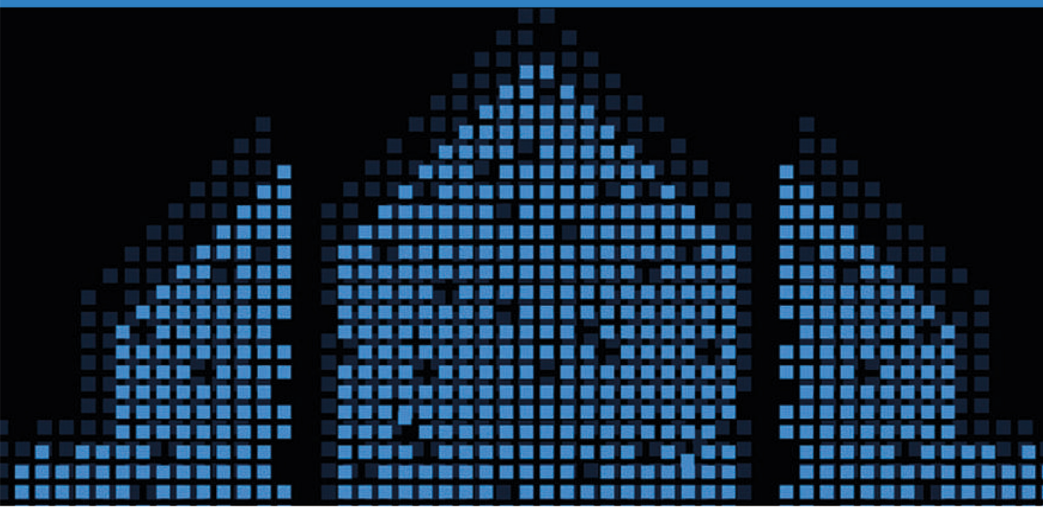
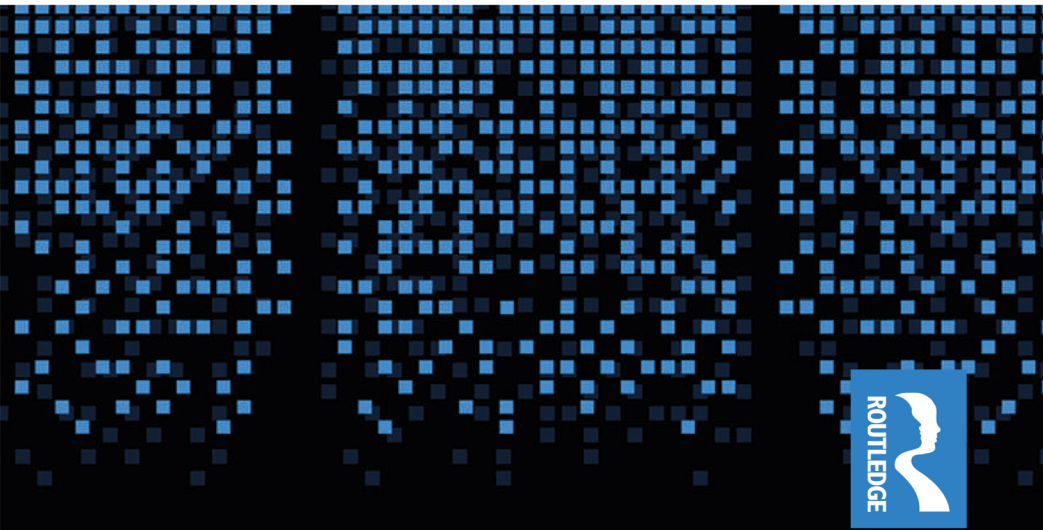
ROUTLEDGE FOCUS



Cypherpunk Ethics

Radical Ethics for the Digital Age

PATRICK D. ANDERSON



ROUTLEDGE

Cypherpunk Ethics

Cypherpunk Ethics explores the moral worldview of the cypherpunks, a movement that advocates the use of strong digital cryptography—or crypto, for short—to defend individual privacy and promote institutional transparency in the digital age.

Focusing on the writings of Timothy May and Julian Assange, two of the most prolific and influential cypherpunks, the book examines two competing paradigms of cypherpunk philosophy—crypto anarchy and crypto justice—and examines the implications of cypherpunk ethics for a range of contemporary moral issues, including surveillance, privacy, whistleblowing, cryptocurrencies, journalism, democracy, censorship, intellectual property, and power.

Rooted in theory but with very real applications, this volume will appeal not only to students and scholars of digital media, communication, journalism, philosophy, political science, critical data studies, sociology, and the history of technology but also to technologists and activists around the world.

Patrick D. Anderson is Assistant Professor of Philosophy in the Department of Humanities at Central State University, USA, and editor-in-chief of the WikiLeaks Bibliography.

Routledge Focus on Digital Media and Culture

The *Serial* Podcast and Storytelling in the Digital Age
Edited by Ellen McCracken

Media Piracy in the Cultural Economy
Intellectual Property and Labor Under Neoliberal Restructuring
Gavin Mueller

Mobilizing the Latinx Vote
Media, Identity, and Politics
Arthur D. Soto-Vásquez

Playlisting
Collecting Music, Remediated
Onur Sesigür

Understanding Reddit
Elliot T. Panek

Algorithms and Subjectivity
The Subversion of Critical Knowledge
Eran Fisher

TikTok Cultures in the United States
Trevor Boffone

Cypherpunk Ethics
Radical Ethics for the Digital Age
Patrick D. Anderson

For more information about this series, please visit:
https://www.routledge.com

Cypherpunk Ethics

Radical Ethics for the Digital Age

Patrick D. Anderson

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2022
by Routledge
4 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
605 Third Avenue, New York, NY 10158

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record has been requested for this book

ISBN: 978-1-032-11359-3 (hbk)
ISBN: 978-1-032-11578-8 (pbk)
ISBN: 978-1-003-22053-4 (ebk)

DOI: 10.4324/9781003220534

Typeset in Times New Roman
by codeMantra

Contents

Figures

Tables

Preface

James Carey (2009) describes two things as "things to think with." The first is the work of Harold Innis. "Opening his books is like reengaging an extended conversation," Carey says, "they are not merely things to read but things to think with" (109). While this book most certainly does not equal Innis' work in terms of intellectual acuity, I have followed Innis' tendency to imbue his writings with moral urgency. Rather than deny the role my values played in the writing of this book, as so many academics do, I openly acknowledge and embrace them. Though I am invested in my subject matter, I do not think this undermines the content of the book. To borrow wisdom from the epitaph of the great C. Wright Mills, one might say that "I have tried to be objective. I do not claim to be detached." The book you are holding, then, does not provide answers; it asks questions. It does not offer solutions; it suggests paths. It does not reach conclusions; it explores possibilities. This book does not seek to understand the problems of the world; it seeks to problematize our understanding of the world. In sum, it is not a thing to think *about*; it is a thing to think *with*.

The second thing that Carey refers to as a "thing to think with" is the telegraph. As Carey explains, "the telegraph was not only a new tool of commerce but also a thing to think with, an agency for the alteration of ideas" (157). Carey convincingly demonstrates that the telegraph changed politics, culture, and economics. Cryptography—or crypto for short—has also changed the way many activists and technologists engage the world. Those people are called cypherpunks, and this book is about them and their philosophical outlook, which I call *cypherpunk ethics*. If it seems strange that technology affect human thinking, the next time you use any technology—even, say, a fork or a pencil—instead of asking *What kinds of things can I do with this technology?* You should ask *What kinds of things does this technology ask me to do?* (Ariel used a "dinglehopper" as a comb in *The Little*

Mermaid.) If you can answer this second question for the technologies you use every day, you will appreciate the ways in which technologies alter our thinking. If you can abstract from your personal milieu and ask such questions about technology at the level of the social structure more generally, you will be able to appreciate Carey's insight regarding the telegraph and the cypherpunk insight regarding crypto.

Also following Carey, the discussion in this book relies upon "a useful ethnocentrism" (2). Issues of privacy and transparency are global, and the cypherpunk movement is certainly global in scope and impact. Nevertheless, many of the topics discussed in the following pages derive from the US context. This approach results partly from my situation as an author, but it also results from the nature of the topics themselves. The cypherpunk movement originated in the US, and because the US remains the most powerful surveillance state with the most extensive reach, cypherpunks globally are compelled to respond to the threat it poses. I hope that many of my findings are applicable to other contexts. To the extent they are not, I ask that scholars more knowledgeable about those contexts extend our understanding of the cypherpunks appropriately.

This book contains no disciplinary scholarship. It is a work of what Allen Repko (2008) calls "critical interdisciplinarity," which "aims to interrogate existing structures of knowledge and education, raising questions of value and purpose," and seeks "to transform and dismantle the boundary between the literary and the political, treat cultural objects relationally, and advocate inclusion of low culture" (18). In the following pages, readers will find ideas, texts, theories, and citations from ethics, political theory, economics, history, journalism studies, communication studies, surveillance studies, literary studies, systems theory, philosophy of technology, cryptography, and mathematics, among others. I take this approach for two reasons. First, cypherpunk ethics cannot be neatly crammed into one discipline or field. The cypherpunks represent a dynamic social movement that transcends the artificial disciplinary boundaries of the academy. No successful study of the cypherpunks can take a narrow disciplinary perspective. Second, scholars across the disciplines have called for more interdisciplinary inquiry into the relationship between digital technologies and humanistic values. While I have witnessed technical scholars in mathematics, engineering, and computer science take steps to learn the philosophical and ethical side, I find very few humanities scholars who reciprocate by truly attempting to learn the technical side. In writing this book, I have tried, in a gesture of good faith, to learn more about the technical side of computer science and cryptography, and

though my understanding may be incomplete or even flawed, I nevertheless hope that more humanities scholars will follow this example. If they do, we may successfully bridge the divide between technical and the humanistic.

This book is also designed to be accessible to the widest possible audiences. For that reason, I have taken care to cite sources that are easily available and accessible for all readers. I have referenced student editions of classical texts, and many of the books cited here are available to read for free through the Internet Archive. To insure against changing URLs and disappearing content, the web sources cited in this book have been referenced using the archive.today service whenever possible. Using the URLs in the References will allow you to access the archived webpage along with the original link. I hope readers will not simply take my word for it but seek out and examine the primary sources for themselves. Interested parties should visit the WikiLeaks Bibliography, where they will find further resources for studying and teaching WikiLeaks and related cypherpunk topics (wikileaksbibliography.org).

Now, if I may, a cliché: No book can account for everything relevant to the topic it covers.

Now, if I may, an analogy: In his famous routine on "stuff," comedian George Carlin (1998) observes that houses are just piles of stuff with covers on them. When you leave your house for, say, a vacation, you can't bring *all* your stuff. You can only bring some of your stuff, a *smaller version* of your stuff. Writing a book is the intellectual equivalent to leaving the house: you can't put all your stuff (ideas) into the book, so the book is, by necessity, a smaller version of your stuff. When it comes to the cypherpunks, I have a lot of ideas (all my stuff), some of which is published elsewhere (please check out this stuff), some of which I hope to publish in the future (stuff in storage), and some of which is in this book (the good stuff). In a book of this size, I could only fit some of my stuff, so I brought the stuff I knew I was *really* going to need. Perhaps a teacher somewhere will take a chapter from this book and use it in a class—an *even* smaller version of my stuff. And that's good because I know that at least they do have some of my stuff with them. This analogy works well, but there is a catch. As Carlin asks: Have you ever noticed that other people's stuff is shit and your shit is stuff? I cannot deny the implication of Carlin's question, but I can extend its logic. As you prepare to read this book, holding my shit in your hands, you do not yet know whether you will take up any of the ideas, adopting them as your own. But if you do, then at least some of my shit will have become your stuff.

Acknowledgments

The direct influence of two people made this book possible. The first is my friend John "Curry" O'Day, who rekindled my interest in technology and taught me a great deal of what I know about digital technologies. When we became officemates in graduate school, I didn't even know how the internet worked, but Curry was willing to teach me. He planted the seeds of my interest in digital technologies by patiently explaining VPNs, crypto, net neutrality, severs, surveillance, and many other topics, and he nurtured those seeds throughout our continued friendship. Without Curry's influence, I wouldn't have written this book. I am still a n00b, though, so any mistakes here are the result of my shortcomings as a student not his abilities as a teacher.

The second person is my friend Melba Vélez Ortiz, who insisted that I write my cypherpunk book *now*, not years in the future when I was "planning" to write it. She put me in contact with the right publisher, a fitting series, and a fantastic editor; she also spent countless hours just listening to me talk through ideas. Melba will claim that she didn't do anything, but she helped me work out the entire project. Much of the research here relies upon my knowledge of communication studies, almost all of which I learned from Melba in one way or another. But I am still a n00b in this area, too, which I guess makes me a Noob-Noob. Nevertheless, this project would not be what it is without her encouragement, support, and friendship.

Other people in my life have also supported me while working on this book and more generally. Rocio Alvarez has had a profound influence on my intellectual and personal development, and her friendship and intellectual camaraderie have enriched my life more that I can say. I also would not be the scholar I am today without my academic mentors—Dwayne Tunstall, Terence Hoagwood, and Tommy Curry. I thank all three of these brilliant thinkers for helping me grow as an intellectual and as a person without ever expecting me to become a

mere carbon copy of themselves. Dwayne, Terence, and Tommy always respected my intellectual autonomy, letting me choose my own goals while working tirelessly to help me achieve them. Thank you to Glen Ford and Charles W. Mills for everything you both did for me personally and for the world generally; you are both missed.

I also want to thank Laurence José for giving me an opportunity to teach Ethics of Digital Culture, Alex Nesterenko for encouraging me to pursue a post-postgraduate degree in Communication, and my colleagues at Central State University for welcoming me with open arms. Thanks to Marty Wolf and Colleen Greer for inviting me to participate in the expert panel they organized as part of the Mozilla Responsible Computer Science Challenge; I learned so much from the amazing team they put together. Thank you to Suzanne Richardson and the editorial board at Routledge for believing in this project and in my ability to execute it, and thank you to two anonymous peer reviewers for their praise of the project. Thank you to Marienna Pope-Weidemann for permission to include an adapted version of her diagram of Assange's censorship pyramid. Thanks goes out to the Internet Archive for keeping information free and for enabling me to continue my research when libraries were closed during the pandemic.

I wish to thank my grandparents, parents, brothers, and all the other special people in my life not only for putting up with my BS in general but also for the patience, support, and love they have given me while writing this book and while being a human more generally. Words cannot express my appreciation.

Finally, thank you to Julian Assange, who is perhaps the most dynamic thinker of our time. When you see someone being persecuted by criminal empire controlled by vicious bastards, there's a good chance that person's work has made meaningful contributions to the realization of justice. This book represents my small part in spreading cypherpunk ideas, and I hope to one day see a world saturated with courageous people—a world with many Julians.

1 Introduction

KOKR KFQG GWQC, AQNW FICW DBKF XWDF HID.
—AQCN AKYY WC

Privacy for the Weak, Transparency for the Powerful

In September 1992, a group of approximately 20 computer activists convened in a Berkeley-area living room to discuss their growing concerns about threats to privacy in the digital age (Levy 2001; Greenberg 2012). All who were present at the meeting understood the fundamental truth about digital communication: that it is highly susceptible to third-party interception. When a computer in New York communicates with a computer in Los Angeles, the protocol leaves a permanent, visible record of the connection, and the information transmitted over the network (the content and the metadata) may be surveilled by anyone who happens to be monitoring the transmission. Concern about surveillance was not merely a theoretical matter, for between the 1960s and the 1990s, the US government had been involved in several surveillance scandals (Bamford 1982; Burnham 1983; Levy 2001). With technological and political changes making mass surveillance almost inevitable, these activists agreed that digital cryptography—the "art and science of keeping messages secure" (Schneier 1996, 1)—was the most important tool, the only effective tool, for preserving privacy and free speech in a world increasingly dominated by computers and fiber optic networks. With digital cryptography, or crypto for short, computer users would be able to encipher their communications and their economic transactions using algorithms that not even the most powerful computers could unlock, thereby preventing government agents, corporate spies, and other criminals from monitoring or intercepting information sent across the newly public internet. While the group originally considered the tongue-in-cheek title Cryptology Amateurs

DOI: 10.4324/9781003220534-1

for Social Irresponsibility, they eventually settled on a more fitting name: the cypherpunks.

In the weeks that followed their inaugural meeting, the cypherpunks created a listserv through which they could share ideas. One of the first documents to be shared on the cypherpunk listserv was "A Cypherpunk's Manifesto," written by Eric Hughes, who, with John Gilmore and Timothy C. May, cofounded the movement. In the manifesto, Hughes (2001) articulates the basic philosophical insight of the cypherpunks: that digital communication systems were, by their very nature, antithetical to privacy. Defining privacy as "the power to selectively reveal oneself," Hughes notes that computers undermine this power. "When my identity is revealed by the underlying mechanisms of the transaction," he writes, "I have no privacy. I cannot here selectively reveal myself; I must always reveal myself" (81–82). Hughes observes that "governments, corporations, and other large, faceless organizations" have no incentive to grant computer users privacy; in fact, it is in their interest that computer users have no privacy, for the more information such organizations have, the more power they wield (82). Calling for all computer users to follow the cypherpunks' lead, Hughes declares that he and the other cypherpunks "are defending our privacy with cryptography," for encryption "removes information from the public realm," restoring the power of individuals to selectively reveal themselves to the world (82–83).

Around the same time that the cypherpunks were organizing in the US, the International Subversives, a small group of underground hackers in Australia, turned the question of privacy back against the governments, corporations, and other large, faceless organizations that seemed to threaten the individual (Assange 2011; Dreyfus and Assange 2012). While the cypherpunks concentrated on the ways that the internet permitted institutions to freely access information about individuals, the International Subversives explored the ways that the internet permitted individuals to freely access information about institutions. With their newly acquired modems, the Subversives set out on nightly cyberspace adventures, finding security weaknesses in various academic, corporate, and government computer networks. Some of their targets, such as Melbourne University, were local, but these were primarily used as springboards for accessing other networks around the globe, especially networks within the US. The networks of Lockheed Martin, NASA, the Los Alamos National Laboratory, and the Pentagon's Eighth Command were all penetrated by the Subversives at one point or another (Greenberg 2012, 106). The International Subversives never stole information nor did they destroy any of the networks

to which they gained access, but they learned that the world's most powerful institutions practice extreme secrecy because publics would oppose their activities if such activities came to light.

One member of the International Subversives, Julian Assange, joined the cypherpunks in the mid-1990s. Assange learned about the power of crypto to protect personal communication online, and he agreed with the other cypherpunks that encryption was a necessary means for preserving privacy and free speech in the digital age. But he also saw another use for crypto: institutional transparency. Drawing upon his previous experience seeing behind the veils of institutional power, Assange (2006) composed "Conspiracy as Governance," a short essay in which he argues that "collaborative secrecy"—or conspiracy—is "the key generative structure of bad governance" (1–2). Powerful institutions perpetuate themselves by seeking and concentrating more power, often in ways that would be opposed by adversaries. Applying this insight to modern governments, Assange argues that secrecy is the central enabling factor for all authoritarian rule. "Authoritarian regimes create forces which oppose them by pushing against a people's will to truth, love and self-realization," he writes. "Plans which assist authoritarian rule, once discovered, induce further resistance. Hence such schemes are concealed by successful authoritarian powers until resistance is futile or outweighed by the efficiencies of naked power" (2). Authoritarianism can be resisted, Assange insists, by undermining its most important tool: secrecy. To do this, Assange (2016) argues that encrypted document submission systems can be established, and potential whistleblowers—the people inside the institutions who witness unjust plans or actions—can be encouraged to leak documentary evidence of organizational wrongdoing. By using crypto, therefore, Assange concludes that it is possible to promote transparency and undermine secrecy, thus limiting the capacity of governments—and corporations—to carry out injustices.

Today, we habitually treat issues of personal privacy and issues of government and corporate transparency as largely distinct, but cypherpunks synthesize these issues, combining the original cypherpunk defense of privacy with Assange's call for transparency into a concise slogan: "privacy for the weak, transparency for the powerful" (Assange et al. 2012). For the cypherpunks, privacy and transparency are intimately connected because they both influence the overall flow of information in our modern networked society (de Zwart 2016; Anderson 2021). "The cypherpunks," Suelette Dreyfus observes, believe "in the right of the individual to personal privacy—and the responsibility of the government to be open, transparent and fully accountable

to the public" (Dreyfus and Assange 2012, xii). As cypherpunk Andy Müller-Maguhn puts it, the cypherpunks aim to "use public information" and to "protect private information" (Assange et al. 2012, 141).

Cypherpunks have been criticized for holding a double standard when it comes to privacy, supposedly demanding privacy for themselves while demanding transparency for others (Brin 1998). Such criticisms, however, overlook some important distinctions and thus miss the point. For the cypherpunks, *privacy* is something that individuals and relatively powerless organizations are permitted by right and guaranteed by encryption, while *secrecy* is something that powerful organizations use to hide their nefarious, unjust, and anti-democratic plans. Likewise, *vulnerability* describes the condition of individuals when their personal data is known by others (especially without their knowledge or consent), while *transparency* describes the condition of organizations and institutions when their data is made available to publics. On the individual scale, privacy and vulnerability are inversely related, and the same holds true for transparency and secrecy on the institutional scale. Societies defined by high levels of vulnerability and secrecy will be extremely authoritarian, centralized, and unjust; societies defined by high levels of privacy and transparency will be open, decentralized, and just.

To understand the cypherpunk juxtaposition of privacy and transparency, it is also necessary to recognize that their corresponding concepts, the *weak* and the *powerful*, depend upon an analysis of power. As Huey P. Newton states, "power is the ability to define phenomena and make it act in a desired manner" (Cleaver 2006, 173), and in the digital age, power and communication define each other. In *Cybernetics*, Norbert Wiener (1961) observes that "the present time is the age of communication and control" (39). "Properly speaking," Wiener explains, "the community extends only so far as there extends effectual transmission of information" (157–158). In other words, the boundaries of a community are coextensive with the boundaries of the community's communication technology. In the small town or village, most communication is oral, which limits the extent of the community but also ensures that the means of communication cannot be dominated by any centralized authority. In the large communities of the contemporary world, however, which are bound together by global electronic communication networks, Wiener writes, "the Lords of Things as They Are protect themselves from hunger by wealth, from public opinion by privacy and anonymity, [and] from private criticism by the laws of libel and the possession of the means of communication" (160). Among these methods, Wiener notes, "the control of the means

of communication is the most effective and most important," for when control over such technology becomes concentrated in the hands of a powerful few, "ruthlessness can reach its most sublime levels" (160). In the digital age, then, having power allows one to exert control over communication, and being able to exert control over communication increases one's power.

It is from within this context of power and communication that the cypherpunk slogan must be understood. As Assange (2014) states, neither privacy nor transparency is intrinsically valuable but instead must be understood within "the calculus of power." On the one hand, "the destruction of privacy widens the existing power imbalance between the ruling factions and everyone else." On the other hand, as institutions keep their affairs "secret from the powerless and to the powerful," transparency becomes a means to check such secrecy (Assange et al. 2012, 141). While the internet has been celebrated for its potential to promote democracy, literacy, and autonomy for the people of the world, James Carey (2009) notes that "modern technology invites the public to participate in a ritual of control in which fascination with technology masks the underlying factors of politics and power" (150). In Assange's words, we may be excited about "people being able to Google and search for the blogs of the world and people's comments," but we should not conclude that access to blogs is equivalent to "powerful insiders knowing every credit card transaction in the world" (Assange et al. 2012, 143). The two are not equal: they do not require equivalent degrees of power to achieve, and they do not result in equivalent augmentations of power for the respective parties. Having access to the records of all financial transactions in the world requires special, centralized corporate and governmental power, and it results in far more power than results from reading all the blogs in the world. Thus, by advocating privacy for the weak and transparency for the powerful, the cypherpunks hope to shift the balance of power, taking power from corporate and government elites and returning it to the people.

Hackers, Cyberpunks, and Cypherpunks

To understand the characteristics of the cypherpunk movement, it is necessary to note the ways in which the cypherpunks differ from two other related but ultimately distinct technology-inspired subcultures: *hackers* and *cyberpunks*. Both the hacker ethic and cyberpunk literature exerted some influence over the cypherpunks, but there are important reasons for recognizing the cypherpunks as a movement in their own right.

The hacker subculture emerged among a group of programmers in the computer labs of the Massachusetts Institute of Technology (MIT) in the 1960s; over the next two decades, it migrated to California, where the hardware and video game hackers initiated the personal computer revolution. Despite their geographical and professional differences, the hackers all seemed to share an implicit set of beliefs: that computers could improve people's lives, that access to computers ought to be unfettered, that systems of centralized authority ought to be replaced with decentralized systems, that people should take a hands-on approach to technology, and—perhaps most famously—that all information should be free. By the early 1980s, however, the hacker ethos of openness, sharing, and decentralization had been eclipsed by business imperatives, with emerging computer and software manufacturers facing financial incentives that promoted the development of a closed, proprietary, and centralized culture (Levy 2010). Meanwhile, the revolution in personal computers carried the hacker ethic out of the labs and into private homes, where an international hacker underground emerged. Like their predecessors, underground hackers—including groups like the International Subversives—believed in open, decentralized systems and the freedom of information, but unlike their predecessors, who enacted these values in computer labs isolated from the larger society, underground hackers enacted these values in direct conflict with corporate and government authority. These underground hackers scoffed at the notion that ideas could be owned, and they openly defied centralized authority by penetrating public and private networks with restricted access. The authorities, of course, viewed underground hackers not as a subculture with different values but as criminals in need of punishment. Thus, the early 1990s witnessed an international "hacker crackdown" in which police harassed, sabotaged, and arrested many accused hackers, while corporate-owned media transformed the image of a "hacker" into an existential threat to civilization (Sterling 1992; Hafner and Markoff 1995; Dreyfus and Assange 2012).

Academic accounts of the cypherpunks have, to varying degrees, overemphasized the similarities between hackers and cypherpunks, often obliterating any difference between the two (Coleman and Golub 2008; Villena Saldaña 2011; Marechal 2013; Hellegren 2017; Di Salvo 2020; Jarvis 2021). For one thing, none of the founding cypherpunks were members of the hacker underground. More importantly, the cypherpunk emphasis on cryptography and concern about privacy distinguishes them from hackers. Writing about Whitfield Diffie, one of the pioneers of public key encryption, Levy (2001) explains that

"unlike some of his hacker colleagues, whose greatest kick came from playing in forbidden computer playgrounds, Diffie was drawn to questions of what software could be written to ensure that someone's files could not be accessed by intruders" (10). In fact, in the 1970s, computer scientists "knew almost nothing about cryptography" unless they worked for the National Security Agency (168). Hackers tacitly agreed that "all information should be free," but following Diffie, cypherpunks provided an important corrective to this principle, insisting on a distinction between public information, which ought to be free, and personal information, which ought to be private. While hacker culture has since come to accept the cypherpunk distinction between public and private information (Chaos Computer Club n.d.), it would nevertheless be a mistake to simply equate cypherpunk ethics with hacker ethics.

While the hackers were active on their computers, the *cyber*punk literary movement arose alongside them, articulating an image of technology-based rebellion through science fiction. As a science fiction subgenre, cyberpunk literature imagines dystopian futures defined by technological advancement and social disorder. As Thomas Michaud (2008) explains, "Cyberpunk is a science fiction movement that describes the future of industrial countries, depicting the influence of massive telecommunications networks upon the lives of individuals and societies" (65). Influential cyberpunk novels include William Gibson's *Neuromancer*, in which the protagonist is forced to navigate a dystopian society of underworld criminals, artificial intelligence, and a global network called the "matrix," and Neal Stephenson's *Snow Crash*, in which the digital and the biological are blurred and society is dominated by transnational corporations and privately owned police forces. The cyberpunk genre often combined "high-tech" worlds with "low-life" characters (Sterling 1986, xiv), most of whom represent some abstract type of anarchist or hacker anti-hero (Michaud 2008).

Just as scholars have mistakenly equated cypherpunks with hackers, scholars have tended to blur the distinctions between the cyberpunks and the cypherpunks, subsuming the latter under the title "cyberpunk activism" and arguing that "the cypherpunks were not simply reading [science fiction]; they were putting it into practice" (Milburn 2020, 377). The cypherpunks were influenced by cyberpunk novels and other genres of science fiction (May 2001a, 38); indeed, Jude Milhon coined the movement's name by replacing "cyber" with "cypher" (Levy 2001). Yet there are three important reasons not to reduce the cypherpunks' intellectual and technological contributions to mere extensions of cyberpunk science fiction. First, the intellectual

genealogy of the cypherpunks has its roots not in literature but in the work of the independent cryptographers of the 1970s. Whitfield Diffie and Martin Hellman, who first published a conceptualization of public key encryption, were responding not to science fiction but technological fact. Without their discovery, the cypherpunk movement simple would have been impossible (Levy 2001). Second, there is a political and philosophical tension between cypherpunk ethics and the worlds constructed by cyberpunk authors, for many cypherpunks are anarcho-capitalists who reject the cyberpunk fear of corporate power. Timothy May (2001a), the foremost anarcho-capitalist cypherpunk, insists that "many 'cyberpunk' (not cypherpunk) fiction authors make a mistake in assuming the future world will be dominated by transnational megacorporate 'states'" (64). In May's view, corporations are just as likely as individuals to be victims of the state's ability to wield violence and coercion, and more importantly, he argues that crypto will destroy nation-state governments. Third, key cypherpunk intellectuals have found greater inspiration beyond the cyberpunk authors. For example, Julian Assange (2011, 2015) explicitly mentions George Orwell, Aleksandr Solzhenitsyn, George Jackson, John Milton, and Harold Innis as inspirations but almost never refers to cyberpunk literature. Thus, just as cypherpunk ethics ought to be distinguished from hacker ethics, the cypherpunks ought to be distinguished from cyberpunks. The cyberpunks represent only one among many influences on the cypherpunks, and it would be a mistake to overdetermine that relationship.

Toward a Cypherpunk Ethics

This book provides neither an encyclopedic overview of all things cypherpunk nor a detailed history of the cypherpunk movement and all its major participants. Other works have already provided such accounts (Levy 2001; Manne 2011; Greenberg 2012; Rid 2016; Hellegren 2017; Jarvis 2021). Instead, this book provides a philosophical look at the ethical, political, social, economic, and technological aspects of the cypherpunk worldview—the sum of which I call *cypherpunk ethics*. Given the explicitly political nature of the cypherpunk movement, it may seem intuitive to consider it a manifestation of what has been called "crypto politics," the political constitution of security, privacy, and surveillance by myriad government, corporate, and movement actors (Monsees 2020). Yet, cypherpunk philosophy is about more than the politics of security and privacy. At its roots, the cypherpunk worldview is fundamentally normative, which means it is built upon claims about what people and institutions *ought to do* and what

societies *ought to be like*. Furthermore, the cypherpunks philosophize beyond mere politics, offering conceptions of human nature, theories of meta-ethics, and definitions of freedom. When the cypherpunks demand privacy for the weak and transparency for the powerful, they are calling for a fundamental reorganization of western societies—a reorganization in which governments and corporations do not and cannot track everything a person says and does, a reorganization in which individuals have unfettered access to the technology they need to bring their desires to fruition, a reorganization in which public ideas are freely shared while private information is respected. The following chapters examine some aspects of what a cypherpunk society might look like.

The first half of the book deals with the theoretical aspects of cypherpunk ethics, while the second half deals with the practical aspects. Chapter 2 presents a cypherpunk philosophy of technology, examining the conceptual, technical, and moral dimensions of digital crypto. Rather than providing an overview of cutting-edge developments in cryptography, this chapter explores the basic technical and ethical features of the technology at the heart of all contemporary digital security and privacy: public key encryption. Beginning with a discussion of crypto is essential because the cypherpunk subculture did not create the technology, but rather the technology created the conditions for the subculture to emerge (Assange 2016, 189). Furthermore, cypherpunks prefer technological over legislative solutions to social and ethical issues. As John Gilmore (1991), a founding member of the cypherpunks, puts it: "I want a guarantee—with physics and mathematics, not with laws—that we can give ourselves things like real privacy of personal communications." Thus, cypherpunks often speak of relying on the "laws of physics" rather than the "laws of man" (Assange et al. 2012). Using Ivan Illich's (2009) distinction between manipulative and convivial tools, I argue that the cypherpunks view crypto as a convivial tool.

Because the cypherpunks have never been an ideologically homogenous movement, Chapters 3 and 4 approach cypherpunk philosophy from the viewpoint of moral philosophy and political theory, focusing on two of the movement's most influential thinkers and prolific writers: Timothy C. May and Julian Assange. May has been described as "the Thomas Jefferson of the cypherpunks" (Greenberg 2012, 89), while Assange is "now one of the most prominent exponents of cypherpunk philosophy in the world" (Assange et al. 2012, 7). As Robert Manne (2011) has explained, the cypherpunk movement attracts individuals subscribing to a wide variety of political and ethical views, including anarcho-capitalist libertarians, mainstream conservatives,

left-liberals, Wobblies, Marxists, and others. "The only thing they all shared," Manne notes, "was an understanding of the political significance of cryptography and the willingness to fight for privacy and unfettered freedom in cyberspace." This insight is crucial, for it allows us to see that the cypherpunk slogan "privacy for the weak, transparency for the powerful" is compatible with multiple meta-ethical and political paradigms.

The two paradigms under examination here are May's "crypto anarchy" (his term) and Assange's "crypto justice" (my term). In the chapter on cypherpunk meta-ethics, I juxtapose the moral philosophies of May and Assange to highlight the radical differences between their distinct articulations of cypherpunk philosophy. May's ethics are thoroughly libertarian, grounded in a theory of anarcho-capitalism, while Assange's ethics are a version of virtue ethics, giving priority to the virtues of justice and courage. In the chapter on cypherpunk theories of the state, I demonstrate how May's anarcho-capitalist rejection of the state and Assange's cybernetic theory of the state as a computational network offer competing understandings of government power and surveillance. Some commentators have misinterpreted Assange, claiming that because he is a cypherpunk, he must be a crypto anarchist (Manne 2011; Di Salvo 2020). As these chapters show, however, crypto anarchy and crypto justice provide radically different philosophical foundations for cypherpunk ethics, though each is compatible with the cypherpunk call for privacy and transparency.

Transitioning from the theoretical to the practical, the remaining chapters explore applied cypherpunk ethics through three notions: privacy for the weak, transparency for the powerful, and all information should be free. Chapter 5 investigates the ways in which digital crypto allows cypherpunks to implement privacy for the weak. After establishing a basic understanding of the relationship between data and surveillance, I explore some of the central cypherpunks arguments for privacy and describe a few crypto tools about which the cypherpunks are most excited. This chapter also explores the cypherpunk interest in cryptocurrencies through the structure of Bitcoin. Chapter 6 investigates the ways in which digital crypto allows cypherpunks to implement transparency for the powerful, using WikiLeaks as a paradigmatic example. After situating WikiLeaks within the cypherpunk conceptions of information markets and platforms, I explain the two primary functions of WikiLeaks: to serve as an outlet for leaks that cripple the cybernetic state and to operate a media outlet that practices scientific journalism, the practice of publishing the primary source documents that inform the journalist's reporting.

Chapter 7 turns to one of the primary continuities between the hacker ethic and cypherpunk ethics, showing how the notion that "all information should be free" permeates cypherpunk thinking. For cypherpunks as for hackers, barriers are the enemies of an open culture, which is why both movements oppose censorship and "intellectual property" regulations. Drawing on the works of Richard Stallman and Aaron Swartz, I clarify the basic ideas of the free software and open access movements and why the cypherpunks are ardent supporters of those movements.

The conclusion poses essential questions regarding the future of crypto and cypherpunk ethics for the remainder of the twenty-first century, but such questions are only possible because the future is open, because it depends on what we *do*. James Carey (2009) argues that all electronic media—from the telegraph to the internet—promote the same type of civilization: "a powerhouse society dedicated to wealth, power, and productivity, to technical perfectionism and ethical nihilism." While we might be soothed by rhetorical flourishes and lyrical upsurges, Carey insists that "only the work of politics and the day-by-day attempt to maintain another and contradictory pattern of life, thought, and scholarship" will prevent the worst (131). The cypherpunks agree. In his assessment of the internet, Assange (2014) echoes Carey, first by observing that the future is open and then in calling for concrete political action:

> the Internet is too complex to be unequivocally categorized as a "tyrannical" or a "democratic" phenomenon…[yet] It is too early to say whether the "democratizing" or the "tyrannical" side of the Internet will eventually win out. But acknowledging them—and perceiving them as the field of struggle—is the first step toward acting effectively. Humanity cannot now reject the Internet, but clearly we cannot surrender it either. Instead, we have to fight for it. Just as the dawn of atomic weapons inaugurated the Cold War, the manifold logic of the Internet is the key to understanding the approaching war for the intellectual center of our civilization.

Cheap to produce and even cheaper to spread, crypto becomes the most important tool in the fight for an open future, and cypherpunk ethics provides the intellectual basis for understanding the ethical, political, social, economic, and technological potentialities of crypto in the digital age. As Eric Hughes (2001) concludes the "Cypherpunk's Manifesto," "Let us proceed together apace. Onward" (83).

References

Addley, Esther . 2014. “Julian Assange Has Had His Human Rights Violated, Says Ecuador Foreign Minister.” The Guardian, August 18, 2014. https://archive.md/wraYU.

Amoore, Louise , and Marieke De Goede . 2005. “Governance, Risk, and Dataveillance in the War on Terror.” Crime Law & Social Change 43: 149–173.

Anderson, Patrick D. 2021. “Privacy for the Weak, Transparency for the Powerful: The Cypherpunk Ethics of Julian Assange.” Ethics and Information Technology 23, no. 3: 295–308.

Androutsellis-Theotokis, Stephanos , and Diomidis Spinellis . 2004. “A Survey of Peer-to-Peer Content Distribution Technologies.” ACM Computing Surveys 36, no. 4: 335–371.

Aristotle . 1999. Nicomachean Ethics. Second Edition. Translated and edited by Terence Irwin . Indianapolis: Hackett Publishing Company.

Assange, Julian . 2006. “Conspiracy as Governance.” Cryptome (blog), December 3, 2006. https://archive.fo/kr8Pr.

Assange, Julian . 2010. “Don’t Shoot Messenger for Revealing Uncomfortable Truths.” The Australian, December 7, 2010. https://archive.fo/SmXpG.

Assange, Julian . 2011. Julian Assange: The Unauthorized Biography. Edinburgh: Canongate Books.

Assange, Julian . 2013 “How Cryptography Is a Key Weapon in the Fight against Empire States.” The Guardian, July 9, 2013: http://archive.ph/Mbsx4.

Assange, Julian . 2014. “Who Should Own the Internet?” New York Times, December 4, 2014: https://archive.fo/vxLJd.

Assange, Julian . 2015. “Introduction: WikiLeaks and Empire.” In The WikiLeaks Files: The World According to US Empire, 1–19. New York: Verso.

Assange, Julian . 2016. When Google Met WikiLeaks. New York: OR Books.

Assange, Julian . 2017. Forward to How I Lost by Hillary Clinton. Edited by Joe Lauria . New York: OR Books.

Assange, Julian , Jacob Appelbaum , Andy Müller-Maguhn , and Jérémie Zimmermann . 2012. Cypherpunks: Freedom and the Future of the Internet. New York: OR Books.

Avila, Renata , Sarah Harrison , and Angela Richter . 2017. Women, Whistleblowing, WikiLeaks: A Conversation. New York: OR Books.

Bady, Aaron . 2010. “Julian Assange and the Computer Conspiracy: ‘To Destroy This Invisible Government.’” zunguzungu (blog), November 29, 2010. https://archive.fo/4nIaQ.

Ball, Jared . 2011. I Mix What I Like: A Mixtape Manifesto. Oakland, CA: AK Press.

Bamford, James . 1982. The Puzzle Palace: A Report on NSA, America’s Most Secret Agency. Boston: Houghton Mifflin.

Bamford, James . 2008. The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America. New York: Doubleday.

Barlow, John Perry . 1996. “Selling Wine without Bottles: The Economy of Mind on the Global Net.” In High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace. Edited by Peter Ludlow , 9–34. Cambridge: The MIT Press.

Bearman, Joshua . 2015a. “The Untold Story of Silk Road, Part 1.” Wired, May 2015. https://archive.md/W1RQi.

Bearman, Joshua . 2015b. “The Untold Story of Silk Road, Part 2: The Fall.” Wired, June 2015. https://archive.md/cYv43.

Bell, Jim . 1997. “Assassination Politics.” Cryptome (blog), April 3, 1997. https://cryptome.org/ap.htm.

Benkler, Yochai . 2011. “A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate.” Harvard Civil Rights-Civil Liberties Law Review 46: 311–397.
Blumenthal, Max . 2020. “‘The American Friends’: New Court Files Expose Sheldon Adelson’s Security Team in US spy operation against Julian Assange.” The Greyzone, May 14, 2020. https://archive.md/rezeG
Brin, David . 1998. The Transparent Society: Will Technology Force us to Choose between Privacy and Freedom? Reading, MA: Addison-Wesley.
Brunton, Finn . 2011. “Keyspace: WikiLeaks and the Assange Papers.” Radical Philosophy 166: 8–20.
Brunton, Finn . 2019. Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists who Built Cryptocurrency. Princeton: Princeton University Press.
Burke, Colin . 2020. “Digital Sousveillance: A Network Analysis of the US Surveillant Assemblage.” Surveillance & Society 18, no. 1: 74–89.
Burnham, David . 1983. The Rise of the Computer State: The Threat to our Freedoms, Our Ethics, and Our Democratic Process. New York: Open Road Distribution.
Carey, James . 2009. Communication as Culture: Essays on Media and Society, Revised Edition. New York: Routledge.
Carlin, George . 1998. Brain Droppings. New York: Hyperion.
Chaos Computer Club . n.d. “Hacker Ethics.” Chaos Computer Club. https://archive.md/ujjnP.
Chaum, David . 1985. “Security without Identification: Transaction Systems to Make Big Brother Obsolete.” Communications of the ACM, 28: 1030–1044.
Chen, Adrian . 2011. “The Underground Website Where You Can Buy Any Drug Imaginable.” Gawker, June 1, 2011. https://archive.md/RIWDc.
Cleaver, Eldridge . 2006. Target Zero: A Life in Writing. Edited by Kathleen Cleaver . New York: Palgrave Macmillan.
Coleman, E. Gabriella , and Alex Golub . 2008. “Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism.” Anthropological Theory 8, no. 3: 255–277.
Crary, David . 2013. “Older, Quieter than WikiLeaks, Cryptome Perseveres.” Associated Press, March 9, 2013. https://archive.md/NR1Ge.
“Cypherpunks Write Code.” 2021. “ReasonTV.” November 1, 2021. Documentary, 33:54. https://youtu.be/9vM0oIEhMag.
Daemen, Joan , and Vincent Rijmen . 1999. “The Rijndael Block Cipher: AES Proposal.” Document Version 2, March 9, 1999. https://web.archive.org/web/20070203204845/https://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael.pdf.
de Lagasnerie, Geoffroy . 2019. “Julian Assange for the Future.” In Defense of Julian Assange, edited by Tariq Ali and Margaret Kunstler , 244–250. New York: OR Books.
de Zwart, Melissa . 2016. “Privacy for the weak, transparency for the powerful.” In Comparative Defamation and Privacy Law, edited by Andrew T. Kenyon , 224–245. Cambridge: Cambridge University Press.
Dembart, Lee . 2001. “The End User: Text for the Taking.” New York Times, March 26, 2001. https://archive.vn/JOhuF.
Di Salvo, Philip . 2020. Digital Whistleblowing Platforms in Journalism: Encrypting Leaks. Cham: Palgrave Macmillan.
Diffie, Whitfield , and Martin Hellman . 1976. “New Directions in Cryptography.” IEEE Transactions on Information Theory 22, no. 6: 644–654.

Dorfman, Zach , Sean D. Naylor , and Michael Isikoff . 2021. “Kidnapping, Assassination and a London Shoot-Out: Inside the CIA’s Secret War Plans against WikiLeaks.” Yahoo! News, September 26, 2021. https://archive.md/2sX3Q.

Dreyfus, Suelette , and Julian Assange . 2012. Underground. Edinburgh: Canongate Books.

Durant, Will , and Ariel Durant . 1967. Rousseau and Revolution: A History of Civilization in France, England, and Germany from 1756, and in the Remainder of Europe from 1715, to 1789. New York: MJF Books.

“English Letter Frequency (based on a sample of 40,000 words).” n.d. https://archive.md/m4HhG.

Epstein, Jim . 2018. “Tim May, Father of ‘Crypto Anarchy,’ Is Dead at 66.” Reason, December 16, 2018. https://archive.md/pmpzS.

Fakhoury, Hanni . 2014. “The U.S. Crackdown on Hackers Is Our New War on Drugs.” Wired, January 23, 2014. https://archive.md/AQDoL.

Friedman, David . 2014. The Machinery of Freedom: Guide to a Radical Capitalism. Third Edition. New York: David Friedman.

Gardner, Lloyd C. 2016. The War on Leakers: National Security and American Democracy, from Eugene V. Debs to Edward Snowden. New York: The New Press.

Garner, Richard T. , and Bernard Rosen . 1967. Moral Philosophy: A Systematic Introduction to Normative Ethics and Meta-Ethics. New York: Macmillan.

Gilmore, John . 1991. “Privacy, Technology, and the Open Society.” Computer Professionals for Social Responsibility First Conference on Computers, Freedom, and Privacy, Burlingame, CA, March 28, 1991. https://archive.md/yF4Z3.

Golianopoulos, Thomas . 2010. “The Original WikiLeaker.” The New York Observer, December 8, 2010. https://archive.md/xY4VZ and https://archive.md/hNoZk.

Grabowski, Mark . 2019. Cryptocurrencies: A Primer on Digital Money. New York: Routledge.

Grima, Joseph . 2011. “Open Source Design 01: The Architects of Information.” Domus 948, June 2011. https://archive.md/mXO8o.

Greenberg, Andy . 2012. This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World’s Information. New York: Dutton.

Greenberg, Andy . 2013. “Collected Quotations of the Dread Pirate Roberts, Founder of Underground Drug Site Silk Road And Radical Libertarian.” Forbes, April 29, 2013. https://archive.md/whWOv.

Greenwald, Glenn . 2011. “WikiLeaks cables and the Iraq War.” Salon, October 23, 2011. https://archive.md/pzFl9.

Greenwald, Glenn . 2014. No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. New York: Picador.

Greenwald, Glenn . 2017. “Gina Haspel, Trump’s Pick for CIA Director, Ran a Black Site for Torture.” The Intercept, February 2, 2017. https://archive.md/3ppKB.

Greenwald, Glenn . 2021. “Julian Assange Loses Appeal: British High Court Accepts U.S. Request to Extradite Him for Trial.” Glenn Greenwald (blog), December 10, 2021. https://archive.md/Yayxu.

Gürses, Seda , Arun Kundnani , and Joris Van Hoboken . 2016. “Crypto and Empire: The Contradictions of Counter-Surveillance Advocacy.” Media, Culture & Society 38, no. 4: 576–590.

Hafner, Katie , and John Markoff . 1995. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Touchstone.

Handley, Robert L. , and Lou Rutigliano . 2012. “Journalistic Field Wars: Defending and Attacking the National Narrative in a Diversifying Journalistic Field.” Media,

Culture & Society 34, no. 6: 744–760.
Harrison, Sarah . 2015. “Indexing the Empire.” In The WikiLeaks Files, 145–158. New York: Verso.
Hayase, Nozomi . 2016. “WikiLeaks, 10 Years of Pushing the Boundaries of Free Speech.” Common Dreams, October 4, 2016. https://archive.fo/GRn4u.
Hellegren, Z. Isadora . 2017. “A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom.” Internet Histories 1, no. 4: 285–311.
Hobbes, Thomas . 1994. Leviathan, with selected variants from the Latin edition of 1668. Edited by Edwin Curley . Indianapolis: Hackett Publishing Company.
Holden, Joshua . 2017. The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption. Princeton, NJ: Princeton University Press.
Hsieh, Steven . 2013. “Why Did the Justice System Target Aaron Swartz?” Rolling Stone, January 23, 2013. https://archive.md/qBF5W.
Hughes, Eric . 2001. “A Cypherpunk’s Manifesto.” In Crypto Anarchy, Cyberstates, and Pirate Utopias, edited by Peter Ludlow , 81–83. Cambridge: MIT Press.
Illich, Ivan . 2009. Tools for Conviviality. New York: Marion Boyars.
Innis, Harold A. 2007. Empire and Communications. Lanham, MD: Rowman & Littlefield.
Innis, Harold A. 2008. The Bias of Communication. Second Edition. Toronto: University of Toronto Press.
Jarvis, Craig . 2021. Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption. Boca Raton, FL: CRC Press.
Kahn, David . 1967. The Codebreakers: The Story of Secret Writing. New York: Macmillan.
Khatchadourian, Raffi . 2010. “No Secrets: Julian Assange’s Mission for Total Transparency.” New Yorker, June 7, 2010. https://archive.fo/nspvA.
Lee, Timothy B. 2013. “The Inside Story of Aaron Swartz’s Campaign to Liberate Court Filings.” Ars Technica, February 8, 2013. https://archive.md/VXuSS.
Levy, Steve . 2001. Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age. New York: Penguin.
Levy, Steve . 2010. Hackers: Heroes of the Computer Revolution—25th Anniversary Edition. Cambridge: O’Reilly Media, Inc.
“Link Encryption vs. End-to-End Encryption.” 2009. Logical Security (blog), December 29, 2009. https://archive.md/o2SpF.
Locke, John . 1980. Second Treatise of Government. Edited by C. B. Macpherson . Indianapolis: Hackett Publishing Company.
Lynch, Lisa . 2012. “‘That’s Not Leaking, It’s Pure Editorial’: Wikileaks, Scientific Journalism, and Journalistic Expertise.” Canadian Journal of Media Studies (Fall): 40–69.
Lynch, Lisa . 2013. “The Leak Heard Round the World? Cablegate in the Evolving Global Mediascape.” In Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society, edited by Benedetta Brevini , Arne Hintz , and Patrick McCurdy , 56–77. New York: Palgrave Macmillan.
Manne, Robert . 2011. “The Cypherpunk Revolutionary.” The Monthly, February 16, 2011. https://archive.fo/kwI60.
Marechal, Natalie . 2013. “WikiLeaks and the Public Sphere: Dissent and Control in Cyberworld.” The International Journal of Technology, Knowledge, and Society 9: 93–106.
Martin, Keith . 2020. Cryptography: The Key to Digital Security, How It Works, and Why it Matters. New York: W. W. Norton.
May, Timothy C. 1996a. “Introduction to BlackNet.” In High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace, edited by Peter Ludlow , 241–243. Cambridge: The MIT Press.

May, Timothy C. 1996b. “BlackNet Worries.” In High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace, edited by Peter Ludlow , 245–249. Cambridge: The MIT Press.
May, Timothy C. 2001a. “True Nyms and Crypto Anarchy.” In True Names and the Opening of Cyberspace, edited by James Frenkel , 33–86. New York: TOR Books.
May, Timothy C. 2001b. “A Crypto Anarchist Manifesto.” In Crypto Anarchy, Cyberstates, and Pirate Utopias, edited by Peter Ludlow , 61–63. Cambridge: MIT Press.
May, Timothy C. 2001c. “Crypto Anarchy and Virtual Communities.” In Crypto Anarchy, Cyberstates, and Pirate Utopias, edited by Peter Ludlow , 65–79. Cambridge: MIT Press.
May, Timothy C. 2018. “Enough with the ICO-Me-So-Horny-Get-Rich-Quick-Lambo Crypto.” Coindesk, October 19, 2018. https://archive.md/zojKA.
McShea, Robert J. 1979. “Human Nature Ethical Theory.” Philosophy and Phenomenological Research 39, no. 3: 386–401.
Melzer, Nils . 2019. “Demasking the Torture of Julian Assange.” Medium (blog), June 26, 2019. https://archive.md/nigOm.
Michaud, Thomas . 2008. “Science Fiction and Politics: Cyberpunk Science Fiction as Political Philosophy.” In New Boundaries in Political Science Fiction, edited by Donald M. Hassler and Clyde Wilcox , 65–77. Columbia: The University of South Carolina Press.
Milan, Stefania , and Lonneke van der Velden . 2016. “The Alternative Epistemologies of Data Activism.” Digital Culture and Society 2, no. 2: 57–74.
Mill, John Stuart . 1873. Considerations on Representative Government. New York: Harper & Brothers.
Milburn, Colin . 2020. “Activism.” In The Routledge Companion to Cyberpunk Culture, edited by Anna McFarlane , Lars Schmeink , and Graham Murphy , 373–381. New York: Routledge.
Mitcham, Carl . 1994. Thinking through Technology: The Path between Engineering and Philosophy. Chicago: University of Chicago Press.
Mitchell, Greg . 2008. So Wrong for So Long: How the Press, the Pundits—and the President—Failed on Iraq. New York: Union Square Press.
Monsees, Linda . 2020. Crypto-Politics: Encryption and Democratic Practices in the Digital Era. New York: Routledge.
Moore, Adam . 2011. “Privacy, Security, and Government Surveillance: WikiLeaks and the New Accountability.“ Public Affairs Quarterly 25, no. 2: 141–156.
Nakamoto, Satoshi . 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System.” October 31, 2008. https://bitcoin.org/bitcoin.pdf.
Narayanan, Arvind . 2013a. “What Happened to the Crypto Dream?, Part 1.” IEEE Security & Privacy 11, no. 2: 75–76.
Narayanan, Arvind . 2013b. “What Happened to the Crypto Dream?, Part 2.” IEEE Security & Privacy 11, no. 3: 68–71.
Nozick, Robert . 1974. Anarchy, State, and Utopia. New York: Basic Books.
O’Day, John C. 2019. “Corporate Media Have Second Thoughts about Exiling Julian Assange from Journalism.” Fairness & Accuracy in Reporting, June 5, 2019. https://archive.fo/ry6Ik.
Peters, John Durham . 1999. Speaking into the Air: A History of the Idea of Communication. Chicago: University of Chicago Press.
“Philosophy of the GNU Project.” n.d. Free Software Foundation, Inc. https://archive.md/WLFz6.
Pope-Weidemann, Marienna . 2013. “Review of *Cypherpunks: Freedom and the Future of the Internet* .” Counterfire, September 13, 2013. https://archive.md/Oyczc.

Prathap, Madana . 2021. “Bitcoin Does Not Make Payments Anonymous—Just Really Hard to Trace.” Business Insider India, August 5, 2021. https://archive.md/AqYLh.
“Proprietary Software Is Often Malware.” 2021. Free Software Foundation, Inc. https://archive.md/uxhz3.
Repko, Allen . 2008. Interdisciplinary Research: Process and Theory. Thousand Oaks, CA: Sage Publications.
Rexhepi, Piro . 2016. “Liberal Luxury: Decentering Snowden, Surveillance, and Privilege.” Big Data & Society (July–December): 1–3.
Rid, Thomas . 2016. Rise of the Machines: A Cybernetic History. New York: W. W. Norton.
Rivest, Ron , Adi Shamir , and Leonard Adleman . 1978. “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.” Communications of the ACM 21, no. 2: 120–126.
Rogaway, Phillip . 2015. “The Moral Character of Cryptographic Work.” Cryptology ePrint Archive, Report 2015/1162. https://ia.cr/2015/1162.
Rosen, Armin . 2014. “A Radical Pro-Transparency Website Is Raising Money to Annoy Glenn Greenwald.” Business Insider, May 30, 2014. https://archive.md/UWSCK.
Rousseau, Jean-Jacques . 1987. Basic Political Writings. Translated and edited by Donald A. Cress . Indianapolis: Hackett Publishing Company.
Rubenfeld, Jed . 2008. “The End of Privacy.” Stanford Law Review 61: 101–161.
Schmidt, Michael . 2013. “Ex-C.I.A. Officer Sentenced to 30 Months in Leak.” New York Times, January 25, 2013. https://archive.md/r0IDu
Schneier, Bruce . 1996. Applied Cryptography. Second Edition. New York: John Wiley & Sons, Inc.
Shane, Scott . 2010. “Keeping Secrets WikiSafe.” The New York Times, December 11, 2010. https://archive.fo/Ah54H.
Singh, Simon . 2000. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. New York: Anchor Books.
Stallman, Richard . 2005. “Bill Gates and Other Communists.” Free Software Foundation, Inc. https://archive.md/6L2x9.
Stallman, Richard . 2021. “Why Open Source Misses the Point of Free Software.” Free Software Foundation, Inc. https://archive.md/Y1E2k.
Sterling, Bruce . 1986. Preface to Burning Chrome, xi–xiv. Written by William Gibson . New York: Harper Collins.
Sterling, Bruce . 1992. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York: Bantam Books.
Sterling, Bruce . 2010. “The Blast Shack.” Webstock, December 22, 2010. https://archive.md/eZFZC.
Suber, Peter . 2015. “Open Access Overview.” December 5, 2015. https://archive.ph/OFwDw.
Swartz, Aaron . 2008. “Guerilla Open Access Manifesto.” July 2008. https://archive.org/stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt.
Taylor, Sven . 2017. “VPNs are Lying about Logs.” Restore Privacy (blog), October 8, 2017. https://archive.md/w9Us1.
Turner, Fred . 2006. From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism. Chicago, IL: University of Chicago Press.
“UN expert says ‘Collective Persecution’ of Julian Assange Must End Now.” 2019. United Nations Office of the High Commissioner for Human Rights. May 31, 2019. https://archive.fo/xZ2Zq.

van der Vlist, Fernando N. 2017. “Counter-Mapping Surveillance: A Critical Cartography of Mass Surveillance Technology After Snowden.” Surveillance & Society 15, no. 1: 137–157.
Van Hoboken, Joris V. J. 2014. “Privacy and Security in the Cloud: Some Realism about Technical Solutions to Transnational Surveillance in the Post-Snowden Era.” Maine Law Review 66, no. 2: 487–534.
Villena Saldaña, David . 2011. “Julian Assange: periodismo, científico, conspiración y ética hacker.” Quehacer 181: 58–69.
Vine, David . 2015. Base Nation: How U.S. Military Bases Abroad Harm America and the World. New York: Metropolitan Books.
Webster, Frank . 2006. Theories of the Information Society. Third Edition. New York: Routledge.
Wiener, Norbert . 1961. Cybernetics: Or Control and Communication in the Animal and the Machine. Second Edition. Cambridge: MIT Press.
“WikiLeaks founder Julian Assange on the ‘War Logs’: ‘I Enjoy Crushing Bastards.’” 2010. Spiegel, July 26, 2010. https://archive.fo/yLNN.
Zuboff, Shoshana . 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs.