems for these long-established anonymizing networks.

FOSS Friends: GNU, Tor, Namecoin, and I2P Work Together

Mindful of this problem, in 2013, a few months after RFC 6761 was adopted, Free and Open Source Software (FOSS) developers Christian Grothoff, Matthias Wachs, Hellekin Wolf, and Jacob Applebaum sought to follow the procedure laid out in Krochmal and Cheshire's 6761 document. They pursued the goal of setting aside several new TLDs as SUTLDs in a proposal submitted to the IETF titled "Special-Use Domain Names of Peer-to-Peer Systems." Its opening reads,

> The hierarchical nature of DNS makes it unsuitable for various Peer-to-Peer (P2P) Name Systems. As compatibility with applications using DNS names is desired, these overlay networks often define alternative pseudo Top-Level Domains (pTLDs) to integrate names from the P2P domain into the DNS hierarchy.
>
> This memo describes common Special-Use Domain Names [RFC6761] pseudo Top-Level DNS Names designed to help harden name resolution security (e.g., [RFC6840] [RFC6975]), provide censorship resistance, and protect the users' privacy on the Internet.
>
> In this IESG Approval document we are asking for domain name reservations for five Special-Use Domain Names [RFC6761] TLDs: ".gnu," ".zkey," ".onion," ".exit," and ".i2p."[5]

In a later draft, Grothoff and colleagues added .bit, the TLD for the Namecoin system. Several of these TLDs—especially .onion and .i2p—represent the state-of-the-art in anonymizing technologies.[6]

The FOSS developers positioned these networks as "peer-to-peer" to contrast them with the hierarchical and centralized domain name system (DNS). Their point was that, rather than relying on the centralized DNS, these networks resolve domain names on their

own (as described in chapter 3). Much like Apple's Bonjour .local TLD, which resolves domain names (such as officeprinter.local) to IP addresses without using the public DNS, GNUnet, Namecoin, Tor, and I2P can resolve names, such as the Dark Web site zzz.i2p, without resorting to the public DNS. Unlike Bonjour, they can do it on a global scale. And again, if these names are not reserved, some entity could buy them from ICANN and cause network confusion on a global scale.

In its collection of TLDs, the Grothoff et al. document represents collaboration among the network builders: GNUnet developers, Tor developers, I2P developers, and Namecoin developers worked together on this draft. On the I2P developer forum at zzz.i2p, I2P lead developer zzz reported that Grothoff shared an early draft written with Wachs and Wolf.[7] In late 2013, after Grothoff shared the draft on the Tor-dev mailing list, the Tor Project's Jacob Appelbaum contributed edits and was accepted as a coauthor.[8] I2P developers Orion and str4d contributed, as well. This level of collaboration among sometimes rival networks was welcomed by I2P developers, who took to Twitter to declare, "Yes it's true @GNUnet @torproject #I2P all working together."[9]

Christian Grothoff expressed hope that FOSS organizations, such as GNU, Tor, and I2P, could get recognition for their traditional TLDs from IETF just as big corporations, such as Apple, had for .local. Accepting their draft "would show that IETF is not entirely owned by companies and it [*sic*] willing to work with free software developers, researchers and document issues for normal users. Call me an idealist, but that was my hope when we wrote the draft."[10] Apple's interest in .local as a SUTLD hinged largely on the fact that Apple had used .local for over a decade in its Bonjour home networking system. Tor and I2P, of course, had used .onion and .i2p since 2003; for Grothoff, this meant their claims to their respective SUTLDs ought to have been as easily accepted as Apple's claim of such status for .local, even if their organizations were small nonprofits producing nonproprietary software.

Of course, being a technical standards body, the IETF had to debate the Grothoff et al. draft and did so in e-mail list threads in starting in late 2013.[11] Indeed, as the decade-long discussion over what would eventually become RFC 6762 reveals, these technical debates can take a long time. Still, the FOSS developers were hopeful that RFC 6761 had opened a way for them to gain recognition of their systems' TLDs by an international standards body.

Yet Grothoff's idealism in hoping that the IETF would approve these projects' requests would be tested after a parallel development: Facebook's entry into the Dark Web.

Https://facebookcorewwi.onion

While the IETF's debate over the Grothoff et al. proposal carried on from 2013 and through the next year, a major new Tor hidden service launched on Halloween 2014: https://facebookcorewwwi.onion.

This multibillion-dollar corporate entry into the same network that had hosted the infamous Silk Road drug market gained a great deal of attention in the news media, with coverage in the *Guardian*, *MIT Technology Review, PC World,* and *Wired*. For those with experience or knowledge of Tor hidden services, much of the attention was paid to the URL. As discussed throughout this book, most Tor hidden service URLs are non-human-readable 16-character alphanumeric strings (e.g., http://toristinkirir4xj.onion/). In contrast, Facebook's onion URL is memorable (to this day, it's the only one I can remember): https://facebookcorewwwi.onion. An .onion URL is a cryptographic hash of the site's public key, so they tend to look like gibberish. Getting a URL with even one long human-readable word takes a great deal of computing power, because the site operator has to generate many key pairs. For Facebook to get a human-readable URL with arguably *three* human-readable words, it had to generate *a lot* of key pairs, leading many to admire (and fear) Facebook's sheer computational capacities.[12]

A bit overlooked, but arguably more important, were the characters preceding Facebook's .onion URL: *https://*. Web users will recognize the S in HTTPS as meaning "secure" SSL-enabled HTTP. It's what turns on the little lock icon in our browsers when we visit banking sites or Amazon.com. It signifies an encrypted connection. Moreover, when you visit https://facebookcorewwwi.onion, the Tor browser also shows green text reading "Facebook, Inc. (US)," indicating you are indeed at Facebook's Tor hidden service. To set up such a connection, a large corporation has to get an Extended Validation certificate from a

certificate authority, which verifies the identity of the site operator. Given that Tor hidden services can be operated anonymously, issuing EV certificates for them seemed to be out of the question.

But one certificate authority, DigiCert, made an exception for Facebook, offering "the first publicly trusted SSL Certificate issued for the Tor browser and its .onion top-level domain."[13] Through a lengthy audit process, DigiCert verified that Facebook, Inc. was indeed the legal owner and controller of https://facebookcorewwwi.onion. In a blog post announcing this, Facebook security engineer Alec Muffett noted,

> We decided to use SSL atop this service due in part to architectural considerations—for example, we use the Tor daemon as a reverse proxy into a load balancer and Facebook traffic requires the protection of SSL over that link. As a result, we have provided an SSL certificate which cites our onion address; this mechanism removes the Tor Browser's "SSL Certificate Warning" for that onion address and increases confidence that this service really is run by Facebook. Issuing an SSL certificate for a Tor implementation is—in the Tor world—a novel solution to attribute ownership of an onion address; other solutions for attribution are ripe for consideration, but we believe that this one provides an appropriate starting point for such discussion.[14]

In other words, the HTTPS connection over Tor was required to make the experience of browsing Facebook's hidden service as close as possible to browsing facebook.com. Moreover, given the problem of onion "cloners" (man-in-the-middle proxies, discussed in chapter 5), DigiCert's EV certificate helped authenticate https://facebookcorewwwi.onion as indeed Facebook's legit hidden service and not a scam.

But DigiCert's EV certificate for Facebook had a short shelf life. It was an exception to many of the rules set by the Certificate Authority/Browser Forum (CAB Forum), which establishes the industry standards for EV certificates. The CAB Forum was largely

supportive of certificate authorities (such as DigiCert) providing certificates to .onion sites.[15] In fact, in February 2015, the CAB Forum passed Ballot 144, "Validation Rules for .onion Names," which formalized the certificate process for Tor hidden services. In a nod toward concerns about state violence and protecting dissidents (echoing the discussions of the network builders I describe in chapter 3), the ballot noted,

> Because onion names are not easily recognizable strings, providing the public with additional information about the operator has significant security improvements, especially in regions where use of the incorrect name could have lethal consequences.[16]

The CAB Forum's decision had only one major condition: the .onion TLD must be recognized by Internet governing bodies by November 1, 2015, a mere nine months away.[17]

The clock was ticking. Thankfully, as the CAB Forum participants noted, .onion was being considered for such status through Grothoff and his coauthors' proposal.

Facebook and Tor Break Away

The Grothoff et al. draft, which would satisfy the CAB by gaining official recognition for .onion (as well as .bit, .gnu, and .i2p), continued to be mired in debate at the IETF, even into 2015. There were repeated themes over the years of debate. Several IETF members questioned the wisdom of including six potential SUTLDs (.exit, .onion, .bit, .gnu. .zkey, and .i2p) since these six represented four distinct networking systems.[18] Others questioned the importance of any of these networks, with the possible exception of Tor (since Tor hidden services had gained some notoriety because of Silk Road).[19] Many of the debaters suggested that these respective projects simply buy these names from ICANN, which would cost $185,000 and require the organizations to have an administrative and technical infrastructure in place (a tall order for these low-budget nonprofits).[20] Others suggested that the IETF create a single SUTLD, such as .alt, and require these networks to use it instead of their preferred SUTLDs.[21] The harshest critique was the accusation that the Tor Project, I2P, GNUnet, and Namecoin were "squatting" on these TLDs and using RFC 6761 to circumvent the ICANN process.[22] As Paul Hoffman puts it,

> Squatters should expect that the name that they are using might eventually be legitimately assigned later, possibly to someone whose intentions are quite different from the squatters. This is how the IETF has worked for over 20 years. The purpose of RFC 6761 is not to say "if you start squatting on a TLD, you will be able to later get it reserved." It is to say "if there are legitimate errors in TLD use, those can be dealt with."[23]

Here, Hoffman warns the anonymizing network projects that the Internet standards bodies have the legitimate authority to take their

TLDs and grant them to someone else (who has a legitimate claim on the name). The only way to get a TLD, in Hoffman's view, is to go through the proper channels, rather than simply declaring one and expecting other entities to respect that claim. A variation on this theme was the snarky "I want a .pony" comment, essentially arguing, "If they get special TLDs, I want one, too!"[24]

Overall, much of the debate pointed to flaws in RFC 6761, since it appeared to offer little guidance for evaluating the Grothoff et al. proposal. In any case, the debate over the FOSS developers' draft dragged on, threatening the CAB Forum's requirement that .onion be recognized by the end of 2015.

In the midst of this debate, on March 5, 2015, a new Internet-Draft was submitted to the IETF: Jacob Appelbaum and Alec Muffett's "The .onion Special-Use Domain Name." Appelbaum of the Tor Project—and one of the coauthors of Grothoff et al.—collaborated with Facebook security engineer Alec Muffett, who was in charge of Facebook's move onto Tor hidden services. The abstract of the document was one line: "This document registers the '.onion' Special-Use Domain Name."[25]

Effectively, Tor had broken away from its collaboration with GNU, Namecoin, and I2P—and it had taken Facebook along with it.

In the terms of this book, this was a legitimacy exchange between Facebook, a company that commands respect and resources, and Tor's Jacob Appelbaum, a legit hacker. Facebook is, of course, a massive Internet corporation with a worldwide presence, enjoying a great deal of legitimacy as propriety. Appelbaum was famous in his own right. As I describe in chapter 3, Appelbaum was a highly respected figure in hacker and liberation technology circles. He was a member of the hacker group Cult of the Dead Cow, had been on the cover of *Rolling Stone,* represented Wikileaks in public, and had access to the Edward Snowden archives, to mention a few bona fides. At the time of this legitimacy exchange between Facebook and Tor, Appelbaum was legit.[26]

This legit hacker and privacy advocate led the way in bringing his and Muffett's I-D to the attention of the IETF. In a March 16, 2015,

e-mail to the DNSOP group mailing list, Appelbaum writes

> Tor's onion names are widely deployed and used by lots of folks all around the world. Our deployment size isn't news or really much of a discussion point—rather, I'm primarily concerned about users who have certificates issued to .onion names. Our Special Use Domain Name for consideration is directly related to things happening in the CAB forum … most importantly is the date October 1st. On that date we'll have a death day for currently issued certifcates [*sic*] with .onion names. This makes the onion name issue rather time sensitive and without further action, some stuff will likely break.[27]

Here, for Appelbaum, Tor's importance ("deployment size") is indisputable. The issue is time. The CAB Forum's decision in Ballot 144 put an expiration date on EV certificates for .onion, such as Facebook's. But, if the IETF were to accept his and Muffett's I-D, all would be well: Ballot 144 had established a mechanism for EV certificates issued to .onion sites as long as the .onion top-level domain was reserved as a special-use top-level domain, just like Apple's .local.

But because Appelbaum and Muffett's I-D was submitted while Grothoff et al.'s was being considered, a bit of confusion arose. After all, both documents were applying for SUTLD status for .onion. In a reply to Appelbaum, Paul Wouters asked, "Is this meant to replace or augment [the Grothoff et al. proposal]?"[28] Neither, replied Muffett: "My understanding is that this is not meant to replace that document, but instead that this document is a separate one."[29] To alleviate some of these concerns, Muffett uploaded a revision to his draft, which included a citation to Grothoff et al.:

> Note that this draft was preceded by [I-D.grothoff-iesg-special-use-p2p-names], which registered .onion alongside other, similar TLDs. Because .onion is in wide use, it has become urgent to expedite its registration. This does not indicate that the other registrations should be abandoned.[30]

Appelbaum and Muffett's draft appeared not to preclude Grothoff et al.

Yet, Appelbaum and Muffett's citation of Grothoff et al. actually undermined it. Tor's hidden services, they claimed, were in "wide use," implying that the user bases of Namecoin, GNUnet, and I2P were smaller and thus less in need of expeditious registration. This is a subtle (if perhaps unintended) delegitimation of the other systems as less important because of their smaller scales.

Moreover, in breaking from the GNU/Tor/Namecoin/I2P collaboration, Appelbaum and Muffett reinforced two repeated themes in IETF discussions of Grothoff et al.: that .onion was the most important of the six TLDs, and that Grothoff et al. ought to be broken up into separate proposals. Facebook's entry into the Tor network, coupled with the notoriety of legit, authentic, dangerous hidden services (especially Silk Road, which was repeatedly cited by IETF members who emphasized the importance of .onion) reinforced the impression that Tor hidden services were far more important than the other Dark Web systems.[31]

These delegitimating arguments won. Whereas Grothoff et al. was mired in debate for years, Appelbaum and Muffett's Internet-Draft became RFC 7686, and thus an Internet standard, in a matter of months. After being proposed in March 2015, it was voted on and approved by October of that year, just in time to satisfy the CAB Forum's timeline.[32]

Grothoff's Reaction

During the debate over what would become RFC 7686, Christian Grothoff grew increasingly angry. After Wouters asked if Appelbaum and Muffett's I-D was meant to replace Grothoff et al., Grothoff replied,

> It's pretty simple. The [Appelbaum and Muffett draft] doesn't obsolete or replace [Grothoff et al.], it's a Lex Facebook, just like reserving ".local" was a Lex Apple. I'm not generally against those at all, but I personally dislike that IETF passes things quickly if they are backed by multi-billion dollar companies, while putting up high hurdles (and delays are obstacles) for proposals that are just as sound but do not come with such support. Corporatocracy at its best. … [T]he multistakeholder process is designed to deadlock on almost everything, except for what the corporations need (as they represent a sufficient number of the "stakeholders").[33]

Though Grothoff was chastised for this comment, RFC 7686's speedy approval, compared to the years of debate over Grothoff et al., supports his observation.[34] This is all the more striking considering that Grothoff took the advice offered on the DNSOP mailing list to break up his proposal into multiple ones, each focusing on their respective special domain names. He did so on June 30, 2015, but all four drafts expired after no debate.[35] So, too, did Grothoff's original draft. To date, the only special-use top-level domains to be approved using the RFC 6761 process, .local and .onion, happened to have the support of multibillion-dollar tech firms (Apple and Facebook). Grothoff's concerns about the IETF working only with large corporations appear to be legit.

Moreover, after multiple bouts of intense debate about SUTLDs, the IETF has since decided to revise RFC 6761, with one member

calling it a “mistake.”[36] The avenue for network builders, such as I2P, to get an SUTLD appears to be closing.

I2P's Reaction

When Grothoff first sent his draft to I2P developer zzz in 2013, zzz shared it with a few others, gathered feedback on it, and gave it his blessing.[37] He and other I2P developers watched the mailing list discussions of Grothoff et al., and I2P developers made sure to meet with Grothoff at the 2014 Chaos Computer Club meeting to further refine the proposal.[38] As retweeted by str4d, he posted to Twitter the note about GNU, Tor, and I2P all working together.

Even in the midst of this optimism, however, by roughly January 2015, zzz predicted, "There's likely to be a push for throwing everybody but tor out of [the Grothoff et al. I-D] … if they try to throw us out we need to fight … they want to divide and conquer."[39] Indeed, this reflected a common theme in IETF mailing list entries: Grothoff et al. should be broken up. And, of course, it predicted the eventual outcome—Appelbaum broke away and coauthored RFC 7686.

After Grothoff et al. expired in 2015, I2P developer str4d continued to push for some solution to the problem of the I2P top-level domain, perhaps through a revision of RFC 6761.[40] In contrast, zzz appeared resigned to the fact that the IETF would never reserve .i2p. As he wrote in the I2P developer forum in 2016,

> We were … dead … when Jake and Alec broke away from the group. As Christian [Grothoff] predicted, we got divided and conquered. Neither he nor Hellekin [Wolf] is throwing bombs any more. There's nobody fighting for us, and [the IETF] doesn't want anything to do with it.[41]

Yet, looking back over the I2P developer notes reveals that I2P contributors apparently did not spend much time and energy advocating for the Grothoff et al. draft, even though they took time to meet with Grothoff in 2014, and despite zzz recruiting I2P

developers to monitor the IETF process. Given the size of many of these FOSS projects, which are, in the end, run by small groups of mostly unpaid volunteers, it made sense for them to pool their energy into one proposal to shepherd it through the IETF Request for Comment process. Christian Grothoff and Hellekin Wolf were clearly attentive to the draft, making multiple revisions and contributing many e-mails to the IETF mailing list. But they did not as clearly represent I2P as well as a dedicated I2P developer might have. Companies with the resources to dedicate employees to the process, as Apple and Facebook had, were far more effective. For example, Apple's Stuart Cheshire worked on what would become RFC 6762, the .local reservation, for more than a decade. Facebook's Alec Muffett monitored the IETF, CAB Forum, and Tor mailing lists and readily answered questions about RFC 7686. In contrast, I2P representatives' involvement was sporadic.[42]

Clear and Dark Collisions

Internet standards debates may be highly technical, boring, and largely relegated to specialized e-mail lists and conferences. They are also profoundly consequential. RFC 7686 has major implications for the future of Dark Web systems that extend beyond the legitimation of Facebook's .onion EV certificate or the "special" status of the .onion TLD. The introduction of certificate authorities, HTTPS, and Facebook into Tor hidden services raises a question: If these corporations increase their presence on a Dark Web system, how different would the Dark Web be from the Clear Web? In other words, taking up and expanding the concept of the "name collision" (where the naming system in one network overlaps with another) what does Facebook's attempt to avoid collisions tell us about the distinctions—and collisions—between Clear and Dark?

Collision One: Real Names Meet Anonymity

Facebook's entry into Tor hidden services is a culture of real names colliding with a culture of anonymity. The middle of this century's first decade was marked by a divergence between these two cultures. In early 2004—right as Tor and I2P were first deploying Dark Web sites—Mark Zuckerberg coded what would become Facebook at Harvard. Originally, Facebook was restricted to Harvard students with a verified Harvard e-mail address. Thus, the identities of members of Facebook were authenticated by a third party, Harvard University. The pattern continued as Facebook expanded to other Ivy League schools, other universities, and selected employers. By the time Facebook was opened to the general public in 2006, it had constructed a culture of real-world identities; its members would further vet one another by "friending" people they knew. Facebook continues this practice to this day, stating in its Terms of Service, "Facebook users provide their real names and information, and we need your help to keep it that way."[43] Facebook

is arguably the largest identity authenticator on the Internet, with services using Facebook Connect as a login system to authenticate the identities of their members.

In contrast, of course, the anonymizing networks Freenet, Tor, and I2P have been developed to dissociate user identities from their reading and publications. Facebook's entry into Tor hidden services is thus a collision between a culture of real identities and that of the anonymizing networks. This collision was met with disdain from some Dark Web users. On a Tor-based wiki that gathers links for Tor hidden services, the link to Facebook's hidden service was annotated "C.I.A. front for gathering the identities of Tor users." Another Tor-based collection of links warns users, "Many sources claim [facebookcorewwwi.onion] to be legit ... but use it at your own risk." As Krueger, the admin of the original Galaxy social network, told me in an interview, "I found it weird to see FB inserting itself in the context of the Deep Web when their policies so far are apparently quite contradictory to the anon philosophy of Tor."[44] On Galaxy2, one member described Facebook as "a swollen hemorrhoid, located in or around the butt-hole of the clearnet." Another Galaxy2 member writes, "Its a cess pool. Anything that ask for that much detail, is not doing for safety, but doing it to collect data. It is a Data mining tool, and the Masses gladly follow along." For these Dark Web users, Facebook represents *illegitimate* social networking because of its data-collecting and real-identity practices, and its entry into the Dark Web undermines the very purpose of anonymizing networks.

Collision Two: Hierarchy Meets Peer-to-Peer

Another collision between Clear (Facebook, central certificate authorities, and "real" identities) and Dark (anonymity, attempts at decentralization) is in the production of hierarchies, both within Tor hidden services and among the Dark Web systems discussed throughout this book.

First, if web users become further conditioned to seeing HTTPS in their browsers and carry this mentality onto Tor hidden services—as

Tor founder Roger Dingledine has theorized they will—then the original dream of Freenet and Free Haven (the precursors to Tor) might fade away.[45] The dream of Freenet and Free Haven was for both anonymous reading *and* publishing, but certificate authorities do not deal with completely anonymous publishers. Instead, certificate authorities use a procedure to verify the legal identity of the would-be EV certificate holder, as well as that legal entity's control of the URL in question. Similar to Facebook's presence on Tor, the idea of certificate authorities verifying the identities of Tor hidden service owners was met with disdain by seasoned Dark Web users. As one prominent Tor hidden service admin put it during a debate on Galaxy2 about certificate authorities for Tor, "The whole point of .onion is that it works without AUTHORITY. Authority is meaningless on darknet. Therefore a certification authority is stupid." By colliding the Dark Web with Clear Web practices of certificate authorities, Facebook and DigiCert alter the equation, bringing identifiable, powerful corporate entities into a previously anonymized space, where they can authorize sites as legitimate and thus mark others as illegitimate. Indeed, a subtle push in this direction was seen in the 7.0.2 version of the Tor Browser Bundle: user name and password pages on hidden services presented a warning that "This connection is not secure" alongside a padlock icon with a red line through it.[46] This warning is patently false: a connection to a Tor hidden service is always end-to-end encrypted. But this false warning may give new Tor users pause: Do I risk an "unsecure" connection and log into Galaxy2, or do I use Facebook's Tor hidden service instead? The spread of HTTPS to the Dark Web (at least on Tor hidden services) may make it more like the contemporary Clear Web, where users will gather at large corporate sites rather than at smaller, noncorporate sites.[47]

There is a more positive interpretation, however. Together, the CAB Forum, IETF, DigiCert, and Facebook have opened the door for legitimated Clear Web sites, such as the search engine DuckDuckGo, the *New York Times*, and the nonprofit news organization ProPublica, to get Extended Validation certificates,

while anonymous Tor hidden service hosts would continue operating without them. This is arguably good for users who wish for the greater security of verifying the identity of these services and helps mitigate the problem of .onion cloners. Further, it drives more traffic into the Tor network, providing cover traffic for those who need anonymity. Above all, it brings a form of Clear Web corporate propriety to one Dark Web system, Tor hidden services. Indeed, as Roger Dingledine wrote on the day Facebook moved onto Tor, "I am excited that this move by Facebook will help to continue opening people's minds about why they might want to offer a hidden service, and help other people think of further novel uses for hidden services."[48]

But even this more positive scenario will result in hierarchies of legitimacy. While Tor hidden services have been legitimated, I2P (as well as GNUnet and Namecoin) have been delegitimated. These latter systems may be locked out of getting something their network builders are clamoring for: popular (read: Clear Web) services mirrored or accessible via their networks, because providing such access today requires HTTPS, which in turn requires the recognition of certificate authorities, which in turn requires the IETF to register the system's top-level domain. The I2P developers, who established .i2p as their TLD in 2003, are effectively condemned to further marginalization. Whereas the Tor project can attract major Internet sites as well as large corporate donations, I2P is failing to do either. It is also not attracting the high-powered network servers that can reduce latency in the network. In other words, developing an innovative anonymous network topology and an anonymous nonprofit is seemingly not enough to be successful; a network must be legally identified, made visible, and consecrated as legit. It must gain respect for its command of resources, attract yet more resources, and have its technology consecrated by various quasi-governmental, technical, and corporate authorities. The network needs to gain legitimacy (through exchange, appropriation, purchase, inheritance, and, yes, delegitimation) from computer science, Internet corporations, hacker communities, government

agencies, as well as users themselves (who develop the sites, such as Silk Road, that gain notoriety in the press). The Tor Project has done all these things, and the Invisible Internet Project has not.

As Grothoff said, I2P, GNU, and Namecoin will keep using .i2p, .gnu, and .bit regardless of the decisions of the IETF, but given the explosive proliferation of gTLDs, top-level domain name collisions are increasingly likely to occur. If, for example, an enterprising name registrar buys .bit and sells domain names with that TLD, Namecoin's unique, non-DNS naming system will collapse. As the possibility of name collisions increases, the likelihood that any new alternative web system could pick its own TLD for its own naming system goes down significantly. Developers would have to either buy a TLD from ICANN and hope that they select one that does not conflict with someone else's intellectual property claims, or use a new naming system (and go against decades of custom and application-level expectations). Either way, new alternative network developers—very likely organizations with small budgets and voluntary labor—seem to be required to engage with the very systems they want to escape, such as DNS, corporate regulation, and global Internet governance. Facebook, DigiCert, and the Tor Project's collision will have consequences for other Dark Web systems, present and future. If the late 1990s and early 2000s were a boom time for new anonymous alternatives to the World Wide Web, the current decade appears to be a time when powerful institutions are working to prevent new networks from being launched.

Collision Three: Clear Meets "Dark" Practices

Another way to consider the Clear and Dark collision is to be clear eyed about the content on Facebook itself. News coverage of the Dark Web has often emphasized its dangerous aspects: scams and lies; child exploitation images, revenge pornography, terrorist propaganda, drug sales, weapons sales, and so-called red rooms, where one can supposedly watch someone be killed.[49] But all of these have appeared on Facebook as well, and some of them—lies,

revenge pornography, terrorist propaganda, and "red rooms"—have had a much larger presence on that social network than on the Dark Web. The prevalence of fake news meant to gin up clicks and likes on Facebook is, of course, well documented.[50] In one widely reported incident, child exploitation videos were shared across Facebook.[51] One Facebook user tweeted, "There's a legitimate child porn video circulating Facebook!"[52] In March 2017, the Center for Investigative Reporting broke the story that U.S. Marines were sharing nude photos of their colleagues in a Facebook group, Marines United.[53] Terrorists use Facebook to recruit.[54] The start of Facebook's Marketplace was marked by drug sales.[55] The *New York Times* has reported on the extent of gun sales on Facebook.[56] Most recently, Facebook seems to be a venue for mediated death and murder, with videos of people being shot, including by cops, posted to the network.[57] This is in contrast to Dark Web red rooms, which are urban legends.

Facebook's efforts to avoid collisions—both for the .onion TLD and for Facebook's own hidden service—bring to light the collisions that occur all the time between Dark and Clear Webs in terms of how we perceive their uses and users. How does one network become delegitimated while another is legitimated? Why does the red room—the mythical website where one can watch someone be tortured and killed—become continually associated with Tor hidden services, while such activities are unthinkable (but actual) on Facebook? In other words, when we name something "legitimate," how does it collide with the "illegitimate"? To be certain, this plays on the moral/ethical connotations of "darkness," a means of defining the Dark Web that I reject (see chapter 1). It also plays on "going dark" in terms of revealing personal information about oneself: here, a system of "real names" (Facebook) collides with a system of pseudonyms and anonymization.

This is not just to pick on Facebook. Many Clear Web sites are struggling with the sort of content and practices typically associated with the Dark Web. To understand Clear/Dark collision a bit further, consider a comment on a Reddit thread titled "What's your

deep web story?" which accuses other Clear Web services of fostering disturbing content:

> I am a Freenet user, and I had quite a few frightening experiences.
>
> Once someone threatened me for telling him that killing Netanjahu is a dumb idea which would only make matters worse for Palestina. But wait, that was on G[oogle]+ ...
>
> Then that other time, when I was insulted by Neonazis. But wait, that was on twitter ...
>
> How about when someone brought down my site to hack into other computers? No, that was my normal clearnet site. Twice ...
>
> So there's the problem with Freenet. We have few horrorstories. People who use Freenet generally know what they are getting into. They are warned at every moment to be careful with what they click on and what they talk about. To the point of generating random names by default, so they aren't tempted to reuse a nickname. I know that there is bad stuff, but I ignore it, because in Freenet that actually makes it go away: If no one accesses it, it gets overwritten by new uploads.
>
> So we don't actually have much interesting to share in this thread, except for: "Freenet works. It works really well."
>
> That wasn't what you wished for? Well: That's the darknet where it works. It ensures freedom of communication by making sure that it works for all its users, including those with a weaker stomach AND those who want to dig into the ugly stuff.[58]

As Facebook moves into Tor, as that corporation helps legitimate Tor hidden services, the lines between Dark and Clear blur a bit more. I am not asserting equivalence between anonymous networks and the Clear Web, but the lines between Dark and Clear are far blurrier than much of the panicky media coverage would have us believe. While the assignment of .onion may have meant that Tor's chosen TLD would not collide with an ICANN TLD, Facebook's

presence on the Dark Web shows us a different sort of collision: between an anonymizing network and its polar opposite, a real-identity-obsessed advertising and marketing firm. What this collision reveals is that the struggles of the Dark Web are the struggles of the Clear Web, perhaps on a different scale, perhaps with different cultural and technical constraints and affordances, but the distinction between the two is harder to see when a site like Facebook joins one of these networks.

Ultimately, the Facebook/Dark Web collisions show that Dark Web shares many aspects of the Clear Web, that it is not some "deeper" level cut off from the standard Internet, nor is it entirely composed of the worst of humanity. Beyond gaining access to password-protected areas—which exist on and off the Dark Web—there is no going "deeper" into the Internet. And the idea that the Dark Web is *entirely* made up of "dark" ("antisocial" or "terrorist") activities is also false: the Dark Web is more than this, and "dark" activities are happening all over the Internet. It's easy to claim the Dark Web is pure evil, just as it's easy to find evil on Facebook or on other Clear Web sites. As this chapter has shown, it took a highly bureaucratic Internet governance process to fully reveal these intimate ties between Clear and Dark.

Notes

Epigraph: "Jrandom's Old Collected Slogans," I2PWiki, June 16, 2016, http://i2pwiki.i2p/index.php?title=Jrandom%27s_old_collected_slogans [I2P].

1. I mean "boring" in the sense Susan Leigh Star, Matthew Fuller, Andrew Goffey, and Brian Cozen mean it: highly consequential, and yet largely ignored. See Susan Leigh Star, "The Ethnography of Infrastructure," *American Behavioral Scientist* 43, no. 3 (1999): 377–391; Matthew Fuller and Andrew Goffey, "Digital Infrastructures and the Machinery of Topological Abstraction," *Theory, Culture and Society* 29, no. 4–5 (July 1, 2012): 311–333, doi:10.1177/0263276412450466; Robert W. Gehl and Brian Cozen, "Passé Media: Communication and Transportation on Commuter and Computer Buses," *Communication Theory* 25, no. 3 (March 31, 2015), doi:10.1111/comt.12056.

2. Andrew L. Russell, *Open Standards and the Digital Age: History, Ideology, and Networks* (New York: Cambridge University Press, 2014).

3. Marc Krochmal and Stuart Cheshire, "Special-Use Domain Names," Request for Comments (Internet Engineering Task Force, February 2013), https://tools.ietf.org/html/rfc6761.

4. Stuart Cheshire and Marc Krochmal, "Multicast DNS, RFC 6762," IETF Datatracker, February 20, 2013, https://datatracker.ietf.org/doc/rfc6762/. To clarify, however, the drafts that lead to what would become 6762 had been debated by the IETF for over a decade. RFC 6761 paved the way for 6762's acceptance after this decade of debate.

5. Christian Grothoff et al., "Special-Use Domain Names of Peer-to-Peer Systems," IETF Datatracker, November 13, 2013, https://tools.ietf.org/id/draft-grothoff-iesg-special-use-p2p-names-00.txt.

6. Freenet is not included in this list, but Freenet's system does not use TLDs; instead, every file is located with a key that has no TLD.

7. Zzz, ".I2P Domain Registration with IETF," Zzz.I2P forum, November 13, 2013, http://zzz.i2p/topics/1518-i2p-domain-registration-with-ietf[I2P].

8. Christian Grothoff, "[Tor-dev] Registering special-use domain names of peer-to-peer name systems with IETF," Tor-dev mailing list archives, November 6, 2013, https://lists.torproject.org/pipermail/tor-dev/2013-November/005747.html; Jacob Appelbaum, "[Tor-dev] Registering special-use domain names of peer-to-peer name systems with IETF," Tor-dev mailing list archives, November 9, 2013, https://lists.torproject.org/pipermail/tor-dev/2013-November/005763.html.

9. Str4d (@str4d), "#P2PNames RT @i2p: Yes it's true @GNUnet @torproject #I2P all working together http://datatracker.ietf.org/doc/draft-grothoff-iesg-special-use-p2p-names/... ," Twitter, January 24, 2015, 2:19 p.m., https://twitter.com/str4d/status/559083166519287811.

10. Christian Grothoff, "Re: [DNSOP] [internet-drafts@ietf.org: I-D Action: draft-grothoff-iesg-special-use-p2p-names-00.txt]," IETF Mail Archive, December 1, 2013, https://mailarchive.ietf.org/arch/msg/dnsop/5TOdxaQzDFLhF4zenKndoR7PVVg.

11. Stephane Bortzmeyer, "[DNSOP] [internet-drafts@ietf.org: I-D Action: draft-grothoff-iesg-special-use-p2p-names-00.txt]," IETF Mail Archive, December 1, 2013,

https://mailarchive.ietf.org/arch/msg/dnsop/wu_uAtNaUieZ5Tb2imJEzW4F5vM; Andrew Sullivan, "[DNSOP] More complete review of draft-grothoff-iesg-special-use-p2p-names-01," IETF Mail Archive, December 31, 2013, https://mailarchive.ietf.org/arch/msg/dnsop/WOlHdAKFxzBNS2dvyL7XD7qL-wo.

12. Arma [Roger Dingledine], "Facebook, Hidden Services, and HTTPS Certs," *Tor Blog*, October 31, 2014, https://blog.torproject.org/blog/facebook-hidden-services-and-https-certs.

13. Jeremy Rowley, "Supporting Anonymous Use of Facebook in Tor," *DigiCert Blog*, November 5, 2014, https://blog.digicert.com/anonymous-facebook-via-tor/.

14. Alec Muffett, "Making Connections to Facebook More Secure," Facebook, October 31, 2014, https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237.

15. See the e-mail threads starting here: Jeremy Rowley, "[Cabfpub] .onion and .exit," CAB Forum, October 14, 2014, https://cabforum.org/pipermail/public/2014-October/004210.html; Jeremy Rowley, "[Cabfpub] .onion proposal," CAB Forum, November 12, 2014, https://cabforum.org/pipermail/public/2014-November/004569.html.

16. Ben Wilson, "Ballot 144—Validation Rules for .onion Names," CAB Forum, February 18, 2015, https://cabforum.org/2015/02/18/ballot-144-validation-rules-dot-onion-names/.

17. Ibid.; Jeremy Rowley, "[Cabfpub] Ballot .onion ballot," CAB Forum, February 4, 2015, https://cabforum.org/pipermail/public/2015-February/004927.html.

18. Ted Lemon, “Re: [DNSOP] [internet-drafts@ietf.org: I-D Action: draft-grothoff-iesg-special-use-p2p-names-00.txt],” IETF Mail Archive, December 1, 2013, https://mailarchive.ietf.org/arch/msg/dnsop/Vzvevk2gO-WkT9fV6aO2bV3Cxno.

19. Andrew Sullivan, “Re: [DNSOP] On squatting and draft-grothoff-iesg-special-use-p2p-names,” IETF Mail Archive, January 6, 2014, https://mailarchive.ietf.org/arch/msg/dnsop/SEJSTssjHFCfXNxHU-hImrilLto.

20. “Frequently Asked Questions,” New Generic Top-Level Domains, ICANN, 2015, https://newgtlds.icann.org/en/applicants/global-support/faqs/faqs-en.

21. Paul Wouters, “Re: [DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt,” IETF Mail Archive, March 17, 2015, https://mailarchive.ietf.org/arch/msg/dnsop/FU9P4MyZGmY6XMqZdG4K1DhM-nY; Warren Kumari and Andrew Sullivan, “Draft-wkumari-dnsop-alt-tld: An ID reserving a TLD for non-DNS use,” GitHub, October 6, 2017, https://github.com/wkumari/draft-wkumari-dnsop-alt-tld.

22. Sullivan, “[DNSOP] More complete review.”

23. Paul Hoffman, “[DNSOP] On squatting and draft-grothoff-iesg-special-use-p2p-names,” IETF Mail Archive, January 2, 2014, https://mailarchive.ietf.org/arch/msg/dnsop/FYis10KCUisRKaEayA1gTysJAhM.

24. Warren Kumari, “Re: [DNSOP] [internet-drafts@ietf.org: I-D Action: draft-grothoff-iesg-special-use-p2p-names-00.txt],” IETF Mail Archive, December 2, 2013, https://mailarchive.ietf.org/arch/msg/dnsop/UuxpCgoYUm_lqCJg3HrrEMrwiL4.

25. Jacob Appelbaum and Alec Muffett, "The .onion Special-Use Domain Name draft-appelbaum-dnsop-onion-tld-00," IETF Datatracker, March 5, 2015, https://tools.ietf.org/html/draft-appelbaum-dnsop-onion-tld-00.

26. As I note in chapter 3, Appelbaum's reputation has recently been severely damaged by revelations that he has sexually harassed, assaulted, bullied, and intimidated multiple people over the past decade. For the purposes of this chapter's timeline, I will note that, at the time of "The .onion Special-Use Domain Name" proposal in 2015, Appelbaum was suspended from the Tor Project for ten days while the project investigated some of the accusations. He was later reinstated and able to contribute to the debates over what would become RFC 7686. In 2016 and well after 7686 was accepted, Appelbaum resigned from the Tor Project amid the allegations against him, though he protested that they were false. Later, the Tor Project hired a private investigator who confirmed multiple victims' allegations against Appelbaum. He was subsequently removed from many of the hacker organizations he was a part of. Until these victims were heard and believed, Appelbaum had used his influence—his status as a "legit" hacker—to abuse and harm others, who in turn have sought to take away the very source of his power: his status as a rock star hacker.

27. Appelbaum has the date wrong here: it was November 1, not October 1. In a later e-mail, Muffett corrects this timeline. See Alec Muffett, "[DNSOP] draft-appelbaum-dnsop-onion-tld-01 update (Was: Interim Meeting on Special Names and RFC 6761)," IETF Mail Archive, April 14, 2015, http://mailarchive.ietf.org/arch/msg/dnsop/eQu-slItK8-qxaIWx4y1F7puxKA; Jacob Appelbaum, "[DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt," IETF Mail Archive, March 16, 2015, http://mailarchive.ietf.org/arch/msg/dnsop/hJ-S6AdyH_SZJJSFD3XIAU95pGo.

28. Wouters, “Re: [DNSOP] Discussion for draft-appelbaum-dnsop-onion-tld-00.txt.”

29. Alec Muffett, “Re: [DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt,” IETF Mail Archive, March 17, 2015, https://mailarchive.ietf.org/arch/msg/dnsop/KZ6uzYQsu4pdFIvR7KXhskuud7k.

30. Jacob Appelbaum and Alec Muffett, “Diff: draft-appelbaum-dnsop-onion-tld-00.txt / draft-appelbaum-dnsop-onion-tld-01.txt,” IETF Datatracker, April 14, 2015, https://www.ietf.org/rfcdiff?url1=draft-appelbaum-dnsop-onion-tld-00&url2=draft-appelbaum-dnsop-onion-tld-01.

31. Stephane Bortzmeyer, “Re: [DNSOP] On squatting and draft-grothoff-iesg-special-use-p2p-names,” IETF Mail Archive, January 6, 2014, https://mailarchive.ietf.org/arch/msg/dnsop/PkLpWrAv7-mHV-EhWC_JZHgiPpI; Nicholas Weaver, “Re: [DNSOP] On squatting and draft-grothoff-iesg-special-use-p2p-names,” IETF Mail Archive, January 6, 2014, https://mailarchive.ietf.org/arch/msg/dnsop/NaNLlarsPibaUrOxYKbkLNlEYCE.

32. “Ballot for draft-ietf-dnsop-onion-tld-01,” IETF Datatracker, September 3, 2015, https://datatracker.ietf.org/doc/rfc7686/ballot/; Jacob Appelbaum and Alec Muffett, “The ‘.onion’ Special-Use Domain Name” (Request for Comments, Internet Engineering Task Force, September 9, 2015), https://tools.ietf.org/html/draft-ietf-dnsop-onion-tld-01.

33. Christian Grothoff, “Re: [DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt,” IETF Mail Archive, March 17, 2015, https://mailarchive.ietf.org/arch/msg/dnsop/9vWYbbczGNzr7ZPLUaqzjZdCSNY.

34. David Conrad, “Re: [DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt.” IETF Mail Archive, March 17, 2015, https://mailarchive.ietf.org/arch/msg/dnsop/ozSKRA8ZyN02zcjqBAh25STwQR8.

35. Christian Grothoff, “Re: [DNSOP] P2P Names Draft 03,” IETF Mail Archive, June 30, 2015, https://mailarchive.ietf.org/arch/msg/dnsop/jEU4fPnBhRjmBr7vbU02e7iDVa8; Christian Grothoff, “Re: [DNSOP] draft-grothoff-iesg-special-use-p2p-bit,” IETF Mail Archive, November 22, 2015, https://mailarchive.ietf.org/arch/msg/dnsop/JRwVmezuniDEDoraADgSZHX0BKQ.

36. George Michaelson, “Draft-michaelson-dnsop-rfc6761-is-closed,” IETF Datatracker, February 22, 2016, https://datatracker.ietf.org/doc/draft-michaelson-dnsop-rfc6761-is-closed/00/?include_text=1.

37. Zzz, “.I2p Domain Registration with IETF.”

38. Zzz, “31C3 Trip Reports,” Zzz.I2P forum, January 2, 2015, http://zzz.i2p/topics/1777?page=1#p9092 [I2P].

39. Zzz, “.I2p Domain Registration with IETF.”

40. “I2P Development Meeting 240,” I2P: The Invisible Internet Project, November 3, 2015, https://geti2p.net/en/meetings/240; str4d, “Re: [DNSOP] Requesting WGLC of draft-grothoff-iesg-special-use-p2p-*,” IETF Mail Archive, October 2, 2015, http://mailarchive.ietf.org/arch/msg/dnsop/1Nf4IYPw8zi2m0k6Oq-oSaqu9pA.

41. Zzz, “6761 Was a Mistake,” Zzz.I2P forum, March 11, 2016, http://zzz.i2p/topics/2101?page=1#p12019 [I2P].

42. Zzz, “.I2p Domain Registration with IETF.”

43. “Terms of Service,” Facebook, accessed July 21, 2017, https://www.facebook.com/legal/terms.

44. Krueger, interview by author, November 1, 2014.

45. Arma [Roger Dingledine], "Facebook, Hidden Services." See also Paul Syverson and Griffin Boyce, "Bake in .onion for Tear-Free and Stronger Website Authentication," *IEEE Security and Privacy* 14, no. 2 (March 2016): 15–21, doi:10.1109/MSP.2016.33. Indeed, new Tor hidden service users are increasingly taking to Reddit and other forums to ask about the lack of HTTPS in their browsers.

46. According to the *Tor Blog*, this was a "regression" due to an upgrade in the underlying Firefox codebase. In subsequent releases, this warning was removed. See boklm, "Tor Browser 7.0.4 Is released," *Tor Blog*, August 8, 2017, https://blog.torproject.org/tor-browser-704-released.

47. This is a repetition of what Ben Klemens laments about HTTPS on the Clear Web: "An HTTPS requirement means that you have to check with a bureaucrat before you post code you wrote to the world." Ben Klemens, "HTTPS: The End of an Era," *Medium* (blog), May 6, 2015, https://medium.com/@b_k/https-the-end-of-an-era-c106acded474.

48. Arma [Roger Dingledine], "Facebook, Hidden Services."

49. Eileen Ormsby has an entertaining writeup about Dark Web red rooms. Alongside hitmen for hire and most weapons sales, they are scams. Eileen Ormsby, "Waiting in the Red Room," *All Things Vice* (blog), August 29, 2015, https://allthingsvice.com/2015/08/29/waiting-in-the-red-room/.

50. Craig Silverman and Lawrence Alexander, "How Teens in the Balkans Are Duping Trump Supporters with Fake News," *BuzzFeed*, November 3, 2016, https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

51. Emil Protalinski, "Child Porn Photos Traded on Facebook in Plain Sight (Report)," *ZDNet*, May 7, 2012, http://www.zdnet.com/article/child-porn-photos-traded-on-facebook-in-plain-sight-report/. Still, there is no doubt that child exploitation is far more prevalent on the Dark Web than on Facebook. For example, Playpen, a Tor-based child exploitation site, reportedly had over 215,000 registered users and distributed 50,000 images. See Cyrus Farivar, "Creator of Infamous Playpen Website Sentenced to 30 Years in Prison," *Ars Technica*, May 5, 2017, https://arstechnica.com/tech-policy/2017/05/creator-of-infamous-playpen-website-sentenced-to-30-years-in-prison/.

52. Neetzan Zimmerman, "The Day Child Porn Went Viral on Facebook," *Gawker*, March 22, 2013, http://gawker.com/5991876/the-day-child-porn-went-viral-on-facebook.

53. Thomas James Brennan, "Hundreds of Marines Investigated for Sharing Photos of Naked Colleagues," *Reveal*, March 4, 2017, https://www.revealnews.org/blog/hundreds-of-marines-investigated-for-sharing-photos-of-naked-colleagues/.

54. David Mielach, "Terrorists Seek Out 'Friends' on Facebook," *Yahoo News*, January 9, 2012, https://www.yahoo.com/news/terrorists-seek-friends-facebook-184606693.html.

55. Ananya Bhattacharya, "Facebook's New Marketplace Is Already Flooded with Illegal Guns, Drugs, Sex, and Wildlife," *Quartz*, October 4, 2016, https://qz.com/799943/facebooks-fb-new-marketplace-is-already-flooded-with-illegal-guns-drugs-sex-and-wildlife/.

56. C. J. Chivers, "Facebook Groups Act as Weapons Bazaars for Militias," *New York Times*, April 6, 2016, http://www.nytimes.com/2016/04/07/world/middleeast/facebook-weapons-syria-libya-iraq.html.

57. Reuters News Agency, "Thai Man Broadcasts Daughter's Murder on Facebook, Then Takes His Own Life," *Telegraph*, April 25, 2017, http://www.telegraph.co.uk/news/2017/04/25/thai-man-broadcasts-daughters-murder-facebook-takes-life/; Joe Tacopino, "Man Wanted for Posting Murder on Facebook," *New York Post*, April 16, 2017, http://nypost.com/2017/04/16/man-wanted-for-broadcasting-murder-on-facebook-live/. See also the concluding chapter of Graham Denyer Willis, *The Killing Consensus: Police, Organized Crime, and the Regulation of Life and Death in Urban Brazil* (Oakland: University of California Press, 2015).

58. Fnanon, "What's your deep web story?" AskReddit, June 25, 2015, https://www.reddit.com/r/AskReddit/comments/3b0kwl/whats_your_deep_web_story/csijae9.

8 Conclusion

The Youth Liberation Front

In an interview in late 2015, one Dark Web site administrator told me about their first experiences on the Dark Web.[1] They first went to one of the Hidden Wikis, wikis that are used as link directories for Tor hidden services. These Hidden Wikis typically include brief descriptions of sites, allowing a new user to get a sense of the content hosted on the Tor network. As they recalled:

> When I entered [the Dark Web and saw a Hidden Wiki] … I was horrified over the fact that there are sites that host child porn and could serve to ruin or even kill innocent people, and surprised because I had no idea there were drug markets on the internet with so-called cryptocurrencies.

Thus, for this admin, many extramedial representations of the Dark Web held true, at least judging from the Hidden Wiki they visited: the Dark Web comprises illegitimate violence, illegal commerce, and sexual exploitation.

Despite the horrifying links found on the Hidden Wiki, however, this admin made a surprising decision: to found and moderate a (now defunct) Dark Web forum dedicated to youth rights, the Youth Liberation Front (YLF), which ran during most of 2015. As the YLF admin told me, the philosophy of the site was

> Liberation and justice for youth, basically. Support of teenagers to take decisions for themselves and have their opinions taken in consideration and their voices heard, exposure and denouncing of anti-youth oppression and double standards and mental and physical protection for kids that genuinely cannot consent to stuff. … [A world] without the insane amount of pressure they sometimes get from school, without being taught gender roles and other sort of brainwashing and negative social conditioning, without having to learn they're not safe from racism or sexualization and rape if they're black or women, without corporal punishment and without being taken advantage from abusive adults.

To build traffic to the YLF, the admin used Dark Web social networking sites to promote the site and recruit participants. There, the admin expressed their hopes for the YLF: that it would be a home for youth and youth rights activists to build on and contribute to previous social justice work on "women's rights, LGBT+ rights" while opposing "white and christian supremacy, discrimination against disabled folk, capitalism."

Reflecting these commitments, the YLF hosted frank discussions among self-described youth on topics such as dealing with abusive parents, foster parents, or bullies; handling the pressure of schoolwork; experiences with homelessness, depression, or dyslexia; and tactics for advancing a pro-youth rights agenda and how that agenda might link to feminist, pro-LGBTQ, or socialist politics. Members were respectful to one another, offering support and sharing their own experiences. As one participant put it, "This is helping me a lot because I see that I'm not alone in my misery and I can say things about my self that I never said [to] anyone before."

This site joined other, older Dark Web sites with similar goals: the Free Political Discussion Movement and the Free Speech Politics Index on Freenet, both of which collect political discussions and categorize them from far left to centrist to far right.[2] On the I2P network, sites such as Manifesto.i2p provided a space for people to write political manifestos. For a brief period, the queer spiritual

group the Radical Faeries established a home page on the Tor network.

These earlier sites likely were started because these networks were built, maintained, and used by people who adhered to the ideals of free speech, anticensorship, and protection of "the dissident," as I discuss in chapter 3. These values were associated with the anonymizing networks from their earliest days at the turn of this century. What makes the Youth Liberation Front remarkable is that it was built at a time—2015—when the Dark Web was associated with far less legitimate practices: sales of illegal items and the exchange of child exploitation images (CEIs). This was a time right after the Silk Road drug bust, as well as the Playpen CEI site bust in February 2015.[3] For the YLF admin, the idea that the Dark Web (specifically Tor hidden services) was to be used for these practices and not the ideals of the network builders was no doubt reinforced by the listings they saw on a Hidden Wiki.

In light of this, I asked the YLF admin: Why would the Dark Web be a place for a forum dedicated to youth rights? Especially when one of the key associations people make with the term Dark Web is child pornography?

> Because the real world and even the clear web in some degree are very hostile and dangerous towards minors in general due to this social and political structure that makes it very easy to dehumanize them. Hosting [the Youth Liberation Front] in the Dark Web not only provides youth a way to have a safe space from anti-youth laws and abusive adults that could harm them and share whatever they want anonymously, but it also motivates them to use tools like Tor to protect themselves. [In addition], YLF does not support child pornography, nor any sort of porn that isn't consensual. This site also prohibits any sort of porn (be it consensual or not) to make it a more pleasant place for everyone who does not need to see it.

Expanding Communicative Possibilities

With the example of the Youth Liberation Front in mind, in this conclusion I want to think through a question I asked in chapter 2 and offer some of my own answers: What is the role, if any, for the Dark Web in our contemporary media environment? Can it be a legitimated communication technology? Can it survive its trial of legitimacy?

The previous chapter shows one possible answer: the Dark and Clear can be brought together, linked through previously legitimated corporate sites such as Facebook. The Tor Project's pursuit of official recognition for its top-level domain (.onion) demonstrates one path toward legitimacy. Indeed, this is what security researchers Daniel Moore and Thomas Rid argue for: either the increase of known, vetted, legitimated Clear Web services, such as Facebook, ProPublica, DuckDuckGo, and the *New York Times*, into the Dark Web (specifically, into Tor hidden services), or the outright elimination of the Dark Web altogether because it can be used for illegal practices.[4]

But in this chapter, I want to consider another way toward legitimacy for the Dark Web: its potential for marginalized social justice advocates to build anonymized digital networks where they can socialize, develop political theories, and discuss ways to put their ideas into practice.

The Dark Web serves as a technological and political alternative to the Clear Web in that its emphasis on dissociating one's activities from one's identity is a direct challenge to the increasing surveillance and monitoring of all other digital activities. One can take to Tor, Freenet, or I2P to write about politics with far less fear of state reprisal or professional consequences. Writing in 2002—in the shadow of the Global War on Terror, and not long after Freenet began—legal scholar Yaman Akdeniz argued, "Anonymity and the use of strong encryption tools can help to preserve political

discourse and dissemination of information related to human rights abuses in the Information Age."[5] More recently, political theorist Trevor Garrison Smith argues in *Politicizing Digital Space* that

> the ability to protect one's private identity online by engaging politically through a pseudonym can enhance conflictual political engagement as the lack of repercussions in one's private life leads to people being more willing to express dissent and unpopular opinions. … When dissent threatens the security of one's body, then the ability to speak politically requires mechanisms to hide bodily identity. Pseudonymity helps ensure that a wide range of views can be expressed publicly by protecting those with outsider opinions from the tyranny of the majority and from state repression.[6]

Akdeniz and Smith are interested in how the Internet can increase the sort of civil debate communication scholar Zizi Papacharissi theorizes, where "civility" means "respect for the collective traditions of democracy," including heated, passionate, robust debate that acknowledges other subjects while furthering societal goals.[7] "Because the absence of face-to-face communication fosters discussion that is more heated," Papacharissi argues, "cyberspace actually promotes [Jean-François] Lyotard's vision of democratic emancipation through disagreement and anarchy."[8] Civil disagreement, passion, and dissent are needed for this Internet-mediated vision of politics, and anonymous/pseudonymous online discourse can support those styles of discourse.

In addition, Smith also argues that many contemporary political discussions are shut down when one participant delegitimizes another based on identity, as in "You can't speak about this topic because you are [white, black, poor, liberal, conservative, Jewish, Muslim, male, female, trans*, a child, etc.]." Such disqualifications, he argues, are antipolitical, stopping political debate before it can even begin, because participants predetermine their reaction to one another based on bodily or political identities.[9] Speakers are also delegitimized because they are not "real" (legit, authentic) members

of a group they purport to belong to. Again, Smith suggests dissociating ideas from embodied identity as a means around this form of short-circuiting debate.

By drawing on Papacharissi's definition of civil debate and suggesting that Akdeniz and Smith are correct in arguing that we need at least some anonymous/pseudonymous channels to foster such civil debate, I realize I'm taking part in a long-standing argument. On the one side stand those who argue that we need to anchor politics in our personal identities. This side sees politics as furthered only by those willing to stand up; put their bodies, names, and identities behind their opinions; and thus face consequences for their unpopular views. Those who hold this view argue that hiding behind a pseudonym or anonymity is at best ineffective because no one is putting a body on the line, and at worst tantamount to political cowardice. On the other side are those—certainly many who develop and use Dark Web sites—who argue for channels to speak unpopular views without identifying oneself. This is especially true when making a statement can lead to being subject to state violence.

This is not a new debate, and it will no doubt continue to happen with no resolution. Of course, there are situations where placing one's body/identity on the line furthers a political agenda; simply consider the Black Lives Matter movement, especially in the face of fascists in Charlottesville, Virginia, or the Indigenous American protests against the Dakota Access Pipeline. But bodily politics does not exhaust what is possible; it does not have to be at the exclusion of Akdeniz's and Smith's points about pseudonyms/anonymity allowing for free expression and the development of new political ideas.

In other words, we cannot even have this identity versus anonymity debate *at all* if every statement made could be anchored in an identity, which is what is increasingly possible as more communication is channeled through digital networks subject to state and corporate surveillance. Today, to speak online without the protections offered by anonymizing networks increasingly means having those statements linked back to oneself. As Zygmunt

Bauman and colleagues write in the wake of the Edward Snowden revelations of U.S. National Security Agency surveillance,

> The subject of surveillance is now a subject whose communicative practices are seen by the surveillance agencies as of potential informational value or utility, where this value might be related to security or the economy. It is hence not that we are all suspects now, but rather that our data inputs and networks might be deemed of value, understood in terms of utility, at some point in the future.[10]

To this end, agencies such as the NSA have constructed massive server farms to collect Internet traffic for later analysis.

And corporate surveillance is just as widespread on the Clear Web, with Internet service providers, corporate social media platforms, search engines, market sites, mobile operating systems, and advertisers all developing increasingly granular profiles of us as we browse, like, tweet, and use networked devices. Much as in Bauman and colleagues' discussion of government surveillance, corporate surveillance develops large archives of our communication for future analysis, hoping to use these data to produce messages and interfaces that modulate us toward consumer goods and services.[11]

Fusions of state and corporate surveillance are also possible, as demonstrated by the U.S. Department of Justice (DOJ) warrant for DreamHost data.[12] DreamHost, a web-hosting company, offers server space to customers. In the normal course of its operations, the company logs access to these servers. Logging access helps with server management, but it is also a stream of valuable business information used to manage DreamHost's customer base.[13] In the DOJ's efforts to identify and arrest political protesters, it also sees value in this information: it has demanded that DreamHost surrender "over 1.3 million visitor IP addresses—in addition to contact information, email content, and photos of thousands of people—in an effort to determine who simply visited" an anti-Trump protest site.[14]

In other words, in monitored networks, any reading habits or published statements of ours *may* be of value to a government agency or corporation in the future, which is why state and corporate actors are building big data archives of online activities as well as the knowledge practices to mine these data for security or profit. Even seemingly anonymous statements made on the Clear Web can be deanonymized using combinations of IP addresses, device identifiers, deep packet inspection, server logs, and other tracking tools.

Of course, such habits and statements are far more valuable if they can be *immediately* anchored to our identities. Indeed, we link our Internet use to our identities quite willingly by signing into Facebook or Google, using Google's or Apple's growing ecosystem of operating systems and devices, supplying our credit card information to online merchants, signing up for hosting services, or tacitly agreeing to allow Internet service providers or mobile networks the ability to monitor what we do online. Thus, as digital ethnographers Monica J. Barratt and Alexia Maddox argue, "The overall trend is towards an identified and authenticated internet."[15] This includes not only our browsing habits, but also our publishing habits: what we write online and the positions we take can be quickly traced to our identities.

The extent and depth of online surveillance is such that we see people colloquially discuss how "Google knows everything about me," or "Facebook knows me better than my mother," or "I hope the NSA is getting off on our conversation." Scholars of surveillance have long warned us of the effects of such monitoring: our discussions will become more docile as we internalize the gaze of those who monitor us. In light of this seemingly inevitable anchoring of statements in bodies, our digital communication may not be able to achieve the ideal Smith and Papacharissi call for: the use of anonymity to allow for unpopular ideas to be aired.

Freenet, Tor, and I2P were designed for this purpose. At the very least, their existence alongside the monitored Internet enables us to imagine politics anchored in bodies/identities *and* in anonymous

communication. As Gabriella Coleman eloquently puts it in the epilogue to her book about the hacker group Anonymous,

> Masking, so often thought of in negative terms—as shirking responsibility or hiding—can also enable a positive, constructive ethics of interacting and of being-in-the-world that runs counter to state, corporate, or colonial interests. Indeed, this right embodies a series of defiant, principled refusals: a refusal to allow that state to track its citizens; a refusal to allow corporations to convert personal communications into profit or manipulate their personal desires; a refusal to capitalize off each other's labor; a refusal, in essence, to prevent a powerful idea—that we are and can be anonymous—from withering away.[16]

Without alternative, anonymized networks, our digital political discourse immediately gets linked to our bodies, exposing us to the power of legitimated state violence. Without the anonymizing networks, our ability to think about communication and politics is instantly delimited.

The Dark Web's Trial of Legitimacy Continues

Of course, anonymizing networks do not necessarily bring about new political discourse in and of themselves. We cannot indulge in what Matteo Pasquinelli has aptly called "digitalism": "The widespread belief that Internet-based communication can be free from any form of exploitation and will naturally evolve towards a society of equal peers."[17] As Moore and Rid argue, "Too many activists treat cryptography as if it were a godlike force for good" while turning a blind eye to the bad purposes to which such technologies can be put.[18] Security researchers and law enforcement agencies repeatedly make one argument about the Dark Web: much of its content is illegitimate. Despite the struggles of the network builders, of search engine operators who build filtered search engines, or of social media administrators like Galaxy2's Lameth, who try to cultivate a largely civil user base, all three Dark Web systems remain in a trial of legitimacy across all three levels covered in this book precisely because people do host Dark Web sites with illegitimate violence (coercion and blackmailing, child exploitation), illegitimate sales, and cultures in which to be an authentic member means taking harassment and incivility to their extremes. In surveys of Dark Web content, security researchers consistently argue that the majority of Dark Web sites are dedicated to illegal activities.[19] The latest black eye is the migration of the alt-right Nazi site the *Daily Stormer* to Tor hidden services, after that site's previous Clear Web hosts refused to continue to host it.[20] Thus, as Moore and Rid argue, because of "the widespread and highly visible abuse" of Dark Web systems, they are an "easy target" for criticism.[21] Indeed, a recent CIGI/Ipsos survey of Internet users showed strong support for shutting down the Dark Web, and security researchers such as Daniel Moore, Thomas Rid, and Clarence Guitton echo this stance.[22]

Shutting down all three anonymizing networks, Freenet, Tor, and I2P, is unlikely, given that they are global open-source software projects. What is more likely is that law enforcement will become increasingly successful at investigating and prosecuting Dark Web crimes.[23] The global operation to seize the AlphaBay and Hansa markets, described in the postscript to chapter 4, shows the sophistication of law enforcement's investigative skills—which is to say, it shows the value of patient, detailed police work. Past operations, such as those that took down the child exploitation site Playpen, or current efforts to arrest purveyors of CEI on Freenet, seek to chase out what one Dark Web site admin called the "true black sheep" of these networks. Indeed, police are no longer merely arresting Dark Web administrators and users; they are also publicizing their presence on the networks. An example is the Dutch National Prosecution Service, which was instrumental in the takeover of Hansa market: it now hosts a Tor hidden service listing recent arrests of drug vendors as well as vendors it is targeting.[24] Yet even as the service succeeds in arresting drug vendors, information thieves, and CEI purveyors, law enforcement press releases and the subsequent media coverage continue the extramedial representation of the Dark Web as *entirely* illegitimate.

So the question of the role of the Dark Web in our contemporary media environment is not answered simply by considering the existence of anonymizing networks. The Dark Web won't legitimate itself. Anonymity alone is not the answer, and if the networks are perceived to be useful only for child exploitation and the sale of stolen information, then that's what they will be used for. Rather, we have to consider the full range of uses to which Dark Webs are put. We have to theorize the work of legitimating these networks. In this book, I have suggested that a fully legitimate Dark Web site would be able to work within the parameters of the three legitimacies, constructing the perceptions that they reject delegitimated violence, or—and this is obviously extremely contentious—that they allow speech that challenges a state's claims to its monopoly on violence. Based on my analysis of OPSEC politics

in chapter 4, I suggest that such sites should refrain from discourses of "weaponized" communication or other military metaphors for cyberspace since these expand, rather than challenge, state power. In addition, legitimate Dark Web sites must develop respect for their command of resources, whether they be informational, monetary, or labor. Corporate surveillance of the Internet and the transformation of our sociality into profit must continue to be rejected in favor of an alternative political economy of resource sharing and collaboration. And perhaps most difficult of all, legit Dark Web sites must develop means for fairly adjudicating the inclusion and exclusion of participants. This is the case for any site that seeks to foster the civil, political discourse Smith and Papacharissi are calling for. If more Freenet freesites, Tor hidden services, or I2P eepsites are put to this purpose, and not to exploitation, then the Dark Web's legitimacy as a channel for anonymous political communication can be realized, and the Dark Web can be legitimated.

In other words, if more activists and social justice organizations take advantage of Dark Web technologies, the Dark Web's claim to legitimacy will be strengthened. This is precisely what the admin of the Youth Liberation Forum chose. Like so many others before them, the YLF admin's first confrontation with the Dark Web was with listings for its most exploitative and illegitimate sites. They would have been right to turn away from these networks. But rather than dismiss anonymizing networks because of these problems, they chose to develop a site of civil political dissent dealing with controversial topics, such as children seeking emancipation from abusive parents and schools. Through a mixture of legitimacy exchange and delegitimation, the YLF sought social justice in the dark. From denouncing illegitimate violence in the form of anti-youth laws, CEIs, and abusive parents, to using forum software to organize a Dark Web site and enable authentic communication among like-minded participants, the YLF sought to balance the legitimacies I have explored throughout the book. Their decision to do so reflected a belief that there are no Clear Web sites where vulnerable participants could remain anonymous and thus

physically safe to express dissent, that the Clear Web was not a legitimate communications system for the ideas they wanted to engage with. These concerns echo those of the network builders, as well as contemporary political and communication theorists, who see anonymity of both readers and producers of content as offering a means for new political and social ideas to emerge.

Sites such as the YLF, political indexes on Freenet, search engines with curated indexes, or social networking sites Galaxy2, Visibility.i2p, or Freenet's Sone are often overlooked when people condemn the Dark Web as entirely composed of illegitimate content. They are also overlooked when people praise the Dark Web for attracting legitimated Clear Web sites such as Facebook, as if corporate social media is the only thing that can save the Dark. But these sites and services can realize the original goals of the network builders: enabling new political speech that is not possible in corporate- or state-monitored networks. If Dark Web administrators and users work together to develop legitimacy across all three registers and foster new political movements that challenge a growing tide of hate and exploitation, the Dark Web can succeed in its public trial of legitimacy. They may make for an "alternative Dark Web," an alternative to the received mythology of horrifying content as well as to the state-based or corporate-based means to clean it up.

New political ways of thinking cannot emerge from the currently legitimated. They will emerge from the marginalized, the overlooked, those still struggling for legitimacy, still grappling with the daunting problems of violence, propriety, and authenticity. For those on the margins, taking to the Dark Web to develop their organizations and challenge the new hegemony of hate and exploitation may make sense. More such sites must appear across Freenet, Tor, and I2P for these anonymizing networks to realize their legitimate potential. More such people should choose to do what the YLF admin did: contribute something legitimate—in all its meanings—to these networks.

Notes

1. I use they/their for pronouns for this interviewee, who was interviewed in the summer of 2015.

2. "FPDM," Free Political Discussion Movement, May 1, 2013, http://127.0.0.1:8888/USK@3Qf7agO4suQrcE9WFLBLNpyCT6vvyuUCeOcn3WpPACk,cupodkdmRR-g1GrRpD3xwpn0GZO6KuDrjQWgsFFBmaE,AQACAAE/fpdm-political/0/[Freenet]; FSP: Free Speech Politics Index, May 11, 2015, http://127.0.0.1:8888/SSK@BnORZ0QmOceBmSlwZ32-RQe~bS-0aW42Ad6G7cn-ixU,qr69TrWH4EajfUaUtBKt1dhQz8JYJjC7toTK9QYFxG8,AQACAAE/index-18/[Freenet].

3. Cyrus Farivar, "Creator of Infamous Playpen Website Sentenced to 30 Years in Prison," *Ars Technica*, May 5, 2017, https://arstechnica.com/tech-policy/2017/05/creator-of-infamous-playpen-website-sentenced-to-30-years-in-prison/.

4. Daniel Moore and Thomas Rid, "Cryptopolitik and the Darknet," *Survival* 58, no. 1 (January 2, 2016): 7–38, doi:10.1080/00396338.2016.1142085.

5. Yaman Akdeniz, "Anonymity, Democracy, and Cyberspace," *Social Research* 69, no. 1 (2002): 224.

6. Trevor Garrison Smith, *Politicizing Digital Space* (London: University of Westminster Press, 2017), 60–61, doi:10.16997/book5.

7. Zizi Papacharissi, "Democracy Online: Civility, Politeness, and the Democratic Potential of Online Political Discussion Groups," *New Media and Society* 6, no. 2 (April 1, 2004): 261, doi:10.1177/1461444804041444.

8. Ibid., 267.

9. Smith, *Politicizing Digital Space*, 48.

10. Zygmunt Bauman et al., "After Snowden: Rethinking the Impact of Surveillance," *International Political Sociology* 8, no. 2 (June 1, 2014): 138, doi:10.1111/ips.12048.

11. Robert W. Gehl, "The Archive and the Processor: The Internal Logic of Web 2.0," *New Media and Society* 13, no. 8 (December 2011): 1228–1244; Keller Easterling, "Disposition," in *Cognitive Architecture: From Bio-Politics to Noo-Politic, Architecture and Mind in the Age of Communication and Information*, ed. Deborah Hauptmann and Warren Neidich (Rotterdam: 010 Publishers, 2010), 250–265.

12. "Superior Court of the District of Columbia Search Warrant," July 12, 2017, https://www.dreamhost.com/blog/wp-content/uploads/2017/08/DH-Search-Warrant.pdf.

13. "Privacy Policy," DreamHost, July 21, 2017, https://www.dreamhost.com/legal/privacy-policy/.

14. DreamHost, "We Fight for the Users," DreamHost.blog, August 14, 2017, https://www.dreamhost.com/blog/we-fight-for-the-users/.

15. Monica J. Barratt and Alexia Maddox, "Active Engagement with Stigmatised Communities through Digital Ethnography," *Qualitative Research* 16, no. 6 (May 22, 2016): 703, doi:10.1177/1468794116648766.

16. Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (New York: Verso, 2014): 426.

17. Matteo Pasquinelli, *Animal Spirits: A Bestiary of the Commons* (Rotterdam: NAi Publishers, 2008), 65.

18. Moore and Rid, "Cryptopolitik and the Darknet," 29.

19. For example, Clement Guitton, "A Review of the Available Content on Tor Hidden Services: The Case against Further Development," *Computers in Human Behavior* 29, no. 6 (November 2013): 2805–2815, doi:10.1016/j.chb.2013.07.031. For an analysis on the prevalence of child exploitation images on Freenet, see Brian N. Levine et al., "Statistical Detection of Downloaders in Freenet," *Proc. IEEE International Workshop on Privacy Engineering*, San Jose, CA, May 2017, http://ceur-ws.org/Vol-1873/IWPE17_paper_12.pdf. For the latest condemnation of I2P (although it's bereft of actual data on the amount of illegal content on that network), see Behnam Bazli, Maxim Wilson, and William Hurst, "The Dark Side of I2P, a Forensic Analysis Case Study," *Systems Science and Control Engineering* 5, no. 1 (2017): 278–286. These surveys are not accepted by all, however; search engine operator Juha Nurmi, for example, has repeatedly argued that his indexes do not reveal the oft-claimed high number of illegal sites.

20. Joseph Cox, "After Shutdown, Daily Storm Users Are Moving to a Dark Web Version of Site," *Motherboard*, August 15, 2017, https://motherboard.vice.com/en_us/article/evvxvz/white-supremacist-website-daily-stormer-goes-offline.

21. Moore and Rid, "Cryptopolitik and the Darknet," 29.

22. Centre for International Governance Innovation and Ipsos, *2016 CIGI-Ipsos Global Survey on Internet Security and Trust* (Waterloo, ON: CIGI and Ipsos, 2016), https://www.cigionline.org/internet-survey-2016; "Global Poll: Dark Web Should Be Banned," PYMNTS.com, March 19, 2016, http://www.pymnts.com/news/security-and-risk/2016/ipsos-poll-dark-web-should-be-banned/.

23. Eric Jardine, "The Dark Web Dilemma: Tor, Anonymity and Online Policing," last updated November 23, 2015 (Paper series, Global Commission on Internet Governance, Waterloo, Ontario,

2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711.

24. The Dutch police Tor hidden service can be found at politiepcvh42eav.onion [Tor].

Bibliography

0x90 [Lance James] and DC. “Media > DC Interview Part 1.” Invisible IRC Project, July 26, 2002. https://web.archive.org/web/20021006073454/http://www.invisiblenet.net/iip/mediaDCInterview1.php.

“A Distributed Decentralised Information Storage and Retrieval System.” Freenet Development Page, October 13, 1999. https://web.archive.org/web/19991013120144/http://freenet.on.openprojects.net/.

Abel, Marc. “TorPark mirrors and China.” Tor-talk mailing list, September 26, 2005. https://lists.torproject.org/pipermail/tor-talk/2005-September/017938.html.

Afilipoaie, Alois, and Patrick Shortis. *From Dealer to Doorstep–how Drugs Are Sold on the Dark Net*. GDPO Situation Analysis. Wales: Swansea University, Global Drugs Policy Observatory, 2015. http://www.swansea.ac.uk/media/Dealer%20to%20Doorstep%20FINAL%20SA.pdf.

“#Agora IRC Server.” Anarplex. Last updated 2013. https://anarplex.net/agorairc/.

Agorism: Revolutionary Market Anarchism. Freesite based on www.agorism.info, December 20, 2016. http://127.0.0.1:8888/USK@fIkEtTMu6F3f7Y48dB4mmZiyFbB-iddMGBvtruSE3Vc,sFg1GrDfJ-k6BE8VmqqQjw~iOgOKu-aws8law90GeY8,AQACAAE/agorism/13/ [Freenet].

Akdeniz, Yaman. “Anonymity, Democracy, and Cyberspace.” *Social Research* 69, no. 1 (2002): 223–237.

Akrich, Madeleine. “The De-Scription of Technical Objects.” In *Shaping Technology/Building Society*, edited by Wiebe Bijker

and John Law, 205–224. Cambridge, MA: MIT Press, 1992.
Albrecht, Michael Mario. “Acting Naturally Unnaturally: The Performative Nature of Authenticity in Contemporary Popular Music.” *Text and Performance Quarterly* 28, no. 4 (October 1, 2008): 379–395. doi:10.1080/10462930802351989.
Aldridge, Judith, and David Décary-Hétu. “Hidden Wholesale: The Drug Diffusing Capacity of Online Drug Cryptomarkets.” *International Journal on Drug Policy* 35 (September 2016): 7–15. doi:10.1016/j.drugpo.2016.04.020.
Alford, C. Fred. “What Would It Matter If Everything Foucault Said about Prison Were Wrong? Discipline and Punish after Twenty Years.” *Theory and Society* 29, no. 1 (2000): 125–146.
Allen, Myria Watkins, and Rachel H. Caillouet. “Legitimation Endeavors: Impression Management Strategies Used by an Organization in Crisis.” *Communication Monographs* 61, no. 1 (1994): 44–62.
“Alphabay statement on PMs bug (fixed now).” Pastebin, January 23, 2017. http://pastebin.com/9whZbnVi.
anarcho47. “What Is the Goal of Silk Road?” Silk Road forums, Darknet market archives, September 5, 2011. https://www.gwern.net/DNM-archives.
Andersen, Rasmus Munksgaard. “Intersections of Drug Dealing and Politics—A Macroanalysis of Cryptomarket Discourse.” Master’s thesis, Copenhagen University, 2015. https://diskurs.kb.dk/item/diskurs:96023:1/component/diskurs:96022/DiskursVersion.pdf.
Ansell-Pearson, Keith. *An Introduction to Nietzsche as Political Thinker: The Perfect Nihilist*. New York: Cambridge University Press, 1994.
Anspach, Whitney, Kevin Coe, and Crispin Thurlow. “The Other Closet?: Atheists, Homosexuals and the Lateral Appropriation of Discursive Capital.” *Critical Discourse Studies* 4, no. 1 (April 2007): 95–119. doi:10.1080/17405900601149509.
Appelbaum, Jacob. “[DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt.” IETF Mail Archive, March 16, 2015.

http://mailarchive.ietf.org/arch/msg/dnsop/hJ-S6AdyH_SZJJSFD3XIAU95pGo.
Appelbaum, Jacob. "[Tor-dev] Registering special-use domain names of peer-to-peer name systems with IETF." Tor-dev mailing list archives, November 9, 2013. https://lists.torproject.org/pipermail/tor-dev/2013-November/005763.html.
Appelbaum, Jacob, and Alec Muffett. "Diff: Draft-appelbaum-dnsop-onion-tld-00.txt / draft-appelbaum-dnsop-onion-tld-01.txt." IETF Datatracker, April 14, 2015. https://www.ietf.org/rfcdiff?url1=draft-appelbaum-dnsop-onion-tld-00&url2=draft-appelbaum-dnsop-onion-tld-01.
Appelbaum, Jacob, and Alec Muffett. "The '.onion' Special-Use Domain Name." Request for Comments. Internet Engineering Task Force, September 9, 2015. https://tools.ietf.org/html/draft-ietf-dnsop-onion-tld-01.
Appelbaum, Jacob, and Alec Muffett. "The. onion Special-Use Domain Name draft-appelbaum-dnsop-onion-tld-00." IETF Datatracker, March 5, 2015. https://tools.ietf.org/html/draft-appelbaum-dnsop-onion-tld-00.
Archer, Louise. "Younger Academics' Constructions of 'Authenticity,' 'Success' and Professional Identity." *Studies in Higher Education* 33, no. 4 (2008): 385–403.
Arma [Roger Dingledine]. "Facebook, Hidden Services, and HTTPS Certs." *Tor Blog*, October 31, 2014. https://blog.torproject.org/blog/facebook-hidden-services-and-https-certs.
Ashforth, Blake E., and Barrie W. Gibbs. "The Double-Edge of Organizational Legitimation." *Organization Science* 1, no. 2 (1990): 177–194.
Aupers, Stef. "'Trust No One': Modernization, Paranoia and Conspiracy Culture." *European Journal of Communication* 27, no. 1 (2012): 22–34. doi:10.1177/0267323111433566.
Babenhauserheide, Arne. "[Freenet-dev] Security Quibbles Was Re: Freenet Canary." Freenet-dev mailing list archives, November 30, 2015.

https://emu.freenetproject.org/pipermail/devl/2015-November/038645.html.
"Ballot for draft-ietf-dnsop-onion-tld-01." IETF Datatracker, September 3, 2015. https://datatracker.ietf.org/doc/rfc7686/ballot/.
Bancroft, Angus, and Peter Scott Reid. "Challenging the Techno-Politics of Anonymity: The Case of Cryptomarket Users." *Information Communication and Society* 20, no. 4 (April 3, 2017): 497–512. doi:10.1080/1369118X.2016.1187643.
Banet-Weiser, Sarah. *Authentic™: Politics and Ambivalence in a Brand Culture*. New York: New York University Press, 2012.
Barker, Rodney. *Legitimating Identities: The Self-Presentations of Rulers and Subjects*. New York: Cambridge University Press, 2001.
Barlow, John Perry. "A Declaration of the Independence of Cyberspace." Electronic Frontier Foundation, February 8, 1996. https://projects.eff.org/~barlow/Declaration-Final.html
Barnes, Connelly. "Chinese Firewall Circumvention." Gmane.network.i2p mailing list archives, October 6, 2005.
Barratt, Monica J., and Judith Aldridge. "Everything You Always Wanted to Know about Drug Cryptomarkets* (*But Were Afraid to Ask)." *International Journal on Drug Policy* 35 (September 2016): 1–6. doi:10.1016/j.drugpo.2016.07.005.
Barratt, Monica J., Jason A. Ferris, and Adam R. Winstock. "Safer Scoring? Cryptomarkets, Social Supply and Drug Market Violence." *International Journal on Drug Policy* 35 (September 2016): 24–31. doi:10.1016/j.drugpo.2016.04.019.
Barratt, Monica J., and Alexia Maddox. "Active Engagement with Stigmatised Communities through Digital Ethnography." *Qualitative Research* 16, no. 6 (May 22, 2016): 701–719. doi:10.1177/1468794116648766.
Bartlett, Jamie. *The Dark Net: Inside the Digital Underworld*. London: Windmill Books, 2014.
Bartmanski, Dominik, and Ian Woodward. "The Vinyl: The Analogue Medium in the Age of Digital Reproduction." *Journal*

of Consumer Culture 15, no. 1 (March 1, 2015): 3–27. doi:10.1177/1469540513488403.
Battelle, John. *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. New York: Portfolio, 2005.
Bauman, Zygmunt, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, and R. B. J. Walker. "After Snowden: Rethinking the Impact of Surveillance." *International Political Sociology* 8, no. 2 (June 1, 2014): 121–144. doi:10.1111/ips.12048.
Bazli, Behnam, Maxim Wilson, and William Hurst. "The Dark Side of I2P, a Forensic Analysis Case Study." *Systems Science and Control Engineering* 5, no. 1 (2017): 278–286.
Bendix, Regina. *In Search of Authenticity: The Formation of Folklore Studies*. Madison: University of Wisconsin Press, 1997.
Benjamin, Walter. "The Work of Art in the Age of Mechanical Reproduction." Marxists Internet Archive, February 2005. http://www.marxists.org/reference/subject/philosophy/works/ge/benjamin.htm.
Benkler, Yochai. "Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate." *Harvard Civil Rights–Civil Liberties Law Review* 46 (2011): 311.
Bergman, Michael K. "The Deep Web: Surfacing Hidden Value." *Journal of Electronic Publishing* 7, no. 1 (2001). http://quod.lib.umich.edu/cgi/t/text/idx/j/jep/3336451.0007.104/--white-paper-the-deep-web-surfacing-hidden-value?rgn=main;view=fulltext.
Berton, Beatrice. *The Dark Side of the Web: ISIL's One-Stop Shop?* EUISS Alert. Paris: European Union Institute for Security Studies, June 2015. http://www.iss.europa.eu/uploads/media/Alert_30_The_Dark_Web.pdf.
Beyer, Jessica L. *Expect Us: Online Communities and Political Mobilization*. New York: Oxford University Press, 2014.
Beyer, Jessica and Fenwick McKelvey. "You Are Not Welcome Among Us: Pirates and the State." *International Journal of*

Communication 9 (2015): 890–908. http://ijoc.org/index.php/ijoc/article/view/3759.
Bhattacharya, Ananya. “Facebook’s New Marketplace Is Already Flooded with Illegal Guns, Drugs, Sex, and Wildlife.” *Quartz*, October 4, 2016. https://qz.com/799943/facebooks-fb-new-marketplace-is-already-flooded-with-illegal-guns-drugs-sex-and-wildlife/.
Blue, Violet. “The Myth of Mariana’s Web, the Darkest Corner of the Internet.” *Engadget*, December 18, 2015. https://www.engadget.com/2015/12/18/the-myth-of-marianas-web-the-darkest-corner-of-the-internet/.
Boellstorff, Tom. *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*. Princeton, NJ: Princeton University Press, 2008.
Bogost, Ian, and Nick Montfort. “Platform Studies: Frequently Questioned Answers.” Paper presented at the Digital Arts and Culture Conference 2009: After Media—Embodiment and Context, UC Irvine, 2009.
boklm. “Tor Browser 7.0.4 Is Released.” *Tor Blog*, August 8, 2017. https://blog.torproject.org/tor-browser-704-released.
Bolter, Jay David, and Richard Grusin. *Remediation: Understanding New Media*. Cambridge, MA: MIT Press, 2003.
Bombe. “JSite.” Freenet Wiki, September 1, 2006. https://old-wiki.freenetproject.org/FreenetJsite?time=2006-09-01+18%3A08%3A42.
Bortzmeyer, Stephane. “[DNSOP] [internet-drafts@ietf.org: I-D Action: draft-grothoff-iesg-special-use-p2p-names-00.txt].” IETF Mail Archive, December 1, 2013. https://mailarchive.ietf.org/arch/msg/dnsop/wu_uAtNaUieZ5Tb2imJEzW4F5vM.
Bortzmeyer, Stephane. “Re: [DNSOP] On squatting and draft-grothoff-iesg-special-use-p2p-names.” IETF Mail Archive, January 6, 2014. https://mailarchive.ietf.org/arch/msg/dnsop/PkLpWrAv7-mHV-EhWC_JZHgiPpI.

Bourdieu, Pierre. *The Field of Cultural Production: Essays on Art and Literature*. New York: Columbia University Press, 1993.
Bourricaud, François. "Legitimacy and Legitimization." *Current Sociology* 35, no. 2 (1987): 57–67.
Bowan, Kate. "R. G. Collingwood, Historical Reenactment and the Early Music Revival." In *Historical Reenactment: From Realism to the Affective Turn*, edited by Iain McCalman and Paul Pickering, 134–158. London: Palgrave Macmillan, 2010.
Bowker, G. "How to Be Universal: Some Cybernetic Strategies, 1943–70." *Social Studies of Science* 23, no. 1 (1993): 107–127.
Bowles, Samuel, and Herbert Gintis. "Contested Exchange: New Microfoundations for the Political Economy of Capitalism." In *The Economic Nature of the Firm: A Reader*, edited by Louis Putterman and Randy Kroszner, 217–232. Cambridge: Cambridge University Press, 1996.
Branwen, Gwern, Nicolas Christin, David Décary-Hétu, Rasmus Munksgaard, and El Presidente StExo. "Darknet Market Archives (2013–2015)." Gwern.Net, December 1, 2013. https://www.gwern.net/DNM-archives.
Bratich, Jack. "User-Generated Discontent." *Cultural Studies* 25 (September 2011): 621–640. doi:10.1080/09502386.2011.600552.
Brennan, Thomas James. "Hundreds of Marines Investigated for Sharing Photos of Naked Colleagues." *Reveal*, March 4, 2017. https://www.revealnews.org/blog/hundreds-of-marines-investigated-for-sharing-photos-of-naked-colleagues/.
Brown, Steven D. "Michel Serres: Science, Translation and the Logic of the Parasite." *Theory, Culture and Society* 19, no. 3 (2002). doi:10.1177/0263276024010815O3.
Bush, Vannevar. "As We May Think." *Atlantic Monthly*, July 1945.
Callon, Michel. "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay." In *Power, Action, and Belief: A New Sociology of Knowledge?* edited by John Law, 169–233. Boston: Routledge and Kegan Paul, 1986.

Centre for International Governance Innovation and Ipsos. *2016 CIGI-Ipsos Global Survey on Internet Security and Trust*. Waterloo, ON: CIGI/Ipsos, 2016. https://www.cigionline.org/internet-survey-2016.
Chadwell, Sean. "Inventing That 'Old-Timey' Style: Southern Authenticity in O Brother, Where Art Thou?" *Journal of Popular Film and Television* 32, no. 1 (2004): 2–9.
Chaum, David L. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms." *Communications of the ACM* 24, no. 2 (1981): 84–90.
Chen, Adrian. "The Underground Website Where You Can Buy Any Drug Imaginable." *Gawker*, June 1, 2011. http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.
Chen, Hsinchun. *Dark Web—Exploring and Data Mining the Dark Side of the Web*. New York: Springer, 2012. http://www.springer.com/computer/database+management+%26+information+retrieval/book/978-1-4614-1556-5.
Chen, Hsinchun, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman, and Gabriel Weimann. "Uncovering the Dark Web: A Case Study of Jihad on the Web." *Journal of the American Society for Information Science and Technology* 59 no. 8 (2008): 1347–1359.
Cheng, Vincent John. *Inauthentic: The Anxiety over Culture and Identity*. Piscataway, NJ: Rutgers University Press, 2004.
Cheshire, Stuart, and Marc Krochmal. "Multicast DNS, RFC 6762." IETF Datatracker, February 20, 2013. https://datatracker.ietf.org/doc/rfc6762/.
Chivers, C. J. "Facebook Groups Act as Weapons Bazaars for Militias." *New York Times*, April 6, 2016. http://www.nytimes.com/2016/04/07/world/middleeast/facebook-weapons-syria-libya-iraq.html.
Chun, Wendy Hui-Kyong. *Control and Freedom: Power and Paranoia in the Age of Fiber Optics*. Cambridge, MA: MIT Press, 2006.

Clarke, Adele. *Situational Analysis: Grounded Theory after the Postmodern Turn*. London: Sage, 2018.
Clarke, Ian. "Creating Websites in Freenet." Freenet Project, December 14, 2000. https://web.archive.org/web/20001214054400/http://freenetproject.org/index.php?page=authoring.
Clarke, Ian. "A Distributed Decentralised Information Storage and Retrieval System." Master's thesis, University of Edinburgh, 1999. http://www.decuslib.com/DECUS/vmslt00a/net/freenet.pdf.
Clarke, Ian. "[Freehaven-dev] [Freenet-chat] Interesting commentary on Freenet from Freehaven." Freenet-dev and Freenet-chat mailing list archives, September 27, 2000. http://archives.seul.org//freehaven/dev/Sep-2000/msg00010.html.
Clarke, Ian. "[Freenet-dev] Fuzzy search." Freenet-dev mailing list archives, May 14, 2000. https://web.archive.org/web/20141117114016/https://emu.freenetproject.org/pipermail/devl/2000-May/001681.html.
Clarke, Ian, Scott G. Miller, Theodore W. Hong, Oskar Sandberg, and Brandon Wiley. "Protecting Free Expression Online with Freenet." *IEEE Internet Computing* 6, no. 1 (2002): 40–49. http://ieeexplore.ieee.org/document/978368/?reload=true.
Coleman, E. Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso, 2014.
collapses. "To Dread Pirate Roberts." Silk Road forums, Darknet market archives, May 4, 2013. https://www.gwern.net/DNM-archives.
Colleoni, Elanor. "CSR Communication Strategies for Organizational Legitimacy in Social Media." *Corporate Communications* 18, no. 2 (2013): 228–248.
Comey, James. "Encryption, Public Safety, and 'Going Dark.'" *Lawfare* (blog), July 6, 2015. http://www.lawfareblog.com/encryption-public-safety-and-going-dark.

Conrad, David. “Re: [DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt.” IETF Mail Archive, March 17, 2015. https://mailarchive.ietf.org/arch/msg/dnsop/ozSKRA8ZyN02zcjqBAh25STwQR8.
Couts, Andrew. “TorSearch Makes Finding the Next Silk Road a Lot Easier.” *Digital Trends*, October 11, 2013. http://www.digitaltrends.com/web/torsearch-tor-network-hidden-services/.
Cox, Joseph. “After Shutdown, Daily Storm Users Are Moving to a Dark Web Version of Site.” *Motherboard*, August 15, 2017. https://motherboard.vice.com/en_us/article/evvxvz/white-supremacist-website-daily-stormer-goes-offline.
Cox, Joseph. “DOJ, FBI Executives Approved Running a Child Porn Site.” *Motherboard*, May 29, 2017. https://motherboard.vice.com/en_us/article/doj-fbi-child-pornography-sting-playpen-court-transcripts.
Cox, Joseph. “It’s Time to Stop Comparing Exploits to Physical Weapons.” *Motherboard*, July 17, 2017. https://motherboard.vice.com/en_us/article/mbaxxv/its-time-to-stop-comparing-exploits-to-physical-weapons.
“Crime Problems.” Ugha.I2p (wiki), February 23, 2015. http://ugha.i2p/CrimeProblems [I2P].
Currid-Halkett, Elizabeth. *Sum of Small Things: A Theory of the Aspirational Class*. Princeton, NJ: Princeton University Press, 2017.
Czarniawska, Barbara, and Tor Hernes. “Constructing Macro Actors According to ANT.” In *Actor-Network Theory and Organizing*, edited by Barbara Czarniawska and Tor Hernes, 7–13. Copenhagen: Copenhagen Business School Press, 2005.
Décary-Hétu, David, Masarah Paquet-Clouston, and Judith Aldridge. “Going International? Risk Taking by Cryptomarket Drug Vendors.” *International Journal on Drug Policy* 35 (September 2016): 69–76. doi:10.1016/j.drugpo.2016.06.003.
Decker, Stephanie. “Corporate Legitimacy and Advertising: British Companies and the Rhetoric of Development in West

Africa, 1950–1970." *Business History Review* 81, no. 1 (April 2007): 59–86. doi:10.1017/S0007680500036254.
DeepDotWeb. "Grams: Becoming Hub for DarkNet Info & Ads (Part 1)." *Deep Dot Web*, May 31, 2014. https://www.deepdotweb.com/2014/05/31/introducing-grams-infodesk-features-part-1/.
DeGenevieve, Barbara. "Ssspread.Com: The Hot Bods of Queer Porn." In *C'lickme: A Netporn Studies Reader*, edited by Katrien Jacobs, Marije Janssen, and Matteo Pasquinelli, 233–236. Amsterdam: Institute of Network Cultures, 2007.
Denyer Willis, Graham. *The Killing Consensus: Police, Organized Crime, and the Regulation of Life and Death in Urban Brazil*. Oakland: University of California Press, 2015.
Dickey, Jack, and Timothy Burke. "Manti Te'o's Dead Girlfriend, the Most Heartbreaking and Inspirational Story of the College Football Season, Is a Hoax." *Deadspin*, January 16, 2013. http://deadspin.com/manti-teos-dead-girlfriend-the-most-heartbreaking-an-5976517.
Dickinson, Greg. "Joe's Rhetoric: Finding Authenticity at Starbucks." *Rhetoric Society Quarterly* 32, no. 4 (2002): 5–27.
Dingledine, Roger R. "The Free Haven Project: Design and Deployment of an Anonymous Secure Data Haven." Master's thesis, Massachusetts Institute of Technology, 2000. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.71.3453&rep=rep1&type=pdf.
Dingledine, Roger. "[Freehaven-dev] Initial musings on the next Free Haven (part one of two)." Freehaven-dev mailing list archives, April 15, 2001. http://archives.seul.org/freehaven/dev/Apr-2001/msg00007.html.
Dingledine, Roger. "(FWD) [or-cvs] a new TODO file with more details." Freehaven.net or-cvs mailing list archives, February 13, 2003. http://archives.seul.org/or/dev/Feb-2003/msg00009.html.
Dingledine, Roger. "Hidden-ssh, irc, ftp, etc etc via socat." Freehaven.net or-dev mailing list archives, April 16, 2004.

http://archives.seul.org/or/dev/Apr-2004/msg00013.html.
Dingledine, Roger. “Name change: or -> tor.” Freehaven.net or-dev mailing list archives, February 3, 2002. http://archives.seul.org/or/dev/Sep-2002/msg00009.html.
Dingledine, Roger. “[Or-cvs] Our program is now called ‘tor’, not ‘or.’” Freehaven.net or-cvs mailing list archives, September 3, 2002. http://archives.seul.org/or/cvs/Sep-2002/msg00011.html.
Dingledine, Roger. “Pre-alpha: run an onion proxy now!” Freehaven.net or-dev mailing list archives, September 20, 2002. http://archives.seul.org/or/dev/Sep-2002/msg00019.html.
Dingledine, Roger. “Re: [Freehaven-dev] re: chapters done—moving forward options.” Freehaven-dev mailing list archives, December 14, 2000. http://archives.seul.org//freehaven/dev/Dec-2000/msg00009.html.
Dingledine, Roger. “Re: [Freehaven-dev] Re: [Freenet-chat] MojoNation.” Freehaven-dev mailing list archives, August 10, 2000. http://archives.seul.org//freehaven/dev/Aug-2000/msg00018.html.
Dingledine, Roger. “Re: I2P (was Re: Psiphon (Was: Bootstraping Tor manually to get past the Great Firewall)).” Or-talk mailing list archives, December 4, 2006. http://archives.seul.org/or/talk/Dec-2006/msg00050.html.
Dingledine, Roger. “Remove faq and hacking files too. they’re now in doc.” Tor’s Source Code, March 18, 2003. https://gitweb.torproject.org/tor.git/commit/?id=f9c541bfcf886248e809d198b19fb1e2e97b924e.
Dingledine, Roger, Michael J. Freedman, and David Molnar. “The Free Haven Project: Distributed Anonymous Storage Service.” In *Designing Privacy Enhancing Technologies*, edited by Hannes Federrath, 67–95. Vol. 2009 of Lecture Notes in Computer Science. Berlin/Heidelberg: Springer, 2001. http://link.springer.com/chapter/10.1007/3-540-44702-4_5.
Dingledine, Roger, Nick Mathewson, and Paul Syverson. “Reputation in P2P Anonymity Systems.” Paper presened at

Workshop on Economics of Peer-to-Peer Systems, Berkeley, CA, 2003. http://mail.freehaven.net/anonbib/cache/rep-anon.pdf.
Dingledine, Roger, Nick Mathewson, and Paul Syverson. "Tor: Next-Generation Onion Routing." Poster presented at CodeCon, San Francisco, 2004. https://web.archive.org/web/20041204074542/http://tor.freehaven.net/slides-codecon04/.
Dingledine, Roger, and Paul Syverson. "Reliable MIX Cascade Networks through Reputation." In *Financial Cryptography*, edited by Matt Blaze, 253–268. Berlin: Springer, 2002. http://link.springer.com/chapter/10.1007/3-540-36504-4_18.
Dolliver, Diana S. "Evaluating Drug Trafficking on the Tor Network: Silk Road 2, the Sequel." *International Journal on Drug Policy* 26, no. 11 (November 2015): 1113–1123. doi:10.1016/j.drugpo.2015.01.008.
Doublehelix. "Admins: Make PGP Compulsory? (Please?)." Silk Road forums, Darknet market archives, November 28, 2012. https://www.gwern.net/DNM-archives.
Dread Pirate Roberts. "***DPR's Book Club***." Silk Road forums, Darknet market archives, August 14, 2012. https://www.gwern.net/DNM-archives.
Dread Pirate Roberts. "If Prohibition Is Lifted." Silk Road forums, Darknet market archives, April 29, 2012. https://www.gwern.net/DNM-archives.
DreamHost. "We Fight for the Users." DreamHost.blog, August 14, 2017. https://www.dreamhost.com/blog/we-fight-for-the-users/.
Du, Shuili, and Edward T. Viera Jr. "Striving for Legitimacy Through Corporate Social Responsibility: Insights from Oil Companies." *Journal of Business Ethics* 110, no. 4 (September 27, 2012): 413–427. doi:10.1007/s10551-012-1490-4.
Duffy, Brooke Erin. "Manufacturing Authenticity: The Rhetoric of 'Real' in Women's Magazines." *Communication Review* 16, no. 3 (July 1, 2013): 132–154. doi:10.1080/10714421.2013.807110.

Easterling, Keller. “Disposition.” In *Cognitive Architecture: From Bio-Politics to Noo-Politics, Architecture and Mind in the Age of Communication and Information*, edited by Deborah Hauptman and Warren Neidich, 250–265. Rotterdam: 010 Publishers, 2010.
Elmer, Greg. *Profiling Machines: Mapping the Personal Information Economy*. Cambridge, MA; London: MIT Press, 2004.
Emirbayer, Mustafa, and Eva M. Williams. “Bourdieu and Social Work.” *Social Service Review* 79, no. 4 (2005): 689–724.
Fairhurst, Gail T., and François Cooren. “Leadership as the Hybrid Production of Presence (S).” *Leadership* 5, no. 4 (2009): 469–490.
Farivar, Cyrus. “Creator of Infamous Playpen Website Sentenced to 30 Years in Prison.” *Ars Technica*, May 5, 2017. https://arstechnica.com/tech-policy/2017/05/creator-of-infamous-playpen-website-sentenced-to-30-years-in-prison/.
Fenris. “To the Shutdown of Dark Matters.” Galaxy2, November 18, 2016. http://w363zoq3ylux5rf5.onion/blog/view/160082/to-the-shutdown-of-dark-matters [Tor].
Finlay, Christopher J. “Legitimacy and Non-State Political Violence.” *Journal of Political Philosophy* 18, no. 3 (September 1, 2010): 287–312. doi:10.1111/j.1467-9760.2009.00345.x.
Fnanon. “What’s your deep web story?” AskReddit, June 25, 2015. https://www.reddit.com/r/AskReddit/comments/3b0kwl/whats_your_deep_web_story/csijae9.
Foxton, Willard. “If Silk Road Was a Legitimate Startup, It Would Be Worth ~$2.4 Billion.” *Business Insider*, October 4, 2013. http://www.businessinsider.com/silk-road-valuation-worth-2-or-3-billion-2013-10.
“The Free Haven Project.” Free Haven, April 9, 2003. https://web.archive.org/web/20030409042914/http://www.freehaven.net/.

FreenetUser. “About AFKindex.” March 2008. http://127.0.0.1:8888/USK@2L-k2U32b3yIl2~YjBU7--QJPTtixSwJHZxYOuGjS3A0,QJBd6zpJgEsijJGQNNcwUhsrW5vJ8VtlmNX5ka2~d [Freenet].
“Frequently Asked Questions.” New Generic Top-Level Domains, ICANN, 2015. https://newgtlds.icann.org/en/applicants/global-support/faqs/faqs-en.
Friz, Amanda, and Robert W. Gehl. “Pinning the Feminine User: Gender Scripts in Pinterest’s Sign-up Interface.” *Media Culture and Society* 38, no. 5 (July 1, 2016): 686–703. doi:10.1177/0163443715620925.
Fuller, Matthew, and Andrew Goffey. “Digital Infrastructures and the Machinery of Topological Abstraction.” *Theory, Culture and Society* 29, nos. 4–5 (July 1, 2012): 311–333. doi:10.1177/0263276412450466.
Furgalj at lakeviewtech.com. “[Freenet-chat] Re: [Freenet-support] Showdown at the Freenode Coral.” Freenet-chat mailing list, August 7, 2004. https://emu.freenetproject.org/pipermail/chat/2004-August/001250.html.
Galison, Peter. “The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision.” *Critical Inquiry* 21 (Autumn 1994): 228–266.
Gehl, Robert W. “The Archive and the Processor: The Internal Logic of Web 2.0.” *New Media and Society* 13, no. 8 (December 2011): 1228–1244.
Gehl, Robert W. “Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network.” *New Media and Society* (October 16, 2014): 1–17.
Gehl, Robert W. *Reverse Engineering Social Media: Software, Culture, and Political Economy in New Media Capitalism*. Philadelphia, PA: Temple University Press, 2014.
Gehl, Robert W., and Brian Cozen. “Passé Media: Communication and Transportation on Commuter and

Computer Buses." *Communication Theory* 25, no. 3 (March 1, 2015). doi:10.1111/comt.12056.
GetYourFix. "REQUEST:Making Pgp a Requirement for a Buyer's Account?" Silk Road forums, Darknet market archives, December 9, 2012. https://www.gwern.net/DNM-archives.
Gillespie, Iain. "Cyber Cops Probe the Deep Web." *Age*, October 24, 2013. First edition, sec. Green Guide.
"Global Poll: Dark Web Should Be Banned." PYMNTS.com, March 19, 2016. http://www.pymnts.com/news/security-and-risk/2016/ipsos-poll-dark-web-should-be-banned/.
Goh, Gabey. "Unpeeling the Dark Web with OnionCity." *Digital News Asia*, March 24, 2015. https://www.digitalnewsasia.com/digital-economy/unpeeling-the-dark-web-with-onioncity.
Goldschlag, David M., Michael G. Reed, and Paul F. Syverson. "Hiding Routing Information." In *Information Hiding*, edited by Ross Anderson, 137–150. Berlin: Springer, 1996. http://link.springer.com/10.1007/3-540-61996-8_37.
Greenberg, Andy. "Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)." *Forbes*, March 21, 2012. http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/.
Grothoff, Christian. "Re: [DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt." IETF Mail Archive, March 17, 2015. https://mailarchive.ietf.org/arch/msg/dnsop/9vWYbbczGNzr7ZPLUaqzjZdCSNY.
Grothoff, Christian. "Re: [DNSOP] draft-grothoff-iesg-special-use-p2p-bit." IETF Mail Archive, November 22, 2015. https://mailarchive.ietf.org/arch/msg/dnsop/JRwVmezuniDEDoraADgSZHXoBKQ.
Grothoff, Christian. "Re: [DNSOP] [internet-drafts@ietf.org: I-D Action: draft-grothoff-iesg-special-use-p2p-names-00.txt]." IETF Mail Archive, December 1, 2013.

https://mailarchive.ietf.org/arch/msg/dnsop/5TOdxaQzDFLhF4zenKndoR7PVVg.
Grothoff, Christian. “Re: [DNSOP] P2P Names Draft 03.” IETF Mail Archive, June 30, 2015. https://mailarchive.ietf.org/arch/msg/dnsop/jEU4fPnBhRjmBr7vbU02e7iDVa8.
Grothoff, Christian. “[Tor-dev] Registering special-use domain names of peer-to-peer name systems with IETF.” Tor-dev mailing list archives, November 6, 2013. https://lists.torproject.org/pipermail/tor-dev/2013-November/005747.html.
Grothoff, Christian, Matthias Wachs, Hellekin Wolf, and Jacob Appelbaum. “Special-Use Domain Names of Peer-to-Peer Systems.” IETF Datatracker, November 13, 2013. https://tools.ietf.org/id/draft-grothoff-iesg-special-use-p2p-names-00.txt.
Guitton, Clement. “A Review of the Available Content on Tor Hidden Services: The Case against Further Development.” *Computers in Human Behavior* 29, no. 6 (November 2013): 2805–2815. doi:10.1016/j.chb.2013.07.031.
Gusterson, Hugh. “Ethnographic Research.” In *Qualitative Methods in International Relations*, edited by Audie Klotz and Deepa Prakash, 93–113, Research Methods Series. Basingstoke, UK: Palgrave Macmillan, 2008.
Hadnagy, Christopher J., Mati Aharoni, and James O’Gorman. *Social Engineering Capture the Flag Results: Defcon 18*. N.p.: Social-Engineer.org, 2010. http://www.social-engineer.org/wp-content/uploads/2014/03/Social-Engineer_CTF_Report.pdf.
Haimson, Oliver L., and Anna Lauren Hoffmann. “Constructing and Enforcing ‘Authentic’ Identity Online: Facebook, Real Names, and Non-Normative Identities.” *First Monday* 21, no. 6 (June 10, 2016). http://firstmonday.org/ojs/index.php/fm/article/view/6791.
Hall, Dobkin. “Inventing the Non-Profit Sector, 1950–1990.” In *The Nature of the Nonprofit Sector*, edited by J. Steven Ott, 112–125. Boulder, CO: Westview Press, 2001.

"Hall of Fame." I2P: The Invisible Internet Project, September 1, 2016. https://geti2p.net/en/about/hall-of-fame.
Haraway, Donna. "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective." *Feminist Studies* 14, no. 3 (1988): 575–599.
Harper, David. "The Politics of Paranoia: Paranoid Positioning and Conspiratorial Narratives in the Surveillance Society." *Surveillance and Society* 5, no. 1 (2008): 1–32.
Hasian, Marouf, Sean T. Lawson, and Megan McFarlane. *The Rhetorical Invention of America's National Security State*. Lanham, MD: Lexington Books, 2015.
Hegtvedt, Karen A., and Cathryn Johnson. "Power and Justice: Toward an Understanding of Legitimacy." *American Behavioral Scientist* 53, no. 3 (November 1, 2009): 376–399. doi:10.1177/0002764209338798.
Heider, Ulrike. *Anarchism: Left, Right, and Green*. San Francisco: City Lights Books, 1994.
Herrmann, Michael, and Christian Grothoff. "Privacy-Implications of Performance-Based Peer Selection by Onion-Routers: A Real-World Case Study Using I2P." Presentation at the International Symposium on Privacy Enhancing Technologies, Waterloo, Ontario, July 29, 2011. http://grothoff.org/christian/teaching/2011/2194/i2p.odp.
Hine, Christine. *Virtual Ethnography*. Thousand Oaks, CA: SAGE, 2000.
Hoffman, Paul. "[DNSOP] On squatting and draft-grothoff-iesg-special-use-p2p-names." IETF Mail Archive, January 2, 2014. https://mailarchive.ietf.org/arch/msg/dnsop/FYis10KCUisRKaEayA1gTysJAhM.
Holstein, Michael. "Paid performance-tor option?" Tor-talk mailing list, August 18, 2008. https://lists.torproject.org/pipermail/tor-talk/2008-August/002283.html.
Hong, Theodore. "Freenet Keys for Testing." May 11, 2000. https://web.archive.org/web/20000511004840/http://longitude.doc.ic.ac.uk/keyindex.

Hunsinger, Jeremy. “Produsing the Hidden: Darknet Consummativities.” In *Produsing Theory in a Digital World 2.0,* edited by Rebecca Ann Lind, 57–73. New York: Peter Lang, 2015.
Hutcherson, Ben, and Ross Haenfler. “Musical Genre as a Gendered Process: Authenticity in Extreme Metal.” In *Studies in Symbolic Interaction*, vol. 35, edited by Norman K. Denzin, 101–121. Bingley, UK: Emerald Group Publishing, 2010. http://www.emeraldinsight.com/doi/abs/10.1108/S0163-2396(2010)0000035010.
Hutchings, Alice, and Thomas J. Holt. “The Online Stolen Data Market: Disruption and Intervention Approaches.” *Global Crime* 18, no. 1 (January 2, 2017): 11–30. doi:10.1080/17440572.2016.1197123.
“I2P Development Meeting 2.” I2P: The Invisible Internet Project, May 29, 2002. https://geti2p.net/en/meetings/2.
“I2P Development Meeting 47.” I2P: The Invisible Internet Project, July 1, 2003. https://geti2p.net/en/meetings/47.
“I2P Development Meeting 65.” I2P: The Invisible Internet Project, November 18, 2003. https://geti2p.net/en/meetings/65.
“I2P Development Meeting 68.” I2P: The Invisible Internet Project, December 9, 2003. https://geti2p.net/en/meetings/68.
“I2P Development Meeting 153.” I2P: The Invisible Internet Project, October 25, 2005. https://geti2p.net/en/meetings/153.
“I2P Development Meeting 240.” I2P: The Invisible Internet Project, November 3, 2015. https://geti2p.net/en/meetings/240.
“I2P Project Members.” I2P: The Invisible Internet Project, January 2016. https://geti2p.net/en/about/team.
“I2PCon 2015.” I2P: The Invisible Internet Project. Accessed September 15, 2016. https://geti2p.net/pt/about/i2pcon/2015.
“I2PCon Day 1: Growing the Network, Spreading the Word (August 15, 2015).” Presentation by zzz. YouTube video, 57:40, posted by KYTV at I2P, August 27, 2015. https://www.youtube.com/watch?v=2KbqgR3avqw.

I2Phreak. “Direct.i2p—New Search Engine.” Forum.i2p, April 11, 2016. forum.i2p/viewtopic.php?t=10685 [I2P].
“I2PTunnel.” I2P: The Invisible Internet Project, January 2016. https://geti2p.net/en/docs/api/i2ptunnel.
Infernal1. “Multiverse | Closing Message.” S-Map: The Social Media Alternatives Project, August 23, 2015. https://socialmediaalternatives.org/archive/items/show/164.
Jackson, Jonathan, Aziz Z. Huq, Ben Bradford, and Tom R. Tyler. “Monopolizing Force? Police Legitimacy and Public Attitudes toward the Acceptability of Violence.” *Psychology, Public Policy, and Law* 19, no. 4 (November 2013): 479–497. doi:10.1037/a0033852.
James, Lance. “About.” IIP—Invisible IRC Project, November 21, 2001. https://web.archive.org/web/20011121032730fw_/http://bovine.artificial-stupidity.net/~nop/iip/about.html.
James, Lance. “IIPv1 White Paper Revision 1.1.1.” December 2002. https://web.archive.org/web/20020110185425fw_/http://bovine.artificial-stupidity.net/~nop/iip/IIPabout.htm.
James, Lance. “Invisible IRC Project.” Presentation at CodeCon, San Francisco, February 16, 2002. http://invisibleip.sourceforge.net/iip/resources/iip_transcript.txt.
James, Lance. “Public Peer Review Request!” gmane.comp.security.invisiblenet.iip.devel mailing list archive, September 3, 2003.
Jancovich, Mark. “‘A Real Shocker’: Authenticity, Genre and the Struggle for Distinction.” *Continuum* 14, no. 1 (2000): 23–35.
Jardine, Eric. “The Dark Web Dilemma: Tor, Anonymity and Online Policing.” Paper Series, Global Commission on Internet Governance, Waterloo, Ontario, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2667711.
John, Nicholas A. *The Age of Sharing*. Malden, MA: Polity, 2017.
JohnGMcKinley. “What Do You See as the Future Implications of the Silk Road and Cypherpunk?” Silk Road forums, Darknet

market archives, August 18, 2013. https://www.gwern.net/DNM-archives.
Jrandom. “0.6.1.30 Release.” I2P: The Invisible Internet Project, October 7, 2010. https://geti2p.net/en/blog/post/2007/10/07/0.6.1.30-Release.
Jrandom. “I2p Project Overview Doc for the SDK.” Gmane mailing list archive, August 8, 2003. http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/344.
Jrandom. “Java Version + Signatures (Fwd: I2P Implementation Questions).” Gmane mailing list archive, August 1, 2003. http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/315.
Jrandom. “Jrandom’s Announcement.” I2P: The Invisible Internet Project, November 2007. https://geti2p.net/en/misc/jrandom-awol.
Jrandom. “Re: /. [How Chinese Evade Government’s Web Controls].” Gmane.network.i2p mailing list archives, November 27, 2005.
Jrandom. “Re: I2P Conspiracy Theories Flamewar.” Gmane.network.i2p mailing list archives, October 5, 2005.
Jrandom. “Sample Java Api.” Gmane mailing list archive, July 15, 2003. http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/280.
Jrandom. “Some Light Reading.” Gmane mailing list archive, July 7, 2003. http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/269.
Jrandom. “Two Quick Things to Consider before Tonights Meeting.” Gmane mailing list archive, July 8, 2003. http://permalink.gmane.org/gmane.comp.security.invisiblenet.iip.devel/271.
“Jrandom’s Old Collected Slogans.” I2PWiki, June 16, 2016. http://i2pwiki.i2p/index.php?

title=Jrandom%27s_old_collected_slogans [I2P].
Jung, Kwangho, and M. Jae Moon. “The Double-Edged Sword of Public-Resource Dependence: The Impact of Public Resources on Autonomy and Legitimacy in Korean Cultural Nonprofit Organizations.” *Policy Studies Journal* 35, no. 2 (May 1, 2007): 205–226. doi:10.1111/j.1541-0072.2007.00216.x.
Kadianakis, George. “[Tor-dev] Memorable onion addresses (was Discussion on the crypto migration plan of the identity keys of Hidden Services).” Tor-dev mailing list archives, May 19, 2013. https://lists.torproject.org/pipermail/tor-dev/2013-May/004884.html.
Kahf, Usama. “Arabic Hip Hop: Claims of Authenticity and Identity of a New Genre.” *Journal of Popular Music Studies* 19, no. 4 (2007): 359–385.
Kitchin, Rob, and Martin Dodge. *Code/Space: Software and Everyday Life*. Cambridge, MA: MIT Press, 2011.
Kleinberg, Jon M. “Navigation in a Small World.” *Nature* 406, no. 6798 (2000): 845.
Klemens, Ben. “HTTPS: The End of an Era.” *Medium* (blog), May 6, 2015. https://medium.com/@b_k/https-the-end-of-an-era-c106acded474.
König, René, and Miriam Rasch. “Reflect and Act!: Introduction to the Society of the Query Reader.” In *Society of the Query Reader: Reflections on Web Search*, edited by René König and Miriam Rasch, 10–15. Amsterdam: Institute of Network Cultures, 2014.
König, René, and Miriam Rasch, eds. *Society of the Query Reader: Reflections on Web Search*. Amsterdam: Institute of Network Cultures, 2014.
Konkin, Samuel Edward, III. *An Agorist Primer*. Huntington Beach, CA: KoPubCo, 2008.
Konkin, Samuel Edward, III. “Interview with Samuel Edward Konkin III.” By _wlo:dek and michal. 2002. http://127.0.0.1:8888/freenet:USK@fIkEtTMu6F3f7Y48dB4mmZiyFbB-iddMGBvtruSE3Vc,sFg1GrDfJ-k6BE8VmqqQjw~iOgOKu-

aws8law90GeY8,AQACAAE/agorism/42/docs/konkin-interview.pdf [Freenet].
Konkin, Samuel Edward, III. "The Last, Whole Introduction to Agorism." *Agorist Quarterly* 1, no. 1 (1995): 3–10.
Konkin, Samuel Edward, III. *New Libertarian Manifesto*. Los Angeles: Koman Publishing, 1983. http://agorism.info/docs/NewLibertarianManifesto.pdf.
Koopman, Colin. *Genealogy as Critique: Foucault and the Problems of Modernity*. Bloomington: Indiana University Press, 2013.
Koopman, Colin, and Tomas Matza. "Putting Foucault to Work: Analytic and Concept in Foucaultian Inquiry." *Critical Inquiry* 39, no. 4 (June 2013): 817–840. doi:10.1086/671357.
Kopano, Baruti N. "Soul Thieves: White America and the Appropriation of Hip Hop and Black Culture." In *Soul Thieves*, edited by Tamara Lizette Brown and Baruti N. Kopano, 1–14. Contemporary Black History. New York: Palgrave Macmillan, 2014. doi:10.1057/9781137071392_1.
Kostakis, Vasilis, and Chris Giotitsas. "The (A)Political Economy of Bitcoin." *TripleC: Communication, Capitalism and Critique* 12, no. 2 (2014): 431–440.
Krochmal, Marc, and Stuart Cheshire. "Special-Use Domain Names." Request for Comments. Internet Engineering Task Force, February 2013. https://tools.ietf.org/html/rfc6761.
Kumari, Warren. "Re: [DNSOP] [internet-drafts@ietf.org: I-D Action: draft-grothoff-iesg-special-use-p2p-names-00.txt]." IETF Mail Archive, December 2, 2013. https://mailarchive.ietf.org/arch/msg/dnsop/UuxpCgoYUm_lqCJg3HrrEMrwiL4.
Kumari, Warren, and Andrew Sullivan. "Draft-wkumari-dnsop-alt-tld: An ID reserving a TLD for non-DNS use." GitHub, October 6, 2017. https://github.com/wkumari/draft-wkumari-dnsop-alt-tld.
Latzko-Toth, Guillaume. "The Socialization of Early Internet Bots." In *Socialbots and Their Friends: Digital Media and the*

Automation of Sociality, edited by Robert W. Gehl and Maria Bakardjieva, 47–68. New York: Routledge, 2016.
Law, John. *Aircraft Stories: Decentering the Object in Technoscience*. Durham, NC: Duke University Press, 2002.
Law, John. "Notes on the Theory of the Actor-Network: Ordering, Strategy, and Heterogeneity." *Systemic Practice and Action Research* 5, no. 4 (August 1992): 379–393. doi:10.1007/BF01059830.
Law, John. "On Hidden Heterogeneities: Complexity, Formalism, and Aircraft Design." In *Complexities: Social Studies of Knowledge Practices*, edited by John Law and Annemarie Mol, 116–141. Durham, NC: Duke University Press, 2002.
Law, John. "On Power and Its Tactics: A View from the Sociology of Science." *Sociological Review* 34, no. 1 (1986): 1–38.
Law, John. *Organizing Modernity*. Cambridge, MA: Blackwell, 1994.
Law, John, and Annemarie Mol, eds. *Complexities: Social Studies of Knowledge Practices*. Durham, NC: Duke University Press, 2002.
Lawson, Sean. "Putting the 'War' in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States." *First Monday* 17, no. 7 (2012). http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270.
Lawson, Sean. "The US Military's Social Media Civil War: Technology as Antagonism in Discourses of Information-Age Conflict." *Cambridge Review of International Affairs* 27, no. 2 (April 3, 2014): 226–245. doi:10.1080/09557571.2012.734787.
Lemon, Ted. "Re: [DNSOP] [internet-drafts@ietf.org: I-D Action: draft-grothoff-iesg-special-use-p2p-names-00.txt]." IETF Mail Archive, December 1, 2013. https://mailarchive.ietf.org/arch/msg/dnsop/Vzvevk2gO-WkT9fV6aO2bV3Cxno.

Levine, Brian N., Marc Liberatore, Brian Lynn, and Matthew Wright. “Statistical Detection of Downloaders in Freenet.” *Proc. IEEE International Workshop on Privacy Engineering*, San Jose, CA, May 2017. http://ceur-ws.org/Vol-1873/IWPE17_paper_12.pdf.
Levine, Yasha. “Almost Everyone Involved in Developing Tor Was (or Is) Funded by the US Government.” *Pando*, July 16, 2014. https://pando.com/2014/07/16/tor-spooks/.
Libicki, Martin C, David Senty, and Julia Pollak. *H4cker5 Wanted: An Examination of the Cybersecurity Labor Market*. Santa Monica, CA: RAND, 2014.
Loll, Anna Catherine. “Power, Secrecy and Cypherpunks: How Jacob Appelbaum Ripped Tor Apart.” *Guardian*, October 11, 2016, sec. Technology. https://www.theguardian.com/technology/2016/oct/11/jacob-appelbaum-tor-project-sexual-assault-allegations.
Lounsbury, Michael, and Mary Ann Glynn. “Cultural Entrepreneurship: Stories, Legitimacy, and the Acquisition of Resources.” *Strategic Management Journal* 22, no. 6–7 (June 1, 2001): 545–564. doi:10.1002/smj.188.
Luckmann, Thomas. “Comments on Legitimation.” *Current Sociology* 35, no. 2 (June 1, 1987): 109–117. doi:10.1177/001139287035002011.
Maddox, Alexia, Monica J. Barratt, Matthew Allen, and Simon Lenton. “Constructive Activism in the Dark Web: Cryptomarkets and Illicit Drugs in the Digital ‘Demimonde.’” *Information Communication and Society* 19, no. 1 (October 15, 2015): 1–16. doi:10.1080/1369118X.2015.1093531.
Mahon, Michael. *Foucault’s Nietzschean Genealogy: Truth, Power, and the Subject*. Albany: State University of New York Press, 1992.
Mallein, Philippe, and Yves Toussaint. “L’intégration Sociale Des Technologies d’information et de Communication: Une Sociologie Des Usages.” *Technologies de l’information et Société* 6, no. 4 (1994): 315–335.

Manivannan, Vyshali. “Tits or GTFO: The Logics of Misogyny on 4chan’s Random - /b/.” *Fibreculture*, no. 22 (2013). http://twentytwo.fibreculturejournal.org/fcj-158-tits-or-gtfo-the-logics-of-misogyny-on-4chans-random-b/.
Maréchal, Nathalie. “‘Use Signal, Use Tor?’: The Political Economy of Circumvention Technology.” PhD diss. in progress, University of Southern California.
Markoff, John. “Cyberspace Programmers Confront Copyright Laws.” *New York Times*, May 10, 2000, sec. A.
Martin, James. “Lost on the Silk Road: Online Drug Distribution and the ‘Cryptomarket.’” *Criminology and Criminal Justice* 14, no. 3 (2014): 351–367. doi:10.1177/1748895813505234.
Martin, James, and Nicolas Christin. “Ethics in Cryptomarket Research.” *International Journal on Drug Policy* 35 (September 2016): 84–91. doi:10.1016/j.drugpo.2016.05.006.
Marwick, Alice Emily. *Status Update: Celebrity, Publicity, and Branding in the Social Media Age*. New Haven, CT: Yale University Press, 2013.
Marwick, Alice E., and danah boyd. “I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience.” *New Media and Society*, July 2010. doi:10.1177/1461444810365313.
Mathewson, Nick. “Add first draft of rendezvous point document.” Tor’s Source Code, June 12, 2003. https://gitweb.torproject.org/tor.git/commit/?id=3d538f6d702937c23bec33b3bdd62ff9fba9d2a3.
Mattelart, Armand. *Networking the World, 1794–2000*. Translated by Liz Carey-Libbrecht and James A. Cohen Minneapolis: University of Minnesota Press, 2000.
Matthews, Chris. “The War on Drugs Comes to Corporate America.” *Fortune*, December 2, 2014. http://fortune.com/2014/12/02/drug-war-corporate-america-silk-road/.
McGee, Micki. *Self-Help, Inc.: Makeover Culture in American Life*. New York: Oxford University Press, 2005.

McGoogan, Cara. “Dark Web Browser Tor Is Overwhelmingly Used for Crime, Says Study.” *Telegraph*, February 2, 2016. http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/.
McGrath, Glenn. “[Freenet-Chat] Deep Philosophical Question.” Freenet Project, January 2, 2002. https://emu.freenetproject.org/pipermail/chat/2002-January/000604.html.
McNab, David. “[Freenet-chat] New Freenet Search Engine.” Freenet-chat mailing list archives, February 23, 2003. https://emu.freenetproject.org/pipermail/chat/2003-February/000631.html.
Meserko, Vincent M. “The Pursuit of Authenticity on Marc Maron’s WTF Podcast.” *Continuum* 29, no. 6 (November 2, 2015): 796–810. doi:10.1080/10304312.2015.1073682.
Metzler, Maribeth S. “Responding to the Legitimacy Problems of Big Tobacco: An Analysis of the ‘People of Philip Morris’ Image Advertising Campaign.” *Communication Quarterly* 49, no. 4 (September 1, 2001): 366–381. doi:10.1080/01463370109385636.
Michaelson, George. “Draft-michaelson-dnsop-rfc6761-is-closed.” IETF Datatracker, February 22, 2016. https://datatracker.ietf.org/doc/draft-michaelson-dnsop-rfc6761-is-closed/00/?include_text=1.
Mielach, David. “Terrorists Seek Out ‘Friends’ on Facebook.” *Yahoo News*, January 9, 2012. https://www.yahoo.com/news/terrorists-seek-friends-facebook-184606693.html.
Mol, Annemarie. “Cutting Surgeons, Walking Patients: Some Complexities Involved in Comparing.” In *Complexities: Social Studies of Knowledge Practices*, edited by John Law and Annemarie Mol, 218–257. Durham, NC: Duke University Press, 2002.
Montfort, Nick, and Ian Bogost. *Racing the Beam: The Atari Video Computer System*. Cambridge, MA: MIT Press, 2009.

Moore, Daniel, and Thomas Rid. “Cryptopolitik and the Darknet.” *Survival* 58, no. 1 (January 2, 2016): 7–38. doi:10.1080/00396338.2016.1142085.
Mr. Bad. “Get in on the Ground Floor of FREEDOM.” *Pigdog Journal* (blog), February 24, 2000. http://www.pigdog.org/auto/liberty/link/1264.html.
Muffett, Alec. “[DNSOP] draft-appelbaum-dnsop-onion-tld-01 update (Was: Interim Meeting on Special Names and RFC 6761).” IETF Mail Archive, April 14, 2015. http://mailarchive.ietf.org/arch/msg/dnsop/eQu-slItK8-qxaIWx4y1F7puxKA.
Muffett, Alec. “Making Connections to Facebook More Secure.” Facebook, October 31, 2014. https://www.facebook.com/notes/protect-the-graph/making-connections-to-facebook-more-secure/1526085754298237.
Muffett, Alec. “Re: [DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt.” IETF Mail Archive, March 17, 2015. https://mailarchive.ietf.org/arch/msg/dnsop/KZ6uzYQsu4pdFIvR7KXhskuud7k.
Mullin, Joe. “The Incredibly Simple Story of How the Gov’t Googled Ross Ulbricht.” *Ars Technica*, January 26, 2015. https://arstechnica.com/tech-policy/2015/01/the-incredibly-simple-story-of-how-the-govt-googled-ross-ulbricht/.
Munksgaard, Rasmus, and Jakob Demant. “Mixing Politics and Crime—The Prevalence and Decline of Political Discourse on the Cryptomarket.” *International Journal on Drug Policy* 35 (September 2016): 77–83. doi:10.1016/j.drugpo.2016.04.021.
Naylor, R. T. “Violence and Illegal Economic Activity: A Deconstruction.” *Crime, Law and Social Change* 52, no. 3 (September 1, 2009): 231–242. doi:10.1007/s10611-009-9198-9.
“New Child Legitimation Law a Success.” Georgia Department of Human Services, September 1, 2005. https://dhs.georgia.gov/new-child-legitimation-law-success.
“New Photos of Edward Snowden.” *Washington Post*, December 23, 2013. https://www.washingtonpost.com/world/national-

security/edward-snowden-says-his-missions-already-accomplished/2013/12/23/764e37fc-6c4c-11e3-aecc-85cb037b7236_gallery.html.
Newsbyte. "[Freenet-chat] [Freenet-dev] Censorship." Freenet-chat and Freenet-dev mailing lists, May 14, 2004. https://emu.freenetproject.org/pipermail/chat/2004-May/001267.html.
Nurmi, Juha. "Ahmia.Fi—Search Engine for Anonymous Hidden Services." Knight Foundation News Challenge, March 18, 2014. https://www.newschallenge.org/challenge/2014/submissions/ahmia-fi-search-engine-for-anonymous-hidden-services.
Nurmi, Juha. "Ahmia Search after GSoC Development." *Tor Blog*, September 14, 2014. https://blog.torproject.org/blog/ahmia-search-after-gsoc-development.
Nurmi, Juha. "Tor Hidden Service (.onion) Search: Ahmia.Fi." Ahmia.fi. Accessed May 21, 2016. https://ahmia.fi/static/presentation/Tor_Ecosystem2.pdf.
O'Neill, Patrick Howell. "Tor's Great Rebranding." *Daily Dot*, March 26, 2015. https://www.dailydot.com/layer8/tor-media-public-relations-perception/.
O'Neill, Patrick Howell. "Tor's Ex-Director: 'The Criminal Use of Tor Has Become Overwhelming.'" *Cyberscoop*, May 22, 2017. https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop/.
"The Onion Router Wiki." Noreply Wiki, August 10, 2004. https://web.archive.org/web/20040810102122/http://wiki.noreply.org/wiki/TheOnionRouter.
"OPSEC: Because Jail Is for Wuftpd." Presentation by The Grugq. YouTube video, 1:04:24, posted by Hack In The Box Security Conference, May 21, 2012. https://www.youtube.com/watch?v=9XaYdCdwiWU.
Ormsby, Eileen. *Silk Road*. Sydney: Macmillan Australia, 2014. Kindle.

Ormsby, Eileen. “Waiting in the Red Room.” *All Things Vice* (blog), August 29, 2015. https://allthingsvice.com/2015/08/29/waiting-in-the-red-room/.
Pace, Jonathan. “Exchange Relations on the Dark Web.” *Critical Studies in Media Communication* 34, no. 1 (January 1, 2017): 1–13. doi:10.1080/15295036.2016.1243249.
Paganini, Pierluigi. “UK Police: Accessing the Darkweb Could Be a Sign of Terrorism.” *Security Affairs*, July 8, 2017. http://securityaffairs.co/wordpress/60798/terrorism/darkweb-terrorism.html.
Paoli, Giacomo Persi, Judith Aldridge, Nathan Ryan, and Richard Warnes. *Behind the Curtain*. Santa Monica, CA: RAND, 2017. https://www.rand.org/pubs/research_reports/RR2091.html.
Papacharissi, Zizi. “Democracy Online: Civility, Politeness, and the Democratic Potential of Online Political Discussion Groups.” *New Media and Society* 6, no. 2 (April 1, 2004): 259–283. doi:10.1177/1461444804041444.
Pasquinelli, Matteo. *Animal Spirits: A Bestiary of the Commons*. Rotterdam: NAi Publishers, 2008.
Pfajfar, Matej. “*Onion Routing*.” Thesis, Cambridge University, UK, 2002.
Pfitzmann, Andreas, Birgit Pfitzmann, and Michael Waidner. “ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead.” In *Kommunikation in verteilten Systemen*, edited by Wolfgang Effelsberg, Hans W. Meuer, and Günter Müller, 451–463. Berlin: Springer, 1991. http://link.springer.com/chapter/10.1007/978-3-642-76462-2_32.
Phelps, Amy, and Allan Watt. “I Shop Online—Recreationally! Internet Anonymity and Silk Road Enabling Drug Use in Australia.” *Digital Investigation* 11, no. 4 (2014): 261–272. doi:10.1016/j.diin.2014.08.001.
Phillips, Whitney. *This Is Why We Can’t Have Nice Things: Mapping the Relationship Between Online Trolling and*

Mainstream Culture. Cambridge, MA: MIT Press, 2016.
Polecat. "Re: I2P Conspiracy Theories Flamewar." Gmane.network.i2p mailing list archives, October 12, 2005.
Pollock, Tristan. "Silk Road Was the Fastest Growing Online Marketplace Ever—Here's Why." *500 Startups* (blog), October 27, 2015. http://500.co/silk-road-marketplace-growth/.
Porter, Simon. "[Freenet-dev] Freenet website redesign—Feedback, ideas and help wanted." Freenet-dev mailing list archives, December 15, 2002. https://web.archive.org/web/20141117122740/https://emu.freenetproject.org/pipermail/devl/2002-December/022664.html.
Price, Roger David. *The French Second Empire: An Anatomy of Political Power*. Cambridge: Cambridge University Press, 2007.
The Principality of Sealand. 2007. http://127.0.0.1:8888/USK@EwuiekEqCT4hHMzs8OpYFQbkfawSRY7sMqvRebmyZ~c,i3RauV~532Oot0MheJNH~~IlHBBkmy~ZNVbOfCYZNtA,AQACAAE/sealand/5/ [Freenet].
"Privacy Policy." DreamHost, July 21, 2017. https://www.dreamhost.com/legal/privacy-policy/.
Protalinski, Emil. "Child Porn Photos Traded on Facebook in Plain Sight (Report)." *ZDNet*, May 7, 2012. http://www.zdnet.com/article/child-porn-photos-traded-on-facebook-in-plain-sight-report/.
"Publicity." Free Network Project, June 6, 2001. https://web.archive.org/web/20010606211622/http://freenetproject.org/index.php?page=publicity.
"Read Me (Fred/Freenet 5.0)." GitHub, December 9, 2007. https://github.com/freenet/legacy/blob/stable/README.
Reagan, Ronald. National Security Decision Directive No. 298. January 22, 1988. Presidential Directives and Executive Orders. https://fas.org/irp/offdocs/nsdd298.htm.
Redacted. *Purple Dragon: The Origin and Development of the United States OPSEC Program*. United States Cryptologic History. Fort Meade, MD: National Security Agency, 1993. https://www.nsa.gov/news-features/declassified-

documents/cryptologic-histories/assets/files/purple_dragon.pdf.
Reddy, Chandan. *Freedom with Violence: Race, Sexuality, and the US State*. Durham, NC: Duke University Press, 2011.
Redhead, Steve, and John Street. "Have I the Right? Legitimacy, Authenticity and Community in Folk's Politics." *Popular Music* 8, no. 2 (May 1989): 177–184. doi:10.1017/S0261143000003366.
Reuters News Agency. "Thai Man Broadcasts Daughter's Murder on Facebook, Then Takes His Own Life." *Telegraph*, April 25, 2017. http://www.telegraph.co.uk/news/2017/04/25/thai-man-broadcasts-daughters-murder-facebook-takes-life/.
Rider, Robert. "Conflict, the Sire of Exchange." *Journal of Economic Behavior and Organization* 40, no. 3 (November 1999): 217–232. doi:10.1016/S0167-2681(99)00065-7.
Rimlogger. "How AlphaBay was taken down due to a simple OPSEC mistake." DarkNetMarkets (subreddit), July 20, 2017. https://www.reddit.com/r/DarkNetMarkets/comments/6ogs83/how_alphabay_was_taken_down_due_to_a_simple_opsec/.
Ringo. "SoC Project: Improving Hidden Service Security and Usability." Tor-talk mailing list, May 25, 2009. https://lists.torproject.org/pipermail/tor-talk/2009-May/014094.html.
Ritchie, O. M., and Ken Thompson. "The UNIX Time-Sharing System." *Bell System Technical Journal* 57, no. 6 (1978): 1905–1929.
Roche, Leigh. "Authenticity." *Philosophy Now* 92 (November 26, 2012): 31–32.
Rose, Daniel E., and Danny Levinson. "Understanding User Goals in Web Search." In *Proceedings of the 13th International Conference on World Wide Web*, 13–19. New York: ACM, 2004. doi:10.1145/988672.988675.
Rosenberg, Scott. *Dreaming in Code: Two Dozen Programmers, Three Years, 4,732 Bugs, and One Quest for Transcendent Software*. 1st ed. New York: Crown, 2007.

Rowley, Jeremy. "[Cabfpub] Ballot .onion ballot." CAB Forum, February 4, 2015. https://cabforum.org/pipermail/public/2015-February/004927.html.
Rowley, Jeremy. "[Cabfpub] .onion and .exit." CAB Forum, October 14, 2014. https://cabforum.org/pipermail/public/2014-October/004210.html.
Rowley, Jeremy. "[Cabfpub] .onion proposal." CAB Forum, November 12, 2014. https://cabforum.org/pipermail/public/2014-November/004569.html.
Rowley, Jeremy. "Supporting Anonymous Use of Facebook in Tor." *DigiCert Blog*, November 5, 2014. https://blog.digicert.com/anonymous-facebook-via-tor/.
Ruef, Martin. "The Emergence of Organizational Forms: A Community Ecology Approach." *American Journal of Sociology* 106, no. 3 (2000): 658–714.
Russell, Andrew L. *Open Standards and the Digital Age: History, Ideology, and Networks*. New York: Cambridge University Press, 2014.
"Samuel Edward Konkin III (SEK3)—The Founder of Agorism." Debate at Dagny's Freedom Festival, Los Angeles, California, 1985. YouTube video, 47:32, posted by David Martin, March 17, 2013. https://www.youtube.com/watch?v=qpoMib89cVk.
Schulman, J. Neil. *Alongside Night*. New York: Avon, 1987.
Senda-Cook, Samantha. "Rugged Practices: Embodying Authenticity in Outdoor Recreation." *Quarterly Journal of Speech* 98, no. 2 (May 2012): 129–152. doi:10.1080/00335630.2012.663500.
Serres, Michel. *The Parasite*. Baltimore: Johns Hopkins University Press, 1982.
Shen, Wade. "Memex." Defense Advanced Research Projects Agency, 2014. http://www.darpa.mil/program/memex.
Shugart, Helene A. "Counterhegemonic Acts: Appropriation as a Feminist Rhetorical Strategy." *Quarterly Journal of Speech* 83, no. 2 (1997): 210–229.

"Silk Road 3.1." *Deep Dot Web*, 2017. https://www.deepdotweb.com/marketplace-directory/listing/silk-road-3.
Silverman, Craig, and Lawrence Alexander. "How Teens in the Balkans Are Duping Trump Supporters with Fake News." *BuzzFeed*, November 3, 2016. https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.
Silverstein, Craig, Hannes Marais, Monika Henzinger, and Michael Moricz. "Analysis of a Very Large Web Search Engine Query Log." *SIGIR Forum* 33, no. 1 (September 1999): 6–12. doi:10.1145/331403.331405.
Smith, Trevor Garrison. *Politicizing Digital Space*. London: University of Westminster Press, 2017. doi:10.16997/book5.
"SR/DPR-Timeline." Accessed February 8, 2017. http://shadowlife.cc/wp-content/uploads/2013/10/SR-Timeline.html.
"Stable Release—IIP v1.1.0." Invisible IRC Project, April 17, 2003. https://web.archive.org/web/20030417093445/http://www.invisiblenet.net/iip/downloadMain.php.
Star, Susan Leigh. "The Ethnography of Infrastructure." *American Behavioral Scientist* 43, no. 3 (1999): 377–391.
"Stateless Law & Counter Economics." A talk by Brad Spangler, March 17, 2011. YouTube video, 31:42, posted by SecularNumanist, March 28, 2011. https://www.youtube.com/watch?v=sWYIIiqPLoY.
Stevenson, Michael. "The Cybercultural Moment and the New Media Field." *New Media and Society* 18, no. 7 (August 1, 2016): 1088–1102. doi:10.1177/1461444816643789.
Stockley, Mark. "Hundreds of Dark Web Sites Cloned and 'Booby Trapped.'" *Naked Security*, July 1, 2015. https://nakedsecurity.sophos.com/2015/07/01/hundreds-of-dark-web-sites-cloned-and-booby-trapped/.
Str4d. "Re: [DNSOP] Requesting WGLC of draft-grothoff-iesg-special-use-p2p-*." IETF Mail Archive, October 2, 2015.

http://mailarchive.ietf.org/arch/msg/dnsop/1Nf4IYPw8zi2mok6Oq-oSaqu9pA.
Suchman, Mark C. “Managing Legitimacy: Strategic and Institutional Approaches.” *Academy of Management Review* 20, no. 3 (1995): 571–610.
Suddaby, Roy, and Royston Greenwood. “Rhetorical Strategies of Legitimacy.” *Administrative Science Quarterly* 50, no. 1 (2005): 35–67.
Sullivan, Andrew. “[DNSOP] More complete review of draft-grothoff-iesg-special-use-p2p-names-01.” IETF Mail Archive, December 31, 2013. https://mailarchive.ietf.org/arch/msg/dnsop/WOlHdAKFxzBNS2dvyL7XD7qL-wo.
Sullivan, Andrew. “Re: [DNSOP] On squatting and draft-grothoff-iesg-special-use-p2p-names.” IETF Mail Archive, January 6, 2014. https://mailarchive.ietf.org/arch/msg/dnsop/SEJSTssjHFCfXNxHU-hImrilLto.
“Superior Court of the District of Columbia Search Warrant.” July 12, 2017. https://www.dreamhost.com/blog/wp-content/uploads/2017/08/DH-Search-Warrant.pdf.
Sussmann, Naomi. “Can Just War Theory Delegitimate Terrorism?” *European Journal of Political Theory* 12, no. 4 (October 1, 2013): 425–446. doi:10.1177/1474885112464478.
Syverson, Paul, and Griffin Boyce. “Bake in .onion for Tear-Free and Stronger Website Authentication.” *IEEE Security and Privacy* 14, no. 2 (March 2016): 15–21. doi:10.1109/MSP.2016.33.
Tacopino, Joe. “Man Wanted for Posting Murder on Facebook.” *New York Post*, April 16, 2017. http://nypost.com/2017/04/16/man-wanted-for-broadcasting-murder-on-facebook-live/.
TC. “Hosts.txt v 1.1.” I2p.Net, December 15, 2003. https://web.archive.org/web/20040413131233/http://dev.i2p.net/i2p/hosts.txt.

T-G, David. “[Freenet-chat] Wireless.” Freenet-chat mailing list, March 26, 2002. https://emu.freenetproject.org/pipermail/chat/2002-March/000978.html.
Tilling, Matthew V. “An Overview of Legitimacy Theory.” Commerce Research Paper Series, Flinders University, Adelaide, South Australia, 2004. http://www.flinders.edu.au/sabs/business-files/research/papers/2004/04-6.pdf.
“Tor Rendezvous Specification.” Tor’s Protocol Specifications, October 12, 2016. https://gitweb.torproject.org/torspec.git/tree/rend-spec.txt.
Toseland, Matthew. “[Freenet-dev] Searching support in 0.7.0?” Freenet-dev mailing list archives, November 14, 2005. https://web.archive.org/web/20141117104945/https://emu.freenetproject.org/pipermail/devl/2005-November/000086.html.
Toseland, Matthew. “Re: [Jrandom-Po2eaMWI3R0@public.Gmane.Org: Re: [Tech] Re: I2P Conspiracy Theories Flamewar].” Gmane.network.i2p mailing list archives, October 6, 2005.
“Tunnel Implementation.” I2P: The Invisible Internet Project, October 2010. https://geti2p.net/en/docs/tunnels/implementation.
Turner, Bryan S. “Nietzsche, Weber and the Devaluation of Politics: The Problem of State Legitimacy.” *Sociological Review* 30, no. 3 (August 1, 1982): 367–391. doi:10.1111/j.1467-954X.1982.tb00659.x.
Turner, Fred. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: University of Chicago Press, 2008.
Twinam, Ann. *Public Lives, Private Secrets: Gender, Honor, Sexuality, and Illegitimacy in Colonial Spanish America.* Stanford, CA: Stanford University Press, 1999.
U.S. Attorney’s Office, Southern District of New York. “Ross Ulbricht, Aka Dread Pirate Roberts, Sentenced in Manhattan Federal Court to Life in Prison.” Press release. Federal Bureau

of Investigation New York Field Office, May 29, 2015. https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-aka-dread-pirate-roberts-sentenced-in-manhattan-federal-court-to-life-in-prison.
U.S. Department of Justice. "AlphaBay, the Largest Online 'Dark Market,' Shut Down." Press release, July 20, 2017. https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down.
U.S. Department of Justice. United States of America v. Alexandre Cazes. Filed July 19, 2017. https://www.justice.gov/opa/press-release/file/982821/download.
Vaara, Eero, and Janne Tienar. "A Discursive Perspective on Legitimation Strategies in Multinational Corporations." *Academy of Management Review* 33, no. 4 (2008): 985–993.
Vaidhyanathan, Siva. *The Googlization of Everything: (And Why We Should Worry)*. Berkeley: University of California Press, 2012.
Van Buskirk, Joe, Sundresan Naicker, Amanda Roxburgh, Raimondo Bruno, and Lucinda Burns. "Who Sells What? Country Specific Differences in Substance Availability on the Agora Cryptomarket." *International Journal on Drug Policy* 35 (September 2016): 16–23. doi:10.1016/j.drugpo.2016.07.004.
van der Aart, Erwin. "The Influence of Legitimacy on Access to Resources: A Case Study." Master's thesis, University of Twente, Netherlands, 2015. http://essay.utwente.nl/68653/.
Van Leeuwen, Theo. "What Is Authenticity?" *Discourse Studies* 3, no. 4 (2001): 392–397.
Vitáris, Benjamin. "Dark Net Markets Launching Bug Bounty Programs." *Deep Dot Web*, February 22, 2017. https://www.deepdotweb.com/2017/02/22/dark-net-markets-launching-bug-bounty-programs/.
Ware, Norma C. "Suffering and the Social Construction of Illness: The Delegitimation of Illness Experience in Chronic

Fatigue Syndrome." *Medical Anthropology Quarterly* 6, no. 4 (1992): 347–361.
Watts, Duncan J., and Steven H. Strogatz. "Collective Dynamics of 'Small-World' Networks." *Nature* 393, no. 6684 (June 4, 1998): 440–442. doi:10.1038/30918.
Weaver, Nicholas. "Re: [DNSOP] On squatting and draft-grothoff-iesg-special-use-p2p-names." IETF Mail Archive, January 6, 2014. https://mailarchive.ietf.org/arch/msg/dnsop/NaNLlarsPibaUrOxYKbkLNlEYCE.
Weber, Max. *From Max Weber: Essays in Sociology*. Edited by C. Wright Mills and Hans Heinrich Gerth. New York: Oxford University Press, 1946.
Weber, Steven. *The Success of Open Source*. Cambridge, MA: Harvard University Press, 2004.
Wedow, Suzanne. "Feeling Paranoid: The Organization of an Ideology About Drug Use." *Urban Life* 8, no. 1 (1979): 72–93.
Weimann, Gabriel. "Going Dark: Terrorism on the Dark Web." *Studies in Conflict and Terrorism* 39, no. 3 (2015): 195–206. http://www.tandfonline.com/doi/abs/10.1080/1057610X.2015.1119546.
"Welcome to FreeWeb." FreeWeb, April 28, 2001. https://web.archive.org/web/20010428125346/http://freeweb.sourceforge.net/main.html.
Weltevrede, Esther, Anne Helmond, and Carolin Gerlitz. "The Politics of Real-Time: A Device Perspective on Social Media Platforms and Search Engines." *Theory, Culture and Society* 31, no. 6 (June 20, 2014): 125–150. doi:10.1177/0263276414537318.
"Who Uses Tor?" Tor Project. Accessed May 31, 2017. https://www.torproject.org/about/torusers.html.en.
Williams, Raymond. *Keywords: A Vocabulary of Culture and Society*. Rev. ed. New York: Oxford University Press, 1985.
Wilson, Ben. "Ballot 144—Validation Rules for .onion Names." CAB Forum, February 18, 2015.

https://cabforum.org/2015/02/18/ballot-144-validation-rules-dot-onion-names/.
Wombat2combat. “What to do now and future tips.” DarkNetMarkets (subreddit), July 20, 2017. https://www.reddit.com/r/DarkNetMarkets/comments/6ohder/what_to_do_now_and_future_tips/.
Woolgar, Steve. “Configuring the User: The Case of Usability Trials.” In *A Sociology of Monsters: Essays on Power, Technology and Domination*, edited by John Law, 57–99. London: Routledge, 1991.
Wouters, Paul. “Re: [DNSOP] discussion for draft-appelbaum-dnsop-onion-tld-00.txt.” IETF Mail Archive, March 17, 2015. https://mailarchive.ietf.org/arch/msg/dnsop/FU9P4MyZGmY6XMqZdG4K1DhM-nY.
Wulf, Herbert. “Challenging the Weberian Concept of the State: The Future of the Monopoly of Violence.” Occasional Paper Series, Australian Centre for Peace and Conflict Studies, Brisbane, 2007. http://www.mobi.tamilnet.com/img/publish/2008/01/h_wulf_occ_paper_9.pdf.
Yegg. “2014 FOSS Donations.” DuckDuckGo Community Platform (blog), March 12, 2014. https://duck.co/blog/post/72/foss2014.
Zetter, Kim. “DARPA Is Developing a Search Engine for the Dark Web.” *Wired*, February 10, 2015. https://www.wired.com/2015/02/darpa-memex-dark-web/.
Zimmer, Michael. “Web Search Studies: Multidisciplinary Perspectives on Web Search Engines.” In *International Handbook of Internet Research*, edited by Jeremy Hunsinger, Lisbeth Klastrup, and Matthew Allen, 507–521. Berlin: Springer, 2009. http://link.springer.com/chapter/10.1007/978-1-4020-9789-8_31.
Zimmerman, Monica A., and Gerald J. Zeitz. “Beyond Survival: Achieving New Venture Growth by Building Legitimacy.” *Academy of Management Review* 27, no. 3 (2002): 414–431.

Zimmerman, Neetzan. “The Day Child Porn Went Viral on Facebook.” *Gawker*, March 22, 2013. http://gawker.com/5991876/the-day-child-porn-went-viral-on-facebook.
Zzz. “31C3 Trip Reports.” Zzz.I2P forum, January 2, 2015. http://zzz.i2p/topics/1777?page=1#p9092 [I2P].
Zzz. “6761 Was a Mistake.” Zzz.I2P forum, March 11, 2016. http://zzz.i2p/topics/2101?page=1#p12019 [I2P].
Zzz. “.I2P Domain Registration with IETF.” Zzz.I2P forum, November 13, 2013. http://zzz.i2p/topics/1518-i2p-domain-registration-with-ietf [I2P].
Zzz. “Proposal: Simplified Console Home Page.” Zzz.I2P forum, January 19, 2012. http://zzz.i2p/topics/1079 [I2P].
Zzz. “State of I2P Search Engines.” Zzz.I2P forum, January 22, 2012. http://zzz.i2p/topics/1083-state-of-i2p-search-engines [I2P].

Index

0x90. *See* James, Lance

4chan, 183

Activists, 39, 69, 102, 138, 222, 228–229

Actor-network theory, 9, 130, 132

AFKindex, 145

Agorism, 16, 89–91, 94–103, 108, 112–114, 116

Agorism.info, 99, 119

Ahmia, 134, 136–138, 140–141, 145, 147–149. *See also* Nurmi, Juha; Search engines

Algorithm, 12–13, 64, 74–77, 92, 141, 145, 147, 149, 151

Alongside Night, 99. *See also* Agorism

AlphaBay, 67, 108, 112–113, 116–119, 228

Alt-right, 187, 228

Amazon, 39, 99, 110, 112, 141, 201

Anarchism, 7–8, 46, 68, 96, 98, 101, 224

Anarplex, 99

Android, 64, 150

Ano+, 184. *See also* Social networking sites

anonCommFramework, 63. *See also* Invisible Internet Project; jrandom

Anonymity, 45–46, 58, 140
Clear Web and, 55
networks and, 6, 54, 60, 62–63, 75, 91, 210
politics and, 45, 67–70, 76, 225–230
research and, 11, 58
search engines and, 130, 134, 136, 149
social networking sites and, 160, 188, 208–209
theories of, 59, 74
Anonymous, 227
Antifa, 175–176, 187
Apache, 91, 93, 141, 169
Apache Lucene, 141
Appelbaum, Jacob, 75–76, 195–196, 200, 204–207
Apple, 198–200, 205–207, 226
Appropriation, 15, 28, 66, 132–133, 162, 211. *See also* Symbolic economy
of legitimacy, 19, 42–43
of violence, 16, 45, 89–90, 94, 105, 112–116
Arbitration, 97
Archive.org, 18, 78
Archives, 3, 10–11, 14, 17, 53, 90, 100, 133, 139, 146, 189, 204, 226
Ashley Madison, 2, 45
Aupers, Stef, 111–112
Authentication, 162, 183, 189, 197

Authenticity, 3, 14–17, 146, 195, 205, 230
and Galaxy2, 174, 177, 179, 181–189
and legitimacy, 161–168
in markets, 100, 112, 118
among network builders, 53–54, 73, 77
symbolic economy and, 34–40, 42–44, 46
Babenhauserheide, Arne, 137, 144
Banet-Weiser, Sarah, 164
Banning, 145, 170, 173, 186
Barratt, Monica, 11, 18, 227
Bartlett, Jamie, 4, 7–8
Bastards, 40–41, 101
Bauman, Zygmunt, 225–226
BBC, 106
Beast, 134, 150. *See also* Search engines
Bendix, Regina, 187
Bergman, Michael, 4
Beyer, Jessica, 30, 170
Bing, 149, 151
Bitcoin, 92–93, 100, 111–112, 119, 175
scams and, 109, 148
surveillance and, 139
and tumbling, 92, 107, 141
BitTorrent, 9, 64, 119
Black Lives Matter, 175, 225

Blockchain, 93
Blogs, 106
    on the Dark Web, 19, 58, 61, 135, 179
Boellstorff, Tom, 11
Bombe, 57
Bonjour, 198, 200
Bourdieu, Pierre, 35, 39–40, 42, 73, 165–167
Bowan, Kate, 165
Bowles, Samuel, 114
boyd, danah, 185
Branwen, Gwern, 10, 100
Bratich, Jack, 115
Browne, Harry, 99
Bullshit, 34–35, 38, 46, 76, 108, 161, 164
Callon, Michel, 9, 130–131
Canada, 117–118, 140
Candle, 134, 150
Carding, 110
Catfishing, 182–183
Cazes, Alexandre, 117–119, 163
Celebrity, 77
Censorship, 66, 72, 74, 98, 185–186, 199, 222
    and the domain name system, 54, 199
    and search engines, 145–146
    and social networking sites, 170, 173

Central Intelligence Agency, 209

Centralization, 55–56, 62–63, 92–93, 137, 141, 169, 197, 199

CERN, 78

Certificate authorities, 201–202. *See also* Certificate Authority/Browser Forum

Certificate Authority/Browser Forum, 202–207

Chans, 174, 183

Chat, 7, 10, 19, 61, 133, 135, 139, 174, 179

Cheng, Vincent, 166

Cheshire, Stuart, 197–199, 207

Child exploitation images, 2, 4, 67, 137, 222, 228–230

    removal from search engine results, 145–149

    and social networking sites, 161, 171, 186, 212

Child pornography, 7, 143, 145–146, 170, 172, 186, 223. *See also* Child exploitation images

China, 65–67

Christin, Nicholas, 139, 186

Chrome, 5

Chun, Wendy, 12, 137

Civility, 172–174, 186, 224, 228

Clarke, Adele, 9–10, 13–14

Clarke, Ian, 54–55, 57–58, 60, 65, 70, 74, 78

Clear Web, 13, 18–19, 60, 91, 141, 160, 223, 230
definition of, 5–7
links to, 104, 177, 180
mirror sites, 99, 228
relationship to the Dark Web, 17, 46, 72, 93, 118, 151, 168, 208–213
surveillance on, 140, 184–187, 226
Clinton, Hillary, 43, 171
Cloners, 147–149, 202, 210
Closed Shell System, 178. *See also* Marianas Web
CNN, 43, 172
Coleman, Gabriella, 11, 227
Comey, James, 2, 6, 19, 67
Communication, 3, 28, 30, 46, 53, 72, 132, 137, 175, 177, 184, 186, 213
and digital networks, 59, 61–64
encryption of, 2, 6, 74
organizational and managerial, 14, 31–32, 38, 128
strategic, 33
surveillance of, 17, 65–69, 140, 223–230
and violence, 16, 89–90, 115–118, 229
Communications Security Establishment Canada, 140
Communism, 98
Communities of practice, 15, 34, 74, 76–77
Computer science, 3, 12, 17, 46, 54, 58, 73–74, 76, 138, 211
Consecration, 42, 112, 150, 165–167, 177–178, 181, 211

Cooren, François, 132

Corporations, 1, 6, 17, 42, 46, 210–211, 223, 225–226

corporate social media, 2, 160, 162, 171, 185, 187, 200–201

and propriety, 3, 28–34, 37, 44, 69–70, 127–132, 163, 195–196

surveillance by, 7, 55, 66–67, 136, 151

Counter-economics, 96, 101. S*ee also* Agorism; Konkin, Samuel Edward, III

Counterfeits, 25–27, 38, 46, 141, 164

Cox, Joseph, 115

Credit cards, 1–2, 7, 46, 93, 110, 226. *See also* Carding

Crime, 39, 138–139, 228

Cryptocurrencies, 92, 100, 118, 221

CSS, 5–6, 57, 63, 99

Cult of the Dead Cow, 204

Cultural studies, 27

Curation, 146

CVS, 62

Czarniawska, Barbara, 130–131

Daily Stormer, 228

Dark Matters, 160–161, 168, 173, 189. *See also* Social networking sites

Dark Net, 4, 7, 9

Darknet Counterfeit Forum, 109

Darknet Market Archives, 10

Darknet Market Avengers, 117

Dark Web,
agorism on, 99–100
definitions of, 4–5, 7–9, 127
and Facebook, 201, 209–214
history of, 54–64
Internet standards and, 195–197, 199
markets on, 25, 89–94, 102–104, 117–119
nonusers of, 135–137, 143
OPSEC on, 107–116
search engines on, 16, 130, 133
social networking sites on, 16–17, 159–161, 168–170, 174, 184–187, 189
trial of legitimacy, 26–28, 37–39, 44–46, 67, 223, 228–230
Dark Web site administrators, 2, 16, 39, 46, 179, 210, 229–231
arrests of, 117, 228
interviews with, 3, 14, 19, 27, 221–223
and markets, 6, 91–94, 100
OPSEC among, 107, 111–113
scams performed by, 109
and search engines, 135, 142–143
and social networking sites, 159–161, 168–169, 171–176, 186–189, 209, 228
DARPA, 70, 139–140, 151
Dash, 92. *See also* Cryptocurrencies
Databases, 4, 93, 108, 110–111, 130, 141, 143, 149
DDOS, 115, 142, 172

Dealers, 2, 27, 39, 160, 186

Deanonymization, 6, 69, 140, 180, 226

Decentralization, 27, 92–93, 99, 144, 209

Deep Dot Web, 93, 135, 141

Deep Web, 4, 7–8, 19, 127, 213

Delegitimation, 17, 108, 111, 132–133, 195, 205, 210–212. *See also* Symbolic economy

- and authenticity, 174, 177, 186, 188, 224
- and symbolic economy, 40, 43–45, 162
- and violence, 65–68, 90, 97, 102–103, 116, 140, 144–145, 197, 229–230

Demant, Jakob, 103

DigiCert, 195, 202, 210–211

Dingledine, Roger, 58–61, 65, 70, 74–75, 209–210

Direct.i2p, 143, 146. *See also* Search engines

Discourse, 9–10, 16, 66, 113, 131, 169, 197

- and agorism, 102–103
- and anonymity, 224, 227, 229
- and authenticity, 164, 166
- and organizations, 128
- and states, 30–31, 45–46

Dissidents, 2, 7, 45, 58, 66–68, 74–75, 196, 202, 222

Distributed Hash Table, 93

Documentation, 12, 74–75, 106, 110, 141

Domain name system (DNS), 54–56, 60, 64, 141, 196, 199–200, 204, 206, 211, 214

Domain squatting, 203, 214
Doxing, 11, 18, 54, 100, 102, 162, 181, 227
Dread Pirate Roberts, 89, 101. *See also* Silk Road; Ulbricht, Ross
DreamHost, 226
Drugs, 25, 93–95, 105, 138, 160, 186, 197, 212
    and authenticity, 34, 46, 167
    and Grams, 6
    markets for, 7, 91, 107, 139, 187, 221
    and the Silk Road, 2, 16, 38, 89, 98–102, 137, 201, 222
    users of, 112
    vendors, 27, 141
    War on Drugs, 39, 109, 115–117, 229
DuckDuckGo, 70, 223
eBay, 39, 91, 99
Eepsites, 26, 46, 75, 91, 99, 137, 141, 229
    development of, 63–64, 196–199
Eepsites.i2p, 134, 150
Electronic Frontier Foundation, 70, 137–138
Elgg, 169, 174
elgoog, 134, 149. *See also* Search engines
E-mail, 59, 64, 70, 93, 204
    archives, 3, 53, 72, 200, 207–208
    and encryption, 107, 176, 180
    and OPSEC, 107, 117–118
    protocols, 9

Encryption, 2, 4, 6, 19, 67–69, 105–106, 137, 180–181, 184, 224. *See also* PGP

and algorithms, 12–13, 74–77, 92

and Freenet, 55–56

and the Invisible Internet Project, 64

and onion routing, 59

and SSL, 201, 210

Enzo, 57, 134, 136, 140, 145, 150. *See also* Search engines

Epsilon, 134, 150. *See also* Search engines

Ethereum, 92. *See also* Cryptocurrencies

Ethnography, 11, 186, 214, 227

EuroGuns, 67

Europol, 116–117

Evolution, 109

Exchange, 58, 62, 138, 176–178, 181, 222. *See also* Symbolic economy

of legitimacy, 15, 19, 28, 40–42, 44–45, 64, 71, 77, 132–133, 150, 162, 167, 174, 204, 211, 230

and markets, 89, 91–98, 102, 113–114

Exit node, 65, 72, 180

Exit scam, 109

Extended Validation certificates, 17, 195, 197, 202, 205, 208–209

Extremists, 4, 7

Facebook, 5, 33, 37, 160, 162, 168–169, 184–185, 187, 223, 226–227, 230
    and markets, 2
    as a Tor hidden service, 7, 17, 195–197, 201, 207, 223
Fairhurst, Gail, 132
Fake news, 43, 212
Fascism, 98, 102, 120, 176, 225
Federal Bureau of Investigation, 67, 116–117
Feminism, 9, 184, 222
File sharing, 57, 62
Firefox, 5–6
Flaming, 75, 170–171
Flogs, 58
FMS, 99
Forrest, Katherine, 103
Forums, 7, 19, 26, 45, 135, 139, 148, 167, 174, 176, 179
    and archives, 10, 14, 74
    and markets, 25, 38, 89–90, 92–94, 99–104, 107–113, 117, 139
    and tc.i2p, 63, 78
    and the Youth Liberation Front, 221–223, 229–230
    and zzz.i2p, 200, 207
Foucault, Michel, 9–10, 41
Fproxy, 57

Free and Open Source Software, 2, 77, 199–200, 204, 207, 228
development of, 12, 55, 62
and Elgg, 169
and markets, 93
and propriety, 69, 71–72
Freedman, Michael, 58–59
Freedom Hosting, 195
Freegle, 134, 149. *See also* Search engines
Free Haven, 58–60, 74, 209
Freenet, 5–6, 11–12, 17–19, 26, 103, 127, 130, 147, 178, 213, 222–224, 227–230. *See also* Babenhauserheide, Arne; Bombe; Clarke, Ian; Enzo; Freesites; McNab, David
and agorism, 98–99
development of, 15, 25, 39, 45–46, 53–58, 209
and legitimacy, 64
and markets, 91, 103
relationship to Invisible Internet Project, 61–64
relationship to Tor Project, 58–60
and search engines, 16, 133–137, 140–145, 147, 149–151
social networking sites on, 2, 160–161, 184
FreenetUser, 145
Freesites, 26, 46, 57–58, 62, 91, 99, 143–145, 229. *See also* Fproxy; jSite
Free speech, 27, 39, 45, 222
FreeWeb, 57
“Fuck you” messages, 160–161, 173, 187, 189

Fullz, 110. *See also* Carding

Galaxy, 168–170, 173, 209. *See also* Social networking sites

Galaxy2, 16, 18, 161–162, 168, 209–210, 228, 230. *See also* Social networking sites

Gawker, 99–100

Genealogy, 10, 40–41, 102, 106

Gintis, Herbert, 114

Globaleaks, 45, 138

Global War on Terror, 66, 224

GNUnet, 5, 196, 200, 203, 205, 210

Google, 149–151, 178–179, 226–227

- and the Deep Web, 4–5, 127
- Google Translate, 18
- indexing of Dark Web, 4, 16
- relation to Dark Web search engines, 46, 127, 134–142
- sponsorship of Dark Web projects, 70

Google Summer of Code, 138

Government Communications Headquarters, 140

Grams, 6, 18, 134, 141, 150. *See also* Search engines

Griffith, Virgil, 151

Grothoff, Christian, 196–197, 199–201, 203–207, 211, 214

Grugq, the, 104–110, 115, 118

Guide Review Board, 112. *See also* AlphaBay

Guitton, Clarence, 228

Guns, 2, 67, 138, 197, 212

Hacking, 12, 56, 137, 165, 211, 213, 227
and authenticity, 37–38, 76, 165, 177–179
and the Invisible Internet Project, 72–75, 77
and legitimacy, 42, 44–46, 195–196, 204
and markets, 110
and violence, 68, 104–105, 115–116
Hammer, M. C., 34
Harassment, 160, 184, 187–189, 228
Harper, David, 111–112
Harvard, 58, 208
Heavy metal, 167, 169
Helmond, Anne, 12, 61
Hermes Center for Transparency and Digital Human Rights, 138
Heterogeneity, 9–10, 13, 130, 132, 135–137
Hidden Answers, 3, 109
Hidden Wiki, 60, 221
Hierarchy, 36, 96, 151, 163, 209–210
Hine, Christine, 186
Hip hop, 35, 42, 167–168
Holland, 117, 228
Hosts.txt, 64
HTML, 5–6, 9, 56–57, 143
HTTPS, 78, 119, 189, 195, 201–202, 208–210, 214. *See also* Certificate authorities; Extended Validation certificates
Hub, the, 107–108, 113, 117

Human trafficking, 139

Hunsinger, Jeremy, 2, 19, 167

I2Phreak, 143. *See also* Direct.i2p

ID3NT, 184. *See also* Social networking sites

Identity, 142, 162, 164, 186

and anonymity, 45, 55, 57, 59–60, 70–71, 74, 77, 136, 223–225

and authenticity, 37–38

and Extended Validation certificates, 7, 196–197, 201

and Facebook, 208–211, 213

and gender, 175, 182–184, 187–189

and Internet Protocol addresses, 6

online and offline, 11

and OPSEC, 107

and PGP, 92, 169

and pseudonymity, 168, 173–174, 179–181

theft of, 7, 93, 110–111, 117

Ignatious Toopie, 72

Infrastructure, 9, 30, 55, 59, 131, 214

Inheritance, 15–16, 40–41, 64, 71, 90, 114, 162, 168–169, 211. *See also* Symbolic economy

of Google's legitimacy, 46, 128, 149–150

Internet Archive, 57. *See also* Archive.org

Internet Assigned Names Authority, 196

Internet Corporation for Assigned Names and Numbers, 196–200, 203, 211, 213

Internet Engineering Task Force, 195–201, 203–207, 210, 214

Internet Freedom, 68, 151

Internet Relay Chat, 3, 9–10, 61–62, 70, 72, 99, 133

Invisible Internet Project, 2–3, 5–6, 15. *See also* Invisible IRC Project; James, Lance; jrandom; zzz

development of, 15, 45–46, 53, 61, 195–200

relation to Tor Project, 211

and search engines, 134–137, 142

Invisible IRC Project, 61–64, 69, 72

IP addresses, 5–6, 55, 62, 140–142, 200, 226

Iraq War, 106

Israel, 171, 184

James, Lance, 60–65, 67, 69, 72–73

Jargon, 46, 74

Java, 55, 63–64, 143, 178

John, Nicholas A., 13

Journalists, 27, 36, 38, 42, 46, 70, 115

coverage of the Dark Web, 90, 99, 100, 110, 137, 195

definitions of the Dark Web, 4, 7

and legitimacy exchange, 42, 46

jrandom, 63–68, 70, 73, 75–76, 195, 214

jSite, 57

Keyword analysis, 13–14, 26

König, Rene, 149, 151

Konkin, Samuel Edward, III, 90, 94–100, 113–114, 119. *See also* Agorism

Krochmal, Marc, 197–199, 214

Krueger, 209. *See also* Galaxy

Lameth, 169–170, 172–177, 181, 184–189, 228. *See also* Galaxy2

Latency, 59, 61–63, 91, 211

Latzko-Toth, Guillaume, 26

Law, John, 9, 130, 132, 147

Law enforcement, 2–3, 16, 27, 43, 70, 105, 110, 167, 170, 228–229

- and the Dark Web, 13, 45
- and markets, 89–91, 93, 107, 109–112, 117–118
- and search engines, 134–140, 144
- and social networking sites, 159–161
- and violence, 28–29, 31, 95, 97, 116, 129, 175

Lawson, Sean, 42, 115

LeFevre, Robert, 95, 98

Legitimacy, 53, 89–90, 95–96, 185–189, 197, 199, 204, 211. *See also* Authenticity; Propriety; Symbolic economy; Violence

- definitions of, 28–46
- and delegitimation, 97
- as a keyword, 9–11, 13–17, 26
- and network builders, 64–74, 76–78
- and organizations, 127–134, 138, 147, 161–170
- and self-legitimation, 19, 30, 33
- and social networking sites, 173–175
- and technical knowledge, 177, 195–196
- trial of, 2–4, 26–27, 44, 67, 223, 227–230

Legitimists, 40
LGBTQ, 175
    politics, 222
Libertarianism, 16, 46, 89, 94–96, 98–99, 101, 108, 114, 119
    Libertarian Party, 96
Linux, 169, 175, 177–178
.local, 198, 200, 205–207. *See also* RFC 6762
localhost, 5, 62, 198
Machine learning, 148
Maddox, Alexia, 11, 18, 100, 102, 227
Mailing lists, 73–75, 78, 133, 135, 204, 206–207
    archives, 10, 14, 133
    and Freenet, 25, 39
    and the Invisible Internet Project, 62–63
    and the Tor Project, 59, 200
Malcolm, Jeremy, 137–138
Mallein, Phillipe, 26, 44
Manichaean science, 69, 116, 118
Manifesto.i2p, 222
Man-in-the-middle attack, 148. *See also* Cloners
Maréchal, Nathalie, 68
Marianas Web, 178. *See also* Closed Shell System
Marines United, 212
Marketplace, 67, 91, 99, 118, 212

Markets, 2, 6–7, 13, 15–16, 19, 61, 78, 129, 135, 139, 167, 187, 221, 226, 228. *See also* Agorism; AlphaBay; Darknet Counterfeit Forum; EuroGuns; Grams; Silk Road

black, 45, 67, 94, 96, 100, 102, 138

gray, 96, 102

politics of, 103

prohibitions against, 170

sociotechnical features of, 91–94

Martin, James, 12, 32, 119, 139

Marwick, Alice, 36, 185

Masculinity, 46, 167, 183, 187–188

Mathewson, Nick, 60

McKelvey, Fenwick, 30

McNab, David, 57, 143

McNaughton, Chris, 149

Memes, 10, 30, 183

Memex, 139–140. *See also* Search engines

Milblogs, 106

Military, 15, 31, 42–43, 70, 89, 103, 115–116, 184, 229. *See also* OPSEC (operations security), origins of

United States, 16

and violence, 29, 38, 65, 95, 97, 112

Mises, Ludwig von, 98, 119

MIT, 58, 201

Mix-nets, 58–59

Molnar, David, 58–59

Monero, 92. *See also* Cryptocurrencies

Money, 1, 7, 38, 101, 109, 113

MoniTOR, 142, 146, 148. *See also* Search engines

MP3s, 57, 62, 74, 143

Muffett, Alec, 196, 202, 204–207

MultiVerse, 159–161, 168, 189. *See also* "Fuck you" messages; Social networking sites

Munksgaard, Rasmus, 103

MySQL, 91, 169

n00bs, 161, 178–179

Namecoin, 196, 199–200, 203–205, 210–211

Name collision, 198, 208

Napster, 57

Nationalism, 37–38

National Security Agency, 68, 71, 105–106, 225–227

Nazis, 98, 213, 228. *See also* Daily Stormer; White supremacism

Neoliberalism, 113

New York Times, 2, 55, 57, 212, 223

NGINX, 93

Nodes, 44, 55–56, 59, 65, 72, 74, 180. *See also* Topology

Nonprofits, 2, 44, 195–196, 200, 210

- Freenet as, 69
- Invisible Internet Project as, 70–71
- and legitimacy, 31, 33–34, 69, 127–129, 211
- Tor Project as, 69, 71

not Evil, 134–135, 148–149. *See also* Search engines

Nurmi, Juha, 135, 137–138, 141, 145, 149. *See also* Ahmia

Obligatory points of passage, 16, 131

Onion.link, 127, 134, 150–151

Onion routing, 59–60

OpenBazaar, 93, 119

OPSEC (operations security), 45, 94, 175, 179, 229

origins of, 105–107

politics of, 15–16, 111–119

use on Dark Web markets, 89–90, 103–104, 107–111

Organizations, 28, 38, 45–46, 65, 96, 102, 197, 203, 210–211, 229. *See also* Communication, organizational and managerial; Nonprofits; Propriety

and Free and Open Source Software, 200

legitimacy of, 15, 31–34, 53–54, 69–73, 77, 127–134

and OPSEC, 106

and power, 163, 165

search engines as, 16

Ormsby, Eileen, 100, 108–109

Outlaw Market, 108

Oxford English Dictionary, 34

Pace, Jonathan, 109

Palestine, 167, 171, 184, 213

Papacharissi, Zizi, 224–225, 227

Paranoia, 90, 103–104, 110–113, 116, 118. *See also* OPSEC (operations security), politics of

Partyarchy, 96, 101. *See also* Libertarianism

PDFs, 99, 112, 143
Peer-to-peer software, 59, 119, 196, 199, 209, 214
and Freenet, 55–56
and the Invisible Internet Project, 72
markets, 93
search engines, 141
Personal information, 7, 11, 212
prohibitions on sharing of, 17, 168, 179–181, 185, 188
sales of, 2, 110–111
Pfajfar, Matej, 60
PGP, 92, 107, 108, 141, 169, 176, 177
Phillips, Whitney, 114
PHP, 91, 169, 178
Pinging, 142
Playpen, 222, 228. *See also* Child exploitation images
Pornography, 4, 8, 19, 135, 170, 172, 223
Exposed, 183, 187–188
revenge, 7, 212
and search engines, 145

Power, 58, 97, 105, 179, 195, 229
and authenticity, 34, 112, 162–167, 173, 186
and discourse, 10–11
and legitimacy, 3, 15, 28, 37–40, 44, 53, 103
practices of, 13
and propriety, 31, 131–132, 210
and software, 12, 72, 201
and surveillance, 55
and violence, 27, 29–30, 45, 65–67, 73, 89–90, 95, 109, 114, 116–118
Principality of Sealand, 62
Privacy, 2, 12, 204, 224
and Internet standards, 196, 199
and network builders, 58–62, 71
and research ethics, 18
search engines and, 130, 138, 140
and social networking sites, 11, 177, 183, 188, 195
Propaganda, 38, 46, 67, 212
Propriety, 3, 14–17, 31–35, 38–40, 53, 127–130, 161–162, 165, 230
and corporations, 45, 195–196, 204, 210
and network builders, 69–72
and search engines, 133, 144, 147, 149
ProPublica, 2, 210, 223

Protocols, 9, 12, 16, 63–64, 135, 143, 151, 197–198
and encryption, 176
HTTP, 54
Internet protocol, 5, 62, 184
SMTP, 63
Proxies, 57, 61, 148, 150–151, 155, 177, 202
Purchase of legitimacy, 15, 40, 42, 44, 115, 129, 162, 211
Purple Dragon, 106. *See also* OPSEC (operations security)
Python, 141, 178
Quantum computing, 178
Radical Faeries, 222
Rasch, Miriam, 149, 151
Reagan, Ronald, 106
Reddit, 26, 93, 118, 135, 141, 175, 213
Red rooms, 45, 212
Rendezvous points, 60. *See also* Tor hidden services
Revenge pornography, 7, 212
RFC 6761, 197–200, 203–204, 206–207, 214
RFC 6762, 198, 200, 214
RFC 7686, 196, 206–208
Rhetoric, 3, 32, 38, 41–42, 116, 164
Rid, Thomas, 25, 223, 228
Rider, Robert, 114
Robots exclusion standard, 142. *See also* Search engines; User agent string
Rothbard, Murray, 98

Routing, 2, 5–7, 18–19, 59–60, 111, 143. *See also* Nodes; Topology

Russia, 18, 148

Satanism, 171

Saudi Arabia, 66

Scams, 13, 46, 116, 138, 144, 167, 202, 212

    on markets, 90, 109–113, 116

Schulman, J. Neil, 99. *See also* Agorism; *Alongside Night*

Script kiddie, 178

Search engines, 6, 16, 32, 46, 53, 61, 93, 119, 133, 162, 210, 228

    and Deep Web, 4, 127, 145

    and indexes, 54, 57, 78, 127, 130, 137, 222, 230

Second Life, 4, 11

Secondrealm.i2p, 99

SecureDrop, 45

Security, 8, 27, 39, 42–44, 66–67, 148, 195, 224–226. *See also* OPSEC (operations security)

    and agorism, 16, 96–98, 102

    of the domain name system, 199

    of information, 2, 46, 68, 76, 78, 110, 181

    of networks, 62, 75, 202, 210

    of software, 12, 72, 93

Seeker, 134, 140, 150. *See also* Search engines

Selfies, 182–184, 189

September 11, 2001 attacks, 66

Serres, Michel, 132, 147

Sessions, Jeff, 116, 118
Silk Road, 2, 25, 38–39, 46, 89–92, 137, 139, 168, 201, 205, 211
    agorism on, 16, 99–103, 114–119
    seizure of, 103, 107–109, 195, 222
Silk Road 2.0, 109
Silk Road Reloaded, 91
Snowden, Edward, 77, 91, 204, 225
Social construction, 36, 41
Social engineering, 38, 111
Social justice, 222–223, 229–230
Social media, 7, 226. *See also* Social networking sites
    and legitimacy, 31, 33, 36
Social networking sites, 13, 19, 26, 119, 135, 151, 212. *See also* Dark Matters; Facebook; Galaxy; Galaxy2; ID3NT; MultiVerse; Sone
    on the Clear Web, 185, 187, 209
    on the Dark Web, 10–11, 45, 53, 58, 78, 222
Sociology, 4, 9, 29–30, 32, 37–38, 41, 44, 128
Sociotechnical systems, 89–91, 94, 100, 131
Software studies, 12
Sone, 184, 230
Spam, 25, 27, 39, 45
Special-Use Domain Name, 196–206
SSL, 6, 201–202. *See also* Extended Validation certificates
Star, Susan Leigh, 9, 130–131, 214
Start-ups, 26, 38, 128

Stats.i2p, 75

Stevenson, Michael, 35

Suchman, Mark, 32, 39, 128

Surveillance, 17, 58, 94, 136, 151, 185, 195, 223–229

    corporate, 7

    by states, 29, 39, 66–68, 71, 78, 90, 111, 140

Swartz, Aaron, 138

Symbolic economy, 15, 17, 27–28, 40, 44, 46, 54, 65–66, 97, 129, 132, 167–168. *See also* Appropriation; Delegitimation; Exchange; Inheritance; Purchase of legitimacy

Syverson, Paul, 59–60

Taxes, 31, 42, 69, 95–96, 100–102

tc.i2p, 63, 78

TCP, 63

Technical standards, 73, 200

Techno-elitism, 177, 179, 184

Terrorism, 2, 4, 7, 43, 160, 186, 212, 224

Terrorist's Handbook, 67–68

Thailand, 117–118

Thatcher, Margaret, 113

Top-level domain, 196

Topology, 73, 75–77, 119, 130, 143, 149, 178, 214. *See also* Nodes; Peer-to-peer software

    centralized, 93

    small-world, 55

Tor2Web, 150–151

Tor Child Protection Agency, 176

Tor hidden services, 26, 46, 99, 212–213, 221–223, 228–229

and cloners, 147–148

and corporate sites, 2

development of, 60

and Extended Validation certificates, 17, 195–197, 201–205, 208–210

lists of, 175

and markets, 89, 91, 99

renaming as “onions,” 8, 205

and search engines, 127, 137–139, 141, 144

and social networking sites, 168–170

Tor Project, 15, 53, 58, 137, 196, 200, 203, 223. *See also* Free Haven

finances of, 68, 71, 211

history of, 58

legitimacy and, 17, 74–77, 138

marketing and, 8, 72

as a nonprofit, 70, 195

TorSearch, 149

Toseland, Matthew, 135–136

Toussaint, Yves, 26, 44

Trolls, 4, 171–172, 202

Trump, Donald J., 39, 43–44, 226

Truth and Light, 1, 3, 13

Twitter, 2, 33, 37, 64, 160, 169–172, 184–187, 200, 213

Ulbricht, Ross, 89–90, 100–103, 107–109, 118, 163, 195. *See also* Dread Pirate Roberts; Silk Road

Uniform Resource Locator (URL), 54, 64, 75, 99, 143, 146–147, 201, 209

United States of America, 43, 69, 98, 105

Unix philosophy, 75

Urban Dictionary, 34

U.S. Department of Justice, 116–117, 226

U.S. Department of State, 68, 70

User agent string, 142

Van Leeuwen, Theo, 165

Vendors, 13, 25, 91–93, 99, 107–108, 143, 167

- of drugs, 94, 139, 229
- and forums, 94
- and OPSEC, 91, 109–113, 117–118
- and search engines, 6, 134–136, 141
- of stolen information, 2

Vietnam, 90, 105–106

Violence, 14, 25, 165
and agorism, 95–103
appropriation of, 105, 111, 118
and communication, 69, 90, 116
and hacking, 115
illegitimate, 68, 197, 221
against pedophiles, 176
by police, 175
and the state, 3, 15–16, 28–35, 38, 40, 44–45, 53, 64–66, 77–78, 89, 94, 129, 161–162, 202, 225–230
and white supremacy, 176
Virtual private network, 93
Visibility.i2p, 161, 168–169, 173, 179, 184, 230. *See also* Social networking sites
Voice of America, 106
War on drugs, 39, 109, 115
Web browsers, 5–9, 57, 63–64, 100, 169, 179
Weber, Max, 14, 28–31, 35, 37, 39–43, 89, 97, 129
Web publishing, 15, 53, 57, 60, 63, 78
Wedow, Suzanne, 112
Weimann, Gabriel, 7–8
Whistleblowing, 2, 45, 61, 77, 138
White supremacism, 175, 187
Wikileaks, 204
Wikis, 10, 60, 214, 221–222
Wire, 169, 172–178, 182, 186. *See also* Galaxy2

World Wide Web, 4–6, 53–57, 61–63, 78, 99, 141, 142, 211. *See also* Clear Web

Youth Liberation Front, 221–223, 229–230

YouTube, 26, 41, 104, 172

Zeitz, Gerald, 128, 130

Zeronet, 5

Zimmerman, Monica, 128, 130

Zotero, 10

Zuckerberg, Mark, 38, 208

zzz, 64, 68, 71, 75–76, 146, 150, 200, 206–207