Ethics and Information Technology (2021) 23:295–308
https://doi.org/10.1007/s10676-020-09571-x

ORIGINAL PAPER

Privacy for the weak, transparency for the powerful: the cypherpunk ethics of Julian Assange

Patrick D. Anderson[1]

Published online: 31 October 2020

Abstract
WikiLeaks is among the most controversial institutions of the last decade, and this essay contributes to an understanding of WikiLeaks by revealing the philosophical paradigm at the foundation of Julian Assange's worldview: cypherpunk ethics. The cypherpunk movement emerged in the early-1990s, advocating the widespread use of strong cryptography as the best means for defending individual privacy and resisting authoritarian governments in the digital age. For the cypherpunks, censorship and surveillance were the twin evils of the computer age, but they viewed encryption as a means to circumvent both. As a cypherpunk, Assange advocates for the use of cryptography in the fight for individual privacy as well as the fight for global justice. His cosmopolitan disposition is informed by his hacker background, antiwar principles, and Enlightenment outlook. This essay places Assange's philosophical idea in historical context, exploring his views on censorship, surveillance, and the right to communicate. It also connects his cypherpunk principles to WikiLeaks, showing that the strategy of encouraging data leaks from powerful political and economic organizations is classic cypherpunk political praxis.

Keywords WikiLeaks · Cypherpunk · Cryptography · Surveillance · Censorship · Whistleblowing

> I am not an original political thinker, never claimed to be, but I know the technology and I understand the structures of government; and I was ready to throw the latter, where possible, into a bath of acid and boil them down to the bone.
> –Julian Assange (2011, p. 129).
> There are few original ideas in politics. In the creation of WikiLeaks, Julian Assange was responsible for one.
> –Robert Manne (2011).

When WikiLeaks is discussed in academic circles, the organization and its actions are almost always analyzed by using established philosophical theories, which are imposed upon WikiLeaks from the outside. Graham Hubb (2014) has analyzed WikiLeaks using Rousseauean social contract theory, arguing that within a Rousseauean theory of democracy, the practices of WikiLeaks are, albeit imperfectly, consistent with the basic functions of the press. Similarly, Edward Spence (2012) has investigated WikiLeaks' relation to the ethics of secrecy and transparency using the classic conceptions offered by Sissela Bok (1989), concluding that WikiLeaks plays an important democratic role by informing publics of government abuses. Finally, Adam Moore (2011) argues that WikiLeaks provides an occasion to question the central justifications of government mass surveillance, noting that the very institutions claiming people should not fear such surveillance if they have "nothing to hide" vociferously condemn transparency when it is turned back upon themselves. Until mass surveillance agencies take the initiative to be more transparent, Moore concludes, organizations like WikiLeaks are necessary.[1]

Notwithstanding the illuminating aspects of such analysis, one thing that is missing form them all is any analysis of Julian Assange's own writings and philosophies. Because academic accounts of WikiLeaks have largely failed to account for the principles upon which it is based, many analyses have misinterpreted WikiLeaks. There is, for instance, a tendency to incorrectly view Assange as an advocate of "radical transparency" (Marechal 2013) or "total transparency" (Wisnewski 2016). "Even as he portrays himself as a radical transparency activist," Nathalie Marechal (2013) writes in

✉ Patrick D. Anderson
anderpat@gvsu.edu

[1] Philosophy Grand Valley State University, Mackinac Hall, B3-105, Allendale, MI 49401, USA

[1] To insure against changing URLs and disappearing content, most of the web sources cited in this article are referenced using the "archive.fo" service. Going to the URLs in the References will allow you to access the archived webpage and also access the original link.

a representative passage, "Assange's actions belie a fierce commitment to protecting his own privacy…This double standard seems prevalent among transparency radicals" (p. 98). Yet Assange (2011) is quite clear that he distinguishes between personal privacy and institutional transparency:

> The issue of privacy would always haunt me. It haunts me now. At WikiLeaks, I would come to seem the arch-proponent of transparency, forever described as the man who thinks all privacy is bad: rather the opposite. We fought, as cypherpunks, to protect people's privacy. What I opposed, and continue to oppose, is the use of secrecy by institutions to protect themselves against the truth of the evil they have done. This is a clear distinction. (p. 86, emphasis added).

The key term in Assange's statement is cypherpunk, a reference to a movement that emerged in the early-1990s, advocating the widespread use of strong cryptography as the best means for defending individual privacy and resisting authoritarian governments in the digital age. "At the core of the cypherpunk philosophy," Robert Manne (2011) explains, "was the belief that the great question of politics in the age of the internet was whether the state would strangle individual freedom and privacy through its capacity for electronic surveillance or whether autonomous individuals would eventually undermine and even destroy the state through their deployment of electronic weapons newly at hand." For the cypherpunks, censorship and surveillance were the twin evils of the computer age, but they viewed encryption as a means to circumvent both. For that reason, Manne observes, "The deepest institutional enemy of the cypherpunks was the National Security Agency." The cypherpunks were sounding the alarm long before Edward Snowden blew the whistle on National Security Agency (NSA) mass surveillance (Greenwald 2014). As "one of the most prominent exponents of cypherpunk philosophy in the world," it comes as no surprise that Assange believes "cryptography is the ultimate form of non-violent direct action" in the fight against surveillance agencies and other powerful organizations (Assange et al. 2012, p. 5). What's more, recognizing Assange's connection to the cypherpunk movement reveals why "radical transparency" is not an adequate label for WikiLeaks or for Assange's worldview. Assange's fundamental principle is not radical transparency but "the traditional cypherpunk juxtaposition": "privacy for the weak, transparency for the powerful" (Assange et al. 2012, p. 7).

This essay seeks to correct misinterpretations of WikiLeaks and Assange's worldview by offering an account of Julian Assange's cypherpunk ethics, expanding our understanding of WikiLeaks as an institution of what has been called the networked fourth estate (Benkler 2011). In the journalistic world, Assange's cypherpunk connections are well known (Manne 2011; Greenberg 2012), but despite Assange having coauthored a book titled Cypherpunks: Freedom and the Future of the Internet, academics have not taken sufficient notice. Entire published volumes explore the connections between WikiLeaks, journalism, ethics, and technology, but they do so without giving serious consideration to the ways in which cypherpunk philosophy informs Assange's political and journalistic activities (Brevini, Hintz & McCurdy 2013; Taylor 2017; Marmura 2018). When it comes to WikiLeaks, most scholarship focuses on the legality (Benkler 2011) or morality (Delmas 2015; Boot 2019) of WikiLeaks' publishing practices, but almost no one focuses on WikiLeaks' foundational principles. When scholars have situated Assange within the world of technology activism, he is commonly referred to as a "hacker" (Villena Saldaña 2011; Marechal 2013), and while there is some truth to this, Assange's roots are more firmly grounded in the cypherpunk movement, which itself is a subset of the broader hacker movement. Assange was influenced by the cypherpunks' celebration of cryptography, their passion for free speech, and their suspicion of powerful, concentrated organizations, but he was also influenced by cypherpunk conceptions of transparency and whistleblowing. In 2010, after WikiLeaks began publishing the Defense Department (DOD) and State Department documents leaked by Chelsea Manning, science fiction writer Bruce Sterling proclaimed: "At last—at long last—the homemade nitroglycerin in the old cypherpunks blast shack has gone off" (qtd. in Manne 2011). Sterling's remark makes sense because he understood that WikiLeaks did not manifest from nothing—it emerged from the cypherpunk tradition as a method for achieving transparency for the powerful.

Importantly, what follows is neither a normative argument regarding any specific technology nor a defense of cypherpunk philosophy in response to its critics. Instead, the argument here is descriptive, claiming that the best way to understand WikiLeaks is to understand how Assange built the organization on a foundation of cypherpunk-inspired principles. While many scholars have criticized WikiLeaks, they have done so without engaging the principles upon which WikiLeaks is founded. Any criticisms or condemnations of WikiLeaks that do not compellingly demonstrate that cypherpunk philosophy is a logically or morally problematic basis for a journalistic or activist worldview will not have provided an adequate account. Thus, this essay changes the terms of the debate when it comes to WikiLeaks. Rather than merely analyzing WikiLeaks using theories already familiar to scholars, scholars ought to first familiarize themselves with the theories that provide impetus for the creation of WikiLeaks.

The essay is organized into two major sections. The first major section offers a genealogy of cypherpunk philosophy, providing an overview of the movement's central principles—privacy for the weak and transparency for the powerful—in historical context. Though there is ideological

diversity among the cypherpunks, they share a passion for freedom of speech, a dedication to defending personal privacy, and an enthusiasm for governmental transparency. The second major section explains Assange's particular interpretation of cypherpunk ethics and use of cypherpunk tools. Because Assange was influenced by the antiwar movement, the Australian underground hacking scene, and Enlightenment philosophy, he offers a cosmopolitan version of cypherpunk ethics with geopolitical applications. Assange also believes that the right to communicate—which consists of the right to know and the right to speak—is perhaps the most important political principle of the digital age. While the right to communicate is threatened by censorship and surveillance, cryptography uses the laws of nature to secure that right against violations by governments and corporations. Finally, Assange synthesizes his Enlightenment conception of the state with the cypherpunk praxis of leaking to offer a theory of non-violent resistance in the face of secretive, authoritarian government. Neither Julian Assange's philosophical views nor the existence of WikiLeaks can be fully appreciated, understood, analyzed, or critiqued without accounting for Assange's commitment to a distinctive paradigm of cypherpunk ethics.

A genealogy of cypherpunk philosophy

Lee Wilkins (2018) convincingly argues that there is an intimate, reciprocal connection between theory and practice, and one implication of this view is that practitioners ought to also be understood as theorists in their own right. When it comes to studying WikiLeaks and treating Assange as a theorist, we gain the best understanding of his worldview by placing into historical context—and the most important context from which Assange's thought emerges is the cypherpunk movement. As Finn Brunton (2011) argues, we cannot merely impose established philosophical ideas onto communities of technology activism; instead, we must "understand the culture and the ethics of hackers and cryptographers in which they were nurtured—a culture that prizes elegant solutions to complex problems, transparency for organizations and privacy for individuals, and the free circulation of knowledge, all of which we find embedded in WikiLeaks" (p. 9). Here, Brunton not only succinctly captures the normative cypherpunk principle "privacy for the weak, transparency for the powerful," he also corroborates Wilkins' (2018) observation, reminding us that we must seek the origins of Assange's principles in the historical context of practice. Thus, it is necessary to understand the origins of the cypherpunk movement and the manner in which their calls for "privacy for the weak" and "transparency for the powerful" manifested form concrete action against government and corporate power. This section provides a brief genealogy of cypherpunk ethics, placing the movement's two basic principles into the context of its activism.

Cypherpunk origins

In the wake of United States government scandals—such as Watergate, the Vietnam War, and COINTELPRO—the 1970s witnessed increased levels of suspicion about the most powerful institutions in society, and it was in this context that the cypherpunk movement was born. The cypherpunks officially named their movement in September 1992, but it emerged out of the broader hacker culture that surrounded the development of computing technologies since the 1950s and coalesced in Silicon Valley in the 1980s (Levy 2001; Greenberg 2012). Tech journalist Steve Levy (2010) traces the development of computer culture in the United States from the 1950s to the 1980s, synthesizing observations and interviews that run the gamut from PhDs working in university laboratories to the hobbyists developing hardware and software in their suburban garages. Despite the wide variety of persons involved, Levy explains, "I found a common element, a common philosophy that seemed tied to the elegantly flowing logic of the computer itself. It was a philosophy of sharing, openness, decentralization, and getting your hands on machines at any cost to improve the machines and to improve the world" (vii). Distilling what he calls "the hacker ethic" into basic principles, Levy identifies some ideas that seemed pervasive in the culture, including, "Access to computers… should be unlimited and total," "All information should be free," "Mistrust Authority—Promote Decentralization," and "Computers can change your life for the better" (pp. 23–32). The hacker ethic gave rise to a worldview that demanded speech be absolutely free, power be purposely decentralized, and computers be widely accessible.

By the early 1990s, attempts by the United States government to restrict the public's access to strong digital cryptography inspired a meeting of cryptology enthusiasts living in the Bay Area (Levy 2001; Greenberg 2012). The crew was motley, to be sure, but every participant shared the hacker's ethic. There are three recognized founders of the movement. Timothy May, who retired from Intel in 1986, was a libertarian programmer influenced by Ayn Rand and Friedrich Nietzsche. Eric Hughes, who studied cryptography with the famous David Chaum, was a mathematician and programmer seeking admittance to graduate school. And John Gilmore, who retired from Sun Microsystems in 1986, was a programmer and cofounder of The Electronic Frontier Foundation (EFF) with John Perry Barlow and Mitch Kapor. Though the group initially called itself Cryptology Amateurs for Social Irresponsibility, the movement would receive its permanent name from Jude Milhon, who coined the name cypherpunk by combining the word "cipher" from cryptographic lingo with the word "cyberpunk," a science fiction

subgenre that imagines dystopian futures defined by technological advancement and social disorder (Michaud 2008).

Privacy for the weak

The cypherpunk founders wrote manifestos describing their visions for the future, and one of their principle aspirations was to ensure privacy for the weak. In his "Crypto Anarchist Manifesto," May (2001a) argued that "Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions" (p. 62). Likewise, in "A Cypherpunk's Manifesto," Hughes (2001) argued that cryptography was the silver bullet for defending privacy in "the electronic age." Because "we cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence," Hughes insisted, "we must defend our own privacy if we expect to have any" (pp. 81–82). After their first meeting, the group established the cypherpunk mailing list to exchange ideas; the list attracted interested parties from all over the world, including a young Australian hacker named Julian Assange. For the cypherpunks, cryptography was the key to preserving individual liberties in the digital age.

Though the cypherpunks evangelized cryptography, they did not invent it. Rather, they took inspiration from other expert mathematicians and computer scientists to came before them. Cryptography has been around for centuries—any kid who has used a decoder ring to decipher a message on the back on a comic book has used cryptography. Imagine that Alice wants to exchange private messages with Bob over time and space. Alice beings by writing her message in plaintext, then she uses a key to encrypt the message, rendering it into ciphertext. Alice transmits the encrypted message so no one else can read it while it is in transit, and once Bob receives the encrypted message, he uses the same key to decrypt the message, rendering the ciphertext into plaintext and making Alice's message intelligible. Historically, cryptography has been symmetrical, meaning that the same key is used both by the sender to encrypt the message and by the receiver to decrypt the message. But there is an important logistical problem with symmetric keys: how do Alice and Bob share keys without meeting the each other in person? After all, if they merely send the key, an eavesdropper, Eve, may intercept it, thus enabling her to decipher all future messages between the Alice and Bob.

In the 1970s, mathematicians Whitfield Diffie and Martin Hellman (1976) solved this problem by discovering asymmetric encryption. Often referred to as public key encryption, the Diffie–Hellman protocol uses two different keys: one used by the sender to encrypt the message, and one used by the receiver to decrypt the message. Mathematically, this process is enabled by the extreme difficulty of factoring the product of two very large prime numbers, a system infinitely stronger than decoder rings. For instance, if we multiply 2 by 3, we get 6, a small enough number to easily factor; however, if 2 and 3 are both replaced by, say, 156 digit prime numbers, almost no existing computer can factor the product of those numbers. Returning to the example, Bob gives Alice his public key, which is the product, and Alice will use that key to encrypt all messages sent to Bob; meanwhile, Bob keeps the private key, which is the two prime factors, and uses it to decrypt all messages received from Alice. Now Bob is free to send his public key to Alice without worrying that Eve will intercept it; even if she does intercept it, the public key is useless to Eve because it only encrypts and does not decrypt. Only Bob has the key that decrypts (Mann 2002; Levy 2001; Schneier 2015). The discovery of public key encryption and the software developed to use it were essential tools for the cypherpunks, who primarily communicated over the internet with people whom they would never meet.

Between the time that Diffie and Hellman discovered public key encryption and the emergence of the cypherpunks, two important individuals saw the potential for cryptography to defend individual privacy in the digital age: David Chaum and Phil Zimmerman. Chaum—who has been called "the prophet and godfather of digital anonymity" (Greenberg 2012 p. 65) and "the ultimate cypherpunk" (Levy 2001 p. 213)—was a mathematician with a concern about the traceability of personal communications and transactions in national and global computerized systems. Taking his cue from David Burnham's (1983) The Rise of the Computer State, which presciently warned of the dangers of massive computerized bureaucracies and databases that enable the tracking of every individual's actions, Chaum (1985) argued that "The foundation is being laid for a dossier society, in which computers could be used to infer individuals life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions" (p. 1030). The answer, he insisted, was to adapt the Diffie-Hellman protocol for use in personal communications and economic transactions.[2] Chaum had a direct influence on the cypherpunks. Not only was May singularly inspired by his work, but Hughes also studied under him (Levy 2001; Greenberg 2012). Similarly, Zimmerman also sought to make public key encryption available for individual use, and during the 1980s, he worked day and night to write his ground-breaking code, Pretty Good Privacy (PGP). When he found out that the United States government was proposing legislation to

[2] David Chaum's work in cryptography and blockchains would provide the foundations for cryptocurrencies, including his own DigiCash and the more well-known Bitcoin. See Chaum (1981), and Danezis and Diaz (2008).

restrict the private use of strong public key encryption, Zimmerman rushed to make PGP available, for free, on the internet. Within 24 h, people from all over the world had downloaded his code; PGP was so popular that, in under a year, Zimmerman worked with other programmers to develop an improved 2.0 version, which the cypherpunks discussed at their first meeting (Levy 2001; Greenberg 2012).

The cypherpunks embraced the works of Chaum and Zimmerman on principle, but they also sided with Zimmerman as he inadvertently catalyzed what is known as the Crypto Wars (Levy 2001; Greenberg 2012).[3] At the time that Zimmerman distributed PGP, cryptography was classified as munitions by the United States government and thus subject to strict domestic distribution regulations and even more strict export regulations. Because people in other countries downloaded PGP, the Bill Clinton administration threatened to charge Zimmerman with unlawfully exporting munitions. But he and the cypherpunks fought back, and their primary weapon was the First Amendment. While Zimmerman worked with a publisher to get PGP printed in a book, Gilmore perused the Library of Congress for classified and unclassified government papers on cryptography, made copies of them, and distributed them online, essentially daring the government to come after him.

Meanwhile, the Clinton administration was proposing two of its own solutions (Levy 2001; Greenberg 2012). First, they proposed the "key escrow" system. Under this plan, all personal computers would contain a cryptographic chip, developed by the National Security Agency (NSA), that would allow the government to keep copies of all users' private keys. Second, the administration sought to require private companies to build "backdoors" into encryption systems so the government could access encrypted data when agents had obtained a warrant. The problem with both proposals is that they are utterly insecure: if the government can access the "backdoor," so can anyone, and public opposition to both plans was immediate and unequivocal. In the end, as Levy (2001) shows, a federal court ruled in favor of Zimmerman, Gilmore, and others on First Amendment grounds. "Government attempts to control encryption…may well implicate not only First Amendment rights of cryptographers," wrote Judge Betty Fletcher, "but also the constitutional rights of each of us as potential recipients of encryption's bounty." In Levy's estimate, "Judge Fletcher was a cypherpunk in robes" (p. 302). With this ruling, the cypherpunks had won an important victory against the United States government at the turn of the millennium, and they had used the First Amendment to do it.

Transparency for the powerful

Though the cypherpunks were busy defending individual privacy in the Crypto Wars, that did not stop them from pursuing their principle aspirations, transparency for the powerful, beginning what would become a long-standing tradition among cypherpunks: publishing leaked documents (Greenberg 2012). In the 1990s, John Young, a veteran of the student movement of the 1960s and "the spiritual godfather of online leaking," took the lead, founding the website Cryptome.org, which hosted many types of documents, including blogs (Assange's among them) and leaked documents from governments and corporations. Over the years, Young's website repeatedly attracted the attention of the United States government, and he was often contacted by agents from the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS). The website, which used a modest email address and a PGP public key to receive submissions, had published the names of thousands of secret agents from the United States, United Kingdom, and Japan; it had also disclosed documents revealing collusion between the government and companies like Microsoft, Cisco, and AT&T. In 2005, Young published leaked maps of Dick Cheney's secret bunker, which resulted in a Reader's Digest story that suggested Cryptome.org was an invitation to terrorists. When asked about his publishing activity, Young pointed inquisitors to a comment made by former NSA council Stewart Baker: "If material is leaked to you, you can probably publish that…Unfortunately, it's not illegal to be a jerk" (qtd. in Greenberg 2012, p. 101).

Like Young, Tim May was also interested in publishing leaks, which he not only wrote about but also designed software for (Greenberg 2012). In a short essay titled "Crypto Anarchy and Virtual Communities," May (2001b) argues that virtual communities—transnational organizations that were, much like the cypherpunks, forming across the newly-available internet—would be subjected to police state rule if they failed to use cryptography. Rendering these communities into a network model, May says that all such communities exist on a spectrum of transparency and opacity in relation to the state. "An interesting way to view issues of network invisibility is in terms of the transparency of nodes and links between nodes," May writes. "Transparent means visible to outsiders, perhaps those in law enforcement or the intelligence community. Opaque means not transparent, not visible" to those same authorities. In a police state, "transparent links and nodes are the norm" because communication channels are tapped, and private use of computers is restricted" (p. 68). Interestingly, not only can encryption can be used to protect virtual communities from being spied on

[3] During the 1990s, Crypto Wars 1.0 (as it is called now) raged (see Levy 2001), but following Edward Snowden's revelations of NSA mass surveillance in 2013, Crypto Wars 2.0 emerged. The most famous battle of Crypto Wars 2.0 was the FBI's attempt to pressure Apple to break compromise the encryption on the iPhone's software. For more, see Meinrath and Vitka (2014).

by law enforcement and intelligence agencies, May argues, but it can also be used by whistleblowers who want to publish secret information anonymously (p. 72).

May does not further elaborate on this insight in the essay, but in a discussion of his prototype whistleblowing program, BlackNet, on the cypherpunk mailing list, he articulated the idea at the foundation of WikiLeaks: "No More Secrets". May continued:

> A subtle point: crypto-anarchy doesn't mean a "no secrets" society; it means a society in which individuals must protect their own secrets and count on governments or corporations to do it for them. It also means "public secrets," like troop movements and stealth production plans, or the tricks of implanting wafers, will not remain secret for long. (qtd. in Greenberg 2012, pp. 90–91).

May's statement captures perfectly the cypherpunk motto privacy for the weak, transparency for the powerful (Assange et al. 2012, p. 7).

Overview of cypherpunk ethics

Based on this genealogy of the cypherpunk movement, we can see that cypherpunk ethics consists of two basic normative principles. First, the cypherpunks argue that privacy for the weak ought to be ensured through practical action and technological engagement. Depending on the state of surveillance in a given context, such privacy may or may not be a manifest reality; regardless, the demand for such privacy is a normative commitment for the cypherpunks. Second, the cypherpunks argue that transparency for the powerful ought to be pursued through practical action and technological engagement. While governments and corporations continue to become increasingly secretive, the cypherpunks argue that citizens and publics can use technology to undermine such secrecy and force these institutions to be more open.

Furthermore, this account of the cypherpunks reveals that they prefer technological solutions to legal ones. To be sure, the cypherpunks did use legal strategies to ensure the availability of cryptography to the public, but one of the movement's core values emphasizes "technological solutions over legal solutions" (May 1994). Because powerful government actors can be trusted to neither unequivocally defend and respect individual privacy nor consistently practice institutional transparency, publics cannot rely upon law for all social and political solutions. Instead, digital cryptography becomes a technical solution that exceeds the power of government and law. As long as strong crypto is available to all, individuals and groups may defend privacy and promote transparency even if the political powers that be do not sanction it.

Finally, there is one remaining important lesson: in the cypherpunk worldview, it is wrong to equivocate privacy and secrecy. 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. In this context, transparency has nothing to do with the privacy of individuals and relatively powerless organizations and has everything to do with the secrecy used by those governments, corporations, major political parties, and surveillance agencies that comprise what the cypherpunks views as an emerging "transnational surveillance dystopia" (Assange et al. 2012, p. 5). Thus, anyone who equates "privacy" with "secrecy" has already misunderstood a basic conceptual distinction within cypherpunk philosophy.

Julian Assange's cypherpunk ethics

The founder of WikiLeaks often shies away from getting into the nitty gritty details regarding the principles at the basis of his worldview. In one instance, when asked why he started WikiLeaks, Julian Assange (2016) replied: "I looked at something that I had seen going on with the world, which is that I thought there were too many unjust acts. And I wanted there to be more just acts, and fewer unjust acts. And one can ask, 'What are your philosophical axioms for this?' And I say, 'I do not need to consider them. This is simply my temperament. And it is an axiom because it is that way'. That avoids getting into further unhelpful philosophical discussion about why I want to do something. It is enough that I do" (pp. 68–69). Despite Assange's apparent reluctance to speak about his first principles, his intellectual background and various writings provide important insights regarding his worldview. In fact, even a cursory understanding of Assange and WikiLeaks is impossible without understanding Assange's cypherpunk ethics.

This section outlines three aspects of Assange's cypherpunk ethics. First, Assange was deeply influenced by the cypherpunk movement, but his distinctive background inspired him to fuse his cypherpunk principles with a brand of cosmopolitanism informed by antiwar sentiments, hacker principles, and Enlightenment philosophy. Second, Assange posits a rights-based theory of the ethics of communication, which leads him to criticize surveillance, censorship, and intellectual property regulations. Third, Assange synthesizes an enlightenment justification of the state with a cybernetic account of the operation of modern states (Brunton 2011). Taken together, these three features of Assange's philosophy constitute the basis of his cypherpunk ethics.

The cosmopolitan cypherpunk

In "A Cryptographic Call to Arms," written one year before Snowden's revelations about NSA surveillance, Assange packs all the wisdom of the cypherpunks into six short pages (Assange et al. 2012). Echoing David Chaum's warning about bureaucracies using computer networks to track every individual forever, Assange warns his audience about the coming "transnational dystopia" ruled by a global "postmodern surveillance state" (p. 1). Echoing Chaum's optimism about cryptography, Assange proclaims that "Cryptography is the ultimate form of non-violent direct action" (p. 5). In Assange's view, because issues of privacy cannot be left to the legal system, we must turn to mathematics. "Encryption is an embodiment of the laws of physics, and it does not listen to the bluster of states, even transnational surveillance dystopias," he writes. "Strong cryptography can resist an unlimited application of violence. No amount of coercive force will ever solve a math problem" (p. 5). Assange argues that the Diffie-Hellman protocol and, more specifically, prime factorization, prove that the universe sanctions individual privacy; to put it another way, surveillance can be resisted using the laws of nature. According to this perspective, by taking a key insight about mathematics and developing it into usable software, Chaum, Zimmerman, and the cypherpunks translated the laws of nature into the socially and politically usable tools necessary to preserve human freedom in the digital age. So much for decoder rings.

As that essay suggests, Assange learned a great deal about encryption as a cypherpunk, but he did not unquestioningly accept everything that May, Hughes, Gilmore, and others believed (Mann 2011). Assange's intellectual beginnings differed from the American cypherpunks, who were groomed in California hacker's culture where "the social liberalism of the New Left and the economic liberalism of the New Right…converged into an ambiguous dream of a high-tech 'Jeffersonian democracy'" (Barbrook & Cameron 2001, p. 377). Before joining the cypherpunks, other influences had imbued Assange with a cosmopolitan outlook that would shape his reception of cypherpunk principles (Ali & Kunstler 2019, p. xxiii).

There are three influences that distinguish Assange's intellectual background from the other cypherpunks. First, there is his connection to the antiwar movement (Assange 2011). Assange was born on July 3, 1971, just weeks after the New York Times began publishing the Pentagon Papers, leaked to the newspaper by Daniel Ellsberg, who sought to expose US government lies and war crimes in relation to the Vietnam War. Assange's parents had met the previous year, at a time when the anti-Vietnam War protests were at their height in Australia. His mother was quite politically active and participated in many antiwar demonstrations. Assange believes that being born in this atmosphere left a profound impression on him, and given his repeated expressions of concern about wars (Assange 2011, 2015, 2016; Assange et al. 2012), there may be some truth to this. "I must have taken it in with my mother's milk," he writes musingly, "the idea that non-conformity is the only real passion being ruled by. I believe I was conceived in that spirit" (Assange 2011, p. 32). The culture of the antiwar movement impressed upon Assange the importance of thinking about the injustices faced by those around the world.

Second, there is Assange's participation in Australia's 1980s hacker underground (Dreyfus & Assange 2012). It is important not to conflate the two hacker cultures. While the hackers in the United States were busy building what would become Silicon Valley' big tech, the hackers in Australia, Assange included, were tech-savvy teenagers gaining access to government and corporate networks by identifying and exploiting their security weaknesses.[4] "By the time I was sixteen," Assange (2011) writes, "the computer had become my consciousness" (p. 55). "By the time I was twenty," he adds, he and his friends "attempting to enter the Xanadu of computer networks, the US Department of Defense's Network Information Center (NIC) computer…We got inside, and the feeling was overwhelming" (pp. 82–83). Though the term "hacker" carries a negative connotation today, the hacking culture of Assange's day was not malicious—it was curious. Suelette Dreyfus explains the "golden rules of hacking" in the Australian underground: "don't damage the systems you break into (including crashing them); don't change the information in those systems (except for altering logs to cover your tracks); and share information." Just like visiting a national part, the rule was "Leave it as you find it" (Dreyfus & Assange 2012, p. 79). Like the antiwar movement, the hacker underground taught Assange to think in terms of "us" rather than in terms of "me" (Assange 2011, p. 56).

Third, there is his attraction to Enlightenment philosophy. Manne (2011) has called Assange "a true Enlightenment Man," and with good reason. While May was reading Rand and Nietzsche, Assange took inspiration from many early modern figures—John Milton, the Levellers, John Wilkes, and others (Assange 2011). As a teenage hacker, Assange took inspiration for his handle from Horace, a Roman lyric poet from the first century BCE whose writings were extremely popular in eighteenth-century Europe. As Assange (2011) explains, he took his handle—Mendax—from "Horace's splendide mendax—nobly truthful, or perhaps 'delightfully deceptive'" (p. 66). Many of Horace's Latin phrases, such as carpe diem (seize the day), were used

[4] To be sure, Dreyfus and Assange (2012) also note that there were hackers in the United States who also gained access to government and corporate networks by identifying and exploiting their security weaknesses. I have just drawn a distinction between "American" and "Australian" hackers for clarity of argument.

by Enlightenment philosophers, perhaps most famously sapere aude, which was used by Immanuel Kant (1991) in his classic essay "What is Enlightenment?" Synthesizing Enlightenment ideals with his antiwar disposition and his technological skills, Assange (2011) expresses optimism that computers would allow the world to be rebuilt, allowing "an increasing universality of freedom" (p. 57).

Because Assange was more cosmopolitan in his vision of social change than the other cypherpunks, he placed not mere individual liberty but global justice as the center of his worldview.[5] For some cypherpunks, Assange (2011) explains, the cypherpunk movement was "essentially about privacy as capitalist freedom, the right to be free of big government, to have your data kept back." But for Assange: "The cypherpunk ethos allowed me to think about how to best oppose the efforts of oppressive bodies—governments, corporations, surveillance agencies…Regimes often rely on having control of the data, and they can hurt people or oppress them or silence them by means of such control. My sense of the cypherpunk ethos was that it could protect people against this: it could turn their knowledge into an unreachable possession of theirs, protecting them in the classic Tom Paine way of securing liberty as a bulwark against harm or aggression" (p. 79). And while many cypherpunks viewed the state as the primary threat, Assange (2016) disagrees: "I don't see a difference between government and big corporations and small corporations. This is all one continuum; these are all systems that are trying to get as much power as possible" (pp. 132–133).

Some scholars have criticized anti-surveillance activists for prioritizing the concerns of (white) westerners at the expense of war, racism, and imperialism (Gürses, Kundnani & Hoboken 2016; Rexhepi 2016). Such criticism may apply to many cypherpunks, but Assange combines his cosmopolitanism with cypherpunk principles to advocate for the use of cryptography in the anti-imperial fight for national self-determination (Avila, Harrison & Richter 2017). In "How cryptography is a key weapon in the fight against empire states," published days after Snowden's revelations, Assange (2013) implores the governments and the people of the Global South to adopt encryption as a means of protecting themselves from the NSA and other western surveillance agencies. Drawing from his roots in cypherpunk philosophy, Assange argues that encryption is one of the most powerful tools for nation-states to defend themselves against Western imperialism. "Mass surveillance is not just an issue for democracy and governance," Assange insists, "it's a geopolitical issue. The surveillance of a whole population by a foreign power naturally threatens sovereignty." But the availability of cryptography means that such imperialist practices may be resisted. "Cryptography can protect not just the civil liberties and rights of individuals," he writes, "but the sovereignty and independence of whole countries, solidarity between groups with common cause, and the project of global emancipation. It can be used to fight not just the tyranny of the state over the individual but the tyranny of the empire over smaller states." Here, Assange shows how cypherpunk principles serve cosmopolitan purposes far beyond "privacy as capitalist freedom."

Communication and cryptography: a cypherpunk theory of rights

Assange's distinctive, cosmopolitan version of cypherpunk ethics informs his theory of rights. Within this theory, Assange identifies three basic rights, two threats to those rights, and one defensive means for protecting those rights. In Assange's view, every individual person has three basic rights, which he calls "the fundamental freedoms from which other freedoms derive" (Assange et al. 2012, p. 86). First, there is the right to movement, which essentially entails the freedom to travel without being physically coerced by powerful institutions. Second, there is the right to transact, which entails the right to interact economically with whomever you wish, buying, selling, and trading as you please (Assange et al. 2012, pp. 85–86).[6] Third, there is the right to communicate, which consists of two other rights: the right to know and the right to speak (Assange 2011, p. 119). Ultimately, Assange's defense of this conception of rights is grounded in his sense of justice, for these three rights "underpin justice" (Assange 2011, p. 119).

While Assange is not entirely explicit about the features of these rights, he seems to suggest that these three fundamental rights are natural, negative, and indefeasible. These

[5] Despite some of the intellectual similarities between Assange and the other cypherpunks, their obvious differences caused a great deal of conflict. As tech journalist Andy Greenberg (2012) explains, Young was initially involved with WikiLeaks, but he quickly grew tired of what he perceived as Assange's liberal-reformist rhetoric; he accused the website of being a front for the Central Intelligence Agency (CIA), and leaked an early WikiLeaks email list to Cryptome.org. "Fuck your cute hustle and disinformation campaign against legitimate dissent," Young blasted Assange. "Same old shit, working for the enemy" (p. 132). Similarly, though May had nearly conceived of a WikiLeaks-esque system himself, he did not put these ideas into practice like Assange. Cypherpunk and Tor developer Jacob Appelbaum has commented that May "could have created WikiLeaks himself and made a real difference in the world" if he wasn't "a fucking racist" (p. 92). But for May, lacking the cosmopolitan sensibilities of Assange, "the idea of trying to be Julian Assange gives me the creeps." "I'm not concerned about things like that. Let the Africans kill each other," May insists. "I don't have those kinds of political interests" (p. 91–91).

[6] Cryptocurrencies are the cypherpunk means for defending the right to transact. See note 2 above and also Assange et al. (2012).

rights are natural because they are derived from one's status as a human being and not from the authority or power of this or that government that human beings might live under. These rights are negative because they impose limitations on the types of activities that governments and corporations can engage in. All organizations whose activities respect these rights are legitimate, and all organizations whose activities violate these rights are illegitimate. These rights are indefeasible because they may not be voided or overridden for extenuating reasons. Governments, for example, may do many things to catch terrorists, money launderers, and drug traffickers, but the rights to move, transact, and communicate cannot be abridged or impeded in the government's pursuit of those ends.

To demonstrate the impotence of these three fundamental rights, we can look at the what Assange sees as the broader implications of the right to communicate. For Assange, the right to communicate produces certain goods, attracts certain threats, and can be protected by certain defenses. The basic good promoted by the right to communicate is the growth of the record of human civilization, which in turn provides the basis for human advancement. As Assange (2016) argues, "human civilization, its good part, is based upon our full intellectual record, and our intellectual record should be as large as possible if humanity is to be as advanced as possible" (p. 139). Other cypherpunks agree with Assange that more information leads to more knowledge which leads to more advancement for the species. Andy Müller-Maguhn, for one, argues that "the history of the human race and the history of culture is the history of copying thoughts, modifying and processing them further on" (Assange et al. 2012, p. 78). Giving the greatest number of people access to the greatest possible amount of information results in the greatest number of innovations. Thus, cypherpunks insist upon dismantling barriers to sharing information, ideas, and culture. "I think this is why the copyright wars are so essential", Jérémie Zimmermann explains, "because with peer-to-peer technologies, since Napster in 1999, people just understood—got it—that by sharing files between individuals…you build better culture…Culture is meant to be shared" (Assange et al. 2012, p. 78). Assange and the other cypherpunks border on a kind of epistemic utopianism, for they truly believe that humanity has the power to shape its own destiny and that the sharing of knowledge is the most important means for doing so. "If all the collected information about the world was public," Assange optimistically states, "that might rebalance the power dynamic and let us, as a global civilization, shape our destiny" (Assange et al. 2012, p. 158).

Yet humanity is not as advanced as it could be because governments and corporations collaborate to infringe upon the right to communicate. For these institutions, surveillance is the means and censorship is the end. Censorship is universally reviled by cypherpunks because it is a direct attack upon the right to communicate (Assange et al. 2012). It might be intuitive to think that censorship infringes upon only the right to speak, but it also infringes upon the right to know. Let's return to Alice and Bob. If a certain type of speech is prohibited by governmental or corporate authorities, then such prohibitions not only prevent Alice from speaking, they also prevent Bob from knowing. Likewise, it might be intuitive to think that government censorship and corporate censorship are two different things, but this is not always the case. Sometimes corporate censorship has nothing to do with government. For example, if Twitter takes down a person's tweet or bans them and deletes their account, the company is free to do so because the First Amendment applies to government actions, not corporate actions. But Jérémie Zimmermann's invocation of Napster and the copyright wars is informative here, for from a cypherpunk perspective, intellectual property regimes are a form a censorship enforced through government and corporate cooperation. By granting proprietary rights over, say, computer code, governments prohibit individuals from sharing that code. Phil Zimmerman was a hero in part because he distributed his code for free, and his subsequent legal battle was important because it validated the cypherpunk view that code is speech not property.[7] Because censorship violates the right to communicate, it impedes positive developments in the trajectory of human advancement.

Governments and corporations pursue censorship for various political and economic reasons, but surveillance is the means by which censorship is enforced (Assange et al. 2012). Assange distinguishes between tactical surveillance (surveilling specific individuals for law enforcement purposes) and strategic surveillance (surveilling entire populations under the guise of "national security"). While tactical surveillance is acceptable if Constitutional procedures are followed properly, strategic surveillance inherently disrupts the free exchange of all kinds of information (p. 144). If corporate and political powers are going to successfully censor anything, they must use strategic surveillance to observe all communications. As Assange notes, "in order to have internet censorship there must also be internet surveillance. In order to check what someone is looking at, to see whether it is permitted or denied, [the authorities] must be seeing it, and therefore if [they] are seeing it [they] can record it all" (p. 114). The worry here is, if the authorities can see and record everything you ever say, they gain a lot of leverage over relatively powerless individual persons, thus

[7] In this sense, cypherpunk ethics are consistent with the principles of Richard Stallman's (2015) Free Software Movement and Aaron Swartz's (2016) guerrilla open access manifesto, both of which imply that intellectual property rights impede the right to know.

implicating their right to speak. Similarly, if the authorities are to successfully police intellectual property right violations, they not only have to surveil all communications, but they may also tell programmers, for example, that they may not distribute certain code and, by implication, that they may not speak.

While censorship and surveillance come together to threaten the right to communicate, Assange agrees with the other cypherpunks that encryption provides the best defense of this right. There is no incentive for powerful organizations to respect my rights on their own accord (Assange et al. 2012, p. 62), but if my communications are encrypted, if the things I read and say are shielded from the prying eyes of surveillance agencies, then they will not be able to impede my right to communicate. They will be able to neither record my statements nor prevent me from accessing information I choose. I would be able to exercise my right to know by reading what I like without being prevented by censorship, paywalls, or copyrights, and I would be able to exercise my right to speak without being constantly monitored and recorded. As May (2001b) once put it, "Strong crypto provides a technological means of ensuring the practical freedom to read and write what one wishes to" (p. 77). Here is where Assange's theory of rights and his cypherpunk advocacy for the use of cryptography come together. For Assange (2011), "Rights are freedoms of action that are known to be enforceable" (p. 118), and encryption is the means by which rights become enforceable. Through the widespread use of strong encryption, no government, corporation, or surveillance agency in the transnational surveillance dystopia can prevent people from exercising their rights.

Leaks and conspiracies: a cypherpunk theory of the state

While the personal use of encryption enables the realization of only the first half of the cypherpunk slogan, privacy for the weak, the use of crypto to induce document leaks enables the realization of the second half, transparency for the powerful. Some people have advocated various democratic and legal reforms for mitigating the worst effects of government and corporate surveillance (Greenwald 2014; Snowden 2019; Zuboff 2019), but Assange follows Young and May, advocating a cypherpunk approach involving leaked communications. Interestingly, Assange's method inverts May's (2001b) discussion of the transparency and opacity of virtual communities, reversing it so it can be applied to governments and corporations. Just as Assange's cosmopolitanism and theory of rights are informed by his study of Enlightenment philosophy, Assange's theory of whistleblowing is rooted in an Enlightenment conception of the state. In creating WikiLeaks, Assange synthesized cypherpunk ideas about encryption, transparency, and whistleblowing with an Enlightenment conception of government to build an anti-secrecy machine.

Enlightenment ideas are part of the inspiration for Assange's view of government, but he gives them a modern cypherpunk twist. "Many modern governments", Assange (2011) laments, "forget that they were founded on the principles of the Enlightenment, that knowledge is a guarantor of liberty, and that no state has the right to dispense justice as if it were merely a favour of power" (p. 242). While some Enlightenment political philosophers, such as Montesquieu (1989; see also Hirschman 1997), argued that that a separation of government powers was the most effective way to guarantee liberty, Assange argues that transparency is now the most effective means for preserving liberty. During the Enlightenment, there was a belief that liberty would be eroded if too much power was concentrated in too few person's hands. But Assange observes that in the United States and other Anglo-Saxon countries, where political systems are at least nominally founded on the separation of powers doctrine, secrecy creates the conditions under which governments enact many policies and programs that threaten liberty at home and around the world; the case of NSA global mass surveillance would be merely one example.

To undermine government secrecy and thus prevent the growth of authoritarian power, Assange conceives of secret government communication networks as connected graphs, which can be disrupted with leaks, causing the communication network to collapse upon itself. In "Conspiracy as Governance", an essay originally published on Cryptome.org, Assange (2006) argues that we must acknowledge that powerful regimes resist change and that secrecy is "the key generative structure of bad governance" (p. 1). As the title suggests, Assange views the secretive communication networks of governments as conspiracies. His technical use of this term relies on the following definition: "Conspiracy, Conspire: make secret plans jointly to commit a harmful act; working together to bring about a particular result, typically to someone's detriment" (p. 1). Citing Machiavelli's The Prince, Assange concludes that regimes use secrecy to consolidate power because, if a regime's nefarious plans were known by its public, the regime would be resisted. For Assange, this practice of secrecy is the foundation of all authoritarian government, and even nominal democracies—those founded on Enlightenment principles—devolve into authoritarianism when they are permitted too much secrecy (see also Assange 2016, p. 139). As Assange (2016) puts it, "secrecy is criminogenic".

To understand how conspiratorial government communication networks operate, Assange takes his cue from the United States government itself, which hires mathematicians to understand terrorist organizations as connected graphs (see Amoore and De Goede 2005). In the connected graphs model, each individual in the conspiracy represents

one node through which communication may pass; some nodes send and receive more important information than other nodes, and the overall communicative capacity of the conspiracy represents what Assange calls the total conspiratorial power. To illustrate this theory, Assange (2006) provides the following visual example: "First take some nails ('conspirators') and hammer them into a board at random. Then take twine ('communication') and loop it from nail to nail without breaking. Call the twine connecting two nails a link… Imagine a thick heavy cord between some nails and fine light thread between others. Call the importance, thickness or heaviness of a link its weight. Between conspirators that never communicate the weight is zero" (pp. 2–3). Assange reminds his readers that modern communication technologies—namely, computers and the internet—enable conspiratorial governments to more easily share information internally, thus increasing the efficiency of the conspiracy.

To disrupt a conspiracy and thus reduce the harm it can do in the world, Assange says that the total conspiratorial power must be reduced to the lowest possible level. This disruption of the conspiracy could be achieved through the assassination of the most powerful members of the conspiracy, as the cypherpunk James Dalton Bell once suggested (Greenberg 2012); however, Assange (2006) opposes this method, disparaging assassination as "the result of mental inclinations honed for the pre-literate societies in which our species evolved" (p. 5). Preferring non-violent means, he advocates three alternative modes: first, blinding the conspiracy, which entails "distorting or restricting the information available to it"; second, separating the conspiracy, which entails somehow "cleaving a conspiracy into halves"; or third, throttling the conspiracy, which entails "constricting (reducing the weight of) those high weight links which bridge regions of equal total conspiratorial power." The most effective way of achieving each of these modes of disruption is to locate or inspire an insider of the conspiracy, someone who is witnessing the harms being planned or carried out in real time, to reveal some portion of the secret communication between the conspiring parties—in other words, leaking. Unlike the US government, which uses the connected graphs model to assassinate (Scahill 2016) or otherwise neutralize individuals who lead terrorist organizations (pulling nails out of the board), Assange argues that leaks represent attacks on the links in the connected graphs (cutting the twine). When a conspiracy is subjected to a series of potentially damaging leaks, it responds by restricting the internal flow of information (or even cutting off some nodes) and thus experiences greater difficult communicating with itself.

Thus, whistleblowers become the key to non-violent resistance to authoritarian government. When a whistleblower discloses documents revealing government wrongdoing, the conspiracy can respond in several ways (Bady 2010; Assange 2006, 2015, 2016). One: the conspiracy could take all of its records off paper, reverting to verbal communication, but this would throttle the conspiracy because it is much more difficult for large communication networks to operate efficiently without a well-developed bureaucracy. Two: it could constrict its internal communications, making sure that the most sensitive information passes only through the hands of a few; but again, this breeds communicative inefficiency. Three: it could rigorously search for the source of the leaks and implement internal surveillance mechanisms to catch or prevent future leaks. These practices also cost the conspiracy time and resources, ultimately throttling the conspiracy.

One might be tempted to ask why Assange does not simply use his hacking skills to retrieve documents from conspiracies. There are two reasons. The first reason is that hacker ethics forbids stealing from the systems they enter (Dreyfus & Assange 2012, p. 79). "You don't steal information," Assange (2011) instructs. "You simply create a platform for it when it finds its way into the public realm" (p. 93). Thus, Assange (2006,2016) concludes that we must call upon the insiders who witness the acts and the plans of injustice to reveal those acts and plans to the world. "We have come to the conclusion," Assange wrote at the moment of WikiLeaks' founding, "that fomenting a worldwide movement of mass leaking is the most effective political intervention available to us" (qtd. in Greenberg 2012, p. 131).

The second reason is that leakers are more dangerous to the conspiracy than hackers. If someone hacks into a system and steals documents, the conspiracy will look for an external threat rather than constrict communications in response to an internal threat. As Aaron Bady (2010) explains, "increasing the porousness of the conspiracy's information system will impede its functioning, that the conspiracy will turn against itself in self-defense, clamping down on its own information flows in ways that will then impede its own cognitive function. You destroy the conspiracy, in other words, by making it so paranoid of itself that it can no longer conspire." Finn Brunton (2011) corroborate this interpretation: "To break into a system and steal a document merely provokes an organization to improve its security, and releasing the document is no guarantee of a positive social result. It is vital that the materials are leaks because that will foment suspicion and paranoia among the conspirators" (p. 15). Returning to the visual example of nails and twine on a board, leaking documents does something that stealing documents does not: it forces the conspiracy to start cutting its own links, "thereby making itself dumber and slower and smaller."

For Assange (2015), a paradigmatic example of technologically enabled conspiratorial power is the US State Department. Under Henry Kissinger's direction in the 1970s, the State Department transitioned from a paper-based to an electric communication system, thereby better linking all

the nodes (diplomats) and making the foreign policy apparatus of the United States more efficient. What's more, citing the State Department's "Strategic Plan, FY 2014–2017", Assange notes that US embassies today house not only diplomats but also NSA, CIA, FBI, and DOD offices, all of which work in close connection with large US corporations. From Assange's perspective, we should understand Manning's decision to blow the whistle on the Iraq and Afghanistan wars as an attack on the conspiratorial communication networks inside the Pentagon and State Department.

It is important to note that the documents leaked by Manning had precisely the effect Assange anticipated. On the one hand, the conspiracy was blinded because, as WikiLeaks uses an encrypted document submission tool, there was no way for the United States government to know who leaked the documents. Manning's eventual arrest resulted not from insecurities in WikiLeaks' system but from Manning confessing to her actions in a chatroom (Zetter and Poulson 2010). To my knowledge, no other source of WikiLeaks' has ever been discovered.[8] On the other hand, the conspiracy was throttled because the US government went to great lengths to prevent future leaks of that type and magnitude. As the New York Times reported in 2010:

> The Defense Department is scaling back information sharing, which its leaders believe went too far after information hoarding was blamed for the failure to detect the Sept. 11 plot. The department has also stripped CD and DVD recorders from its computers; it is redesigning security systems to require two people, not one, to move large amounts of information from a classified computer to an unclassified one; and it is installing software to detect downloads of unusual size. (Shane 2010).

Furthermore, the Pentagon created an automatic email filter to block all incoming and outgoing emails containing the word "WikiLeaks," which prevented Pentagon prosecutors from receiving important information related to Manning's prosecution (Assange 2015). The similar thing happened to Bank of America when it was rumored that WikiLeaks planned to publish leaked documents from it (Greenberg 2012), and Assange would likely argue that the documents leaked by Snowden had the same effect on the NSA.

In an age when the all-seeing eyes of a transnational surveillance dystopia pose an existential threat to the right to communicate, Assange views encryption as the best defense of one's rights, but he also views leaking as the best offense against the conspiratorial governments, corporations, and agencies can comprise that dystopia. And to the extent that leaking undermines those organizations" ability to violate the right to communicate in the first place, Assange may well be suggesting that the best defense is a good offense.

Assange's cypherpunk ethics

While many other members of the cypherpunk movement primarily think of "privacy for the weak" and "transparency for the powerful" on the national scale and through a libertarian lens, Assange adapts those central cypherpunk principles for a cosmopolitan outlook. This modification of cypherpunk ethics leads Assange to use privacy for the weak and transparency for the powerful in a slightly different manner than the other cypherpunks. On the one hand, Assange argues that pursuing privacy for the weak through the use of cryptography does not merely prevent government intrusions into individual privacy but actually forms the basis of an open world culture. Because crypto allows individuals everywhere to express their ideas and access information of their choosing, humanity gains the possibility of creating an open and accessible intellectual record, which may allow global civilization to advance more quickly than closed culture would. On the other hand, Assange argues that pursuing transparency for the powerful through the use of cryptography does not merely create information black markets but actually disrupts the conspiratorial networks hidden inside large institutions. By using encrypted platforms to induce leaks in such institutions, Assange argues that conspiracies may be throttled, thus diminishing their capacity for success. In the end, two of the most controversial aspects of WikiLeaks—its practice of publishing archives of primary documents and its claim that publics have a right to know what governments do in their names—manifest from

[8] There is perhaps one exception, and that is Joshua Schulte, a former CIA employee who the government has accused of leaking documents that WikiLeaks published under the name of Vault 7 in early 2017. The *New York Times* described Vault 7 as "thousands of pages describing sophisticated software tools and techniques used by the agency to break into smartphones, computers and even Internet-connected televisions" (Shane, Rosenberg & Lehren 2017). Though Schulte was arrested in August 2017, the government waited over a year to charge him with leaking the documents. This was probably because "The government had no direct proof that Mr. Schulte sent the files to WikiLeaks. Instead, prosecutors relied on circumstantial evidence" (Hong 2020b). Meanwhile, the government is charging Schulte with possession of child pornography, but again, the evidence is flimsy. "Investigators obtained a search warrant to enter his New York City apartment," wrote the *Times*, "where they found dozens of electronic devices and more than 10,000 images and videos of child pornography, buried under three levels of encryption" (Hong 2020a). This case demonstrates the importance of educating the public about encryption, for no one—not even the US government—simply "finds" anything "buried under three levels of encryption." Unfortunately, reporting on the matter does not explain exactly how the government broke any of the encryption, let alone three layers. One would think that if the government could break encryption so easily, it would not repeatedly claim that law enforcement is "going dark" under the increasing use of encryption as part of Crypto Wars 2.0 (see Meinrath & Vitka 2014).

a combination of the right to communicate and the network theory of the state. WikiLeaks is not a "radical transparency" or "total transparency" organization, as some of its critics have claimed. Instead, it is a cypherpunk organization that promotes transparency for the powerful.

Conlusion

This essay responds to two major shortcomings in the scholarship on WikiLeaks, namely, the tendency to treat Julian Assange as WikiLeaks as objects of study and the resulting misinterpretation that WikiLeaks is a "radical transparency" organization. Instead, I argue that any account of WikiLeaks must grapple with Assange's cypherpunk ethics, the main principle of which is privacy for the weak, transparency for the powerful. This principle emerged from the cypherpunk movement in the 1990s, as they fought to make cryptography available for all people. The cypherpunks saw that encryption was the technological answer to the social and political problem of protecting privacy in a digital age. They also realized that crypto created the conditions in which powerful institutions, such as national governments, would have a difficult time protecting their own secrets. As a participant in the movement, Assange adopted the principles of cypherpunk ethics, but he placed them into a distinctively cosmopolitan context. By combining cypherpunk ethics with antiwar values and Enlightenment ideals, Assange developed a truly global conception of cypherpunk philosophy. Within this worldview, crypto defends privacy for the weak, thereby upholding the right to communicate, and promotes transparency for the powerful, thereby limiting the harm caused by bad governance. While previous scholarship on WikiLeaks imposed already established theories onto the organization, future research ought to engage the cypherpunk ethics as the basis of Assange worldview. Until then, let us remember that the cypherpunks have worked to protect the innocent from the strong, and while that work has been difficult, it is not yet done. "Our task", Assange writes on behalf of the cypherpunks, "is to secure self-determination where we can, to hold back the coming dystopia where we cannot, and if all else fails, to accelerate its self-destruction" (Assange et al. 2012, p. 6).

References

Ali, T., & Kunstler, M. (2019). Introduction. In T. Ali & M. Kunstler (Eds.), *In defense of Julian Assange*. New York: OR Books.

Amoore, L., & De Goede, M. (2005). Governance, risk, and dataveillance in the war on terror. *Crime Law & Social Change, 43,* 149–173.

Assange, J. (2006). Conspiracy as governance. *Cryptome.org*. https://archive.fo/kr8Pr. Accessed 28 Oct 2020.

Assange, J. (2011). *Julian Assange: The unauthorized autobiography*. Edinburgh: Canongate Books.

Assange, J. (2013). How cryptography is a key weapon in the fight against empire states. *The Guardian*. https://archive.fo/Mbsx4 . Accessed 28 Oct 2020.

Assange, J. (2015). Introduction: WikiLeaks and empire. *The WikiLeaks files: The world according to US empire*. New York: Verso.

Assange, J. (2016). *When Google met WikiLeaks*. New York: OR Books.

Assange, J., Appelbaum, J., Müller-Maguhn, A., & Zimmermann, J. (2012). *Cypherpunks: Freedom and the future of the internet*. New York: OR Books.

Avila, R., Harrison, S., & Richter, A. (2017). *Women, whistleblowing, WikiLeaks: A conversation*. New York: OR Books.

Bady, A. (2010). Julian Assange and the computer conspiracy: "To destroy this invisible government". Personal blog. *zunguzungu*. https://archive.fo/4nIaQ. Accessed 28 Oct 2020.

Barbrook, R., & Cameron, A. (2001). Californian ideology. In P. Ludlow (Ed.), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 363–388). Cambridge: MIT Press.

Benkler, Y. (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.

Bok, S. (1989). *Secrets: On the ethics of concealment and revelation*. New York: Vintage Books.

Boot, E. R. (2019). *The ethics of whistleblowing*. New York: Routledge.

Brevini, B., Hintz, A., & McCurdy, P. (Eds.). (2013). *Beyond WikiLeaks: Implications for the future of communications, journalism and society*. New York: Palgrave Macmillan.

Brunton, F. (2011). Keyspace: WikiLeaks and the Assange papers. *Radical Philosophy, 166,* 8–20.

Burnham, D. (1983). *The rise of the computer state: The threat to our freedoms, our ethics and our democratic process*. New York: Random House.

Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM, 24*(2), 84–90.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM, 28*(10), 1030–1044.

Danezis, G. & Diaz, C. (2008). Survey of anonymous communication channels. Technical Report MSR-TR-2008-35. Microsoft Research. https://www.microsoft.com/en-us/research/wp-content/uploads/2008/02/tr-2008-35.pdf. Accessed 28 Oct 2020.

Delmas, C. (2015). The ethics of government whistleblowing. *Social Theory and Practice, 41*(1), 77–105.

Dreyfus, S., & Assange, J. (2012). *Underground*. Edinburgh: Canongate Books.

Greenberg, A. (2012). *This machine kills secrets: How WikiLeakers, cypherpunks, and hacktivists aim to free the world's information*. New York: Dutton.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York: Picador.

Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture & Society, 38*(4), 576–590.

Hirschman, A. O. (1997). *The passions and the interests: Political arguments for capitalism before its triumph*. Princeton: Princeton University Press.

Hong, N. (2020a). Ex-C.I.A. analyst faces trial in biggest leak of agency's history. *The New York Times*. https://archive.fo/p2924 . Accessed 28 Oct 2020.

Hong, N. (2020b). Trial of programmer accused in C.I.A. leak ends in hung jury. *The New York Times*. https://archive.fo/MP5s9. Accessed 28 Oct 2020.

Hubbs, G. (2014). Transparency, corruption, and democratic institutions. *Les ateliers de l'éthiques/The Ethics Forum, 9*(1), 65–83.
Hughes, E. (2001). A cypherpunk's manifesto. In P. Ludlow (Ed.), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 81–84). Cambridge: MIT Press.
Kant, I. (1991). *Political writings*, 2nd ed. In H. S. Riess (Ed.). Cambridge: Cambridge University Press.
Levy, S. (2001). *Crypto: How the code rebels beat the government—saving privacy in the digital age*. New York: Penguin.
Levy, S. (2010). *Hackers: heroes of the computer revolution—25th* (anniversary). Cambridge: O'Reilly Media Inc.
Mann, C. C. (2002). A primer on public-key encryption. *The Atlantic*. https://archive.fo/cA3uv. Accessed 28 Oct 2020.
Manne, R. (2011). The cypherpunk revolutionary. *The Monthly*. https://archive.fo/kwI60. Accessed 28 Oct 2020.
Marechal, N. (2013). WikiLeaks and the public sphere: Dissent and control in cyberworld. *The International Journal of Technology, Knowledge, and Society, 9,* 93–106.
Marmura, S. M. E. (2018). *The WikiLeaks paradigm*. Cham, Switzerland: Palgrave Macmillan.
May, T. (1994). *The Cyphernomicon: Cypherpunks FAQ and more*. https://archive.fo/vBms5. Accessed 28 Oct 2020.
May, T. (2001a). The crypto anarchist manifesto. In P. Ludlow (Ed.), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 61–64). Cambridge: MIT Press.
May, T. (2001b). Crypto anarchy and virtual communities. In P. Ludlow (Ed.), *Crypto anarchy, cyberstates, and pirate utopias* (pp. 65–80). Cambridge: MIT Press.
Meinrath, S. D., & Vitka, S. (2014). Crypto war II. *Critical Studies in Media Communication, 31*(2), 123–128.
Michaud, T. (2008). Science fiction and politics: Cyberpunk science fiction as political philosophy. In D. M. Hassler & C. Wilcox (Eds.), *New boundaries in political science fiction* (pp. 65–77). Columbia: The University of South Carolina Press.
Montesquieu. (1989). *The spirit of the laws*. In A. M. Cohler, B. C. Miller & H. S. Stone (Eds.). Cambridge: Cambridge Univesity Press.
Moore, A. (2011). Privacy, security, and government surveillance: WikiLeaks and the new accountability. *Public Affairs Quarterly, 25*(2), 141–156.
Rexhepi, P. (2016). Liberal luxury: Decentering Snowden, surveillance, and privilege. *Big Data & Society*, 1–3. https://doi.org/10.1177/2053951716679676.
Scahill, J. & The Staff of the Intercept. (2016). The assassination complex: Inside the government' s secret drone warfare program. New York: Simon & Schuster.
Schneier, B. (2015). *Applied cryptography: Protocols, algorithms and source code in C*. New York: John Wiley & Sons.
Shane, S. (2010). Keeping secrets WikiSafe. *The New York Times*. https://archive.fo/Ah54H. Accessed 28 Oct 2020.
Shane, S., Rosenberg, M. & Lehren, A. W. (2017). WikiLeaks releases trove of alleged C.I.A. hacking documents. *The New York Times*. https://archive.fo/nY9Hs. Accessed 28 Oct 2020.
Snowden, E. (2019). *Permanent record*. New York: Metropolitan Books.
Spence, E. H. (2012). Government secrecy, the ethics of WikiLeaks, and the fifth estate. *International Review of Information Ethics, 17*(7), 37–45.
Stallman, R. M. (2015). *Free software, free society: selected essays of Richard M. Stallman* (3rd ed.). Boston: GNU Press.
Swartz, A. (2016). *The boy who could change the world: The writings of Aaron Swartz*. New York: The New Press.
Taylor, C. A. (Ed.). (2017). *The ethics of WikiLeaks*. New York: Greenhaven Publishing LLC.
Villena Saldaña, D. (2011). Julian Assange: periodismo, científico, conspiración y ética hacker. *Quehacer, 181,* 58–69.
Whitfield, D., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory, 22*(6), 644–654.
Wilkins, L. (2018). A history of media ethics: From application to theory and back again. In P. L. Plaisence (Ed.), *Communication and media ethics* (pp. 15–30). Berlin: De Gruyter Mouton.
Wisnewski, J. (2016). WikiLeaks and whistleblowing: Privacy and consent in an age of digital surveillance. In J. Galliott (Ed.), *Ethics and the future of spying* (pp. 205–216). New York: Routledge.
Zetter, K. & Paulson, K. (2010, June 6). U.S. intelligence analyst arrested in WikiLeaks video probe. *Wired*. https://archive.fo/gsvu5 . Accessed 28 Oct 2020.
Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. New York: Public Affairs.