Surveillance & Society

Article | Of Cypherpunks and Sousveillance

Patrick D. Anderson

Central State University, USA
panderson@centralstate.edu

Abstract

For three decades, the cypherpunk movement has fought for the right of individuals and publics to use digital cryptography—or crypto—to defend their individual privacy and promote institutional transparency and accountability. The cypherpunks have also fought for institutional transparency through various strategies of sousveillance. Yet the movement's contribution to theories of surveillance and the praxis of resistance have been largely overlooked by scholars. This essay bridges the gap between the movement and the academy by outlining the normative and epistemological aspects of cypherpunk philosophy. Cypherpunk ethics is captured by the normative cypherpunk slogan "privacy for the weak, transparency for the powerful." Cypherpunk epistemology is a form of data activism that calls for a hands-on response to the datafication of surveillance and relies upon both *pro*-active (transparency) and *re*-active (privacy) strategies. While the cypherpunks are famously concerned about privacy, because cypherpunk philosophy also calls for "transparency for the powerful," cypherpunks have practiced a distinctive form of cypherpunk sousveillance. By understanding that cypherpunk theory and practice each consist of two complementary dynamics—privacy/transparency, pro-active/re-active—it becomes possible to understand that the cypherpunk movement provides the basis for activists and citizens to resist large surveillance institutions like the National Security Agency and Google by altering information fluxes at the systemic level. The cypherpunk movement provides an intelligible, viable, and effective model of data activism and strategic agency, and this essay contributes to the pluralistic, multidisciplinary understanding of resistance to surveillance and practice of sousveillance by outlining the basic normative, epistemic, and pragmatic aspects of cypherpunk theory and practice.

CEREAL: Snoop unto them… NIKON: …as they snoop unto us.

– Hackers *(1995)*

When encryption is outlawed, figmujjo icy hwxish.

– Cypherpunk Proverb

Introduction

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. Cryptography—or crypto, for short—is the "art and science of keeping messages secure" (Schneier 1996: 1), and in the digital age, crypto is designed using complex mathematical formulas inside the software we use daily (Holden 2017). For the cypherpunks, crypto was the central technological means for preventing powerful institutions from dominating the lives of individuals. "At the core of the cypherpunk philosophy," Robert Manne (2011) explains, is "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

Anderson, Patrick. 2022. Of Cypherpunks and Sousveillance. *Surveillance & Society* 20(1): 1-17.
https://ojs.library.queensu.ca/index.php/surveillance-and-society/index | ISSN: 1477-7487

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, and for that reason, Manne (2011) observes, "The deepest institutional enemy of the cypherpunks was the National Security Agency." Throughout the 1990s, during what has been called the Crypto War, the cypherpunks were part of a coalition of anti-surveillance privacy activists who went toe-to-toe with the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI), challenging the United States government's attempt to unilaterally control digital cryptography (Levy 2001; Greenberg 2012). The NSA and the FBI opposed the widespread use of crypto because they believed it would undermine national security intelligence gathering and evidence gathering for law enforcement purposes. In contrast, the cypherpunks argued that a society deprived of the security and privacy afforded by crypto would devolve into sheer authoritarianism. In the end, the cypherpunks' eventual victory in the Crypto War helped make strong crypto available for the global public.[1]

Despite the cypherpunks' role in the history of anti-surveillance activism, their theoretical contributions to our understanding of surveillance—and, more importantly, their strategies of resistance in the face of surveillance systems—have been rarely observed and largely misunderstood within the field of surveillance studies. David Brin (1998: 194) has accused the cypherpunks of hypocrisy, claiming that their concerns about privacy were the product of "the type of self-righteous tunnel vision that might keep us from finding useful answers to some of the perils we will face in the coming decades." For Brin (1998: 19), the problem was that the cypherpunks vacillated between two contradictory principles: Principle A, which holds that increased information or data flows are dangerous, and Principle B, which holds that increased information or data flows are beneficial. In Brin's (1998: 20) view, the cypherpunks were "self-righteously demanding" more transparency for their opponents than they were willing to take on themselves. More recently, Mir Adnan Ali and Steve Mann (2013) have situated cypherpunk advocacy for encryption-based privacy as the inverse of their project of sousveillance. "Both enable control over the information in a transaction," Ali and Mann (2013: 253) write, "cryptography by giving the option to keep it private, and veillance by giving the option to share it."

Notwithstanding their different aims and reasons, Brin (1998) and Ali and Mann (2013) each misconstrue some aspect of cypherpunk philosophy. Ali and Mann (2013), on one hand, view the cypherpunks as having something to say about privacy but nothing to say about veillance, especially sousveillance. Yet the central principle of the cypherpunk movement can be expressed in a simple but elegant slogan: "privacy for the weak, transparency for the powerful" (Assange et al. 2012). "The cypherpunks," Suelette Dreyfus observes, "believed 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 2012: xii). While cypherpunks believe that crypto can defend individual privacy, they also believe that crypto promotes transparency through a distinctive form of sousveillance. In other words, Ali and Mann (2013) fail to appreciate the cypherpunk insight that crypto can be used as a means of conducting sousveillance and not simply as an anti-surveillance tool.

Brin (1998), on the other hand, fails to recognize the cypherpunk insight that surveillance and transparency only take on meaning in the context of power relations (Mann 2020). As Adam Moore (2011: 152) incisively notes, "One marker of power is the ability to demand information disclosures from others while keeping one's own information secret." As one of the foremost proponents of cypherpunk philosophy today (Assange et al. 2012), Julian Assange (2014) argues that privacy should not be defended because it is inherently valuable; instead, he says, it should be defended within a "calculus of power," for "the destruction of privacy widens the existing power imbalance between the ruling factions and everyone else."

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

This essay initiates a conversation between the cypherpunk movement and surveillance studies by showing how the basic principle of cypherpunk philosophy—which I will call cypherpunk ethics—expands our understanding of data activism as resistance to surveillance in the digital age. Though this project is sympathetic to the cypherpunk worldview, its primary aim is to describe and systematize key aspects of cypherpunk philosophy as a means of better understanding, and perhaps learning from, the movement's resistance strategies. The notion of "resistance" in surveillance studies is both pluralistic and multidisciplinary (Martin, van Brakel, and Barnhard 2009), and the account of cypherpunk ethics presented here expands upon this pluralism by presenting the general principles of the cypherpunk movement as yet another resistance paradigm. Jonah Bossewitch and Aram Sinnreich (2012: 225) argue that "in the face of the communication infrastructure's increasing scope and complexity, individuals will require simple and effective models of participation to avoid paralysis and to catalyze strategic agency." The cypherpunk model of resistance provides such a model.

The essay proceeds in four sections. The first section outlines the fundamental normative principles of *cypherpunk ethics* by placing the cypherpunk notion "privacy for the weak, transparency for the powerful" into its historical and theoretical context, explaining the cypherpunks' role in the Crypto Wars of the 1990s, and highlighting the place of power in cypherpunk conceptions of privacy, secrecy, and transparency.[2] Like all social movements, there are ideological and ethical disagreements among the participants of the cypherpunk movement. While this paper offers *a* cypherpunk perspective on surveillance and sousveillance, it does not claim to offer *the* cypherpunk perspective on these issues. While other studies have noted the internal ideological disagreements among cypherpunks (Manne 2011; Greenberg 2012), this paper focuses on the more often overlooked intergenerational disagreements within the movement. As a result, the cypherpunk perspective offered here specifically reflects cypherpunk philosophy as it is articulated by the most prolific third-generation cypherpunk authors.

The second section outlines the basic features of *cypherpunk epistemology*, a form of data activism that gives priority to encryption in its calls for a hands-on response to the datafication of surveillance and in its reliance upon both *pro*-active (transparency) and *re*-active (privacy) strategies. Using WikiLeaks as a case study in the applied use of the normative principle "transparency for the powerful," the third section outlines a cypherpunk mode of transparency activism called *cypherpunk sousveillance*, a form of sousveillance that emphasizes the formal aspects of digital data sousveillance.[3] The fourth section situates cypherpunk data activism within what Bossewitch and Sinnreich (2012) have called the field of "information flux," demonstrating its potential practical effects when deployed within and among existing surveillance assemblages (Haggerty and Ericson 2000). While institutions like the NSA and Google can be defined as information black holes—collecting all external data and emitting no internal data—the cypherpunk principle "privacy for the weak, transparency for the powerful" suggests that individuals can most successfully fight these information black holes by mirroring their behavior and becoming black holes. Here, the cypherpunk notion "privacy for the weak, transparency for the powerful" and its simultaneous pro-active and re-active strategy of data activism provide a possible basis for reversing information fluxes at the systemic level.

By understanding the normative claims of cypherpunk ethics and the epistemic orientation of cypherpunk epistemology, it becomes possible to recognize a form of cypherpunk sousveillance and to see the

---

[2] The first section of this essay draws inspiration from Ashlin Lee's (2015) application of ethno-epistemic assemblages (EEAs) to surveillance studies. This section can be considered a case study in EEA, looking at the ways in which the cypherpunks developed their surveillance consciousness in context. Though space does not permit a full treatment, while the cypherpunks' slogan seems to imply a simple individual/institution surveillance binary, most members of the movement are hackers and thus think in terms of cybernetics or networked systems. For an account of cybernetics as the basis of the hacker worldview, see Turner (2006). For a discussion of Assange's cybernetic thinking, see Brunton (2011).

[3] Mette Mortensen (2014) has interpreted WikiLeaks' publication of the Collateral Murder video as a form of sousveillance but neither develops the theoretical aspect nor connects it to the cypherpunk movement.

cypherpunk movement as offering an intelligible, viable, and effective model of data activism and strategic agency.

Privacy and Transparency in Cypherpunk Ethics

To understand the genesis of the normative cypherpunk principle "privacy for the weak, transparency for the powerful," it is necessary to see how the movement emerged as a reaction to the Crypto Wars, which saw the US government face-off against computer specialists, privacy advocates, and hackers (Levy 2001). It is also necessary to acknowledge that as the movement evolved from the 1990s to the 2000s, a second- or third-generation of cypherpunks pushed the movement's perspective beyond the first-generation's emphasis on privacy to also advocate for institutional transparency. While there is a great deal of intergenerational agreement among the cypherpunks regarding privacy for the weak, there is also a great deal of intergenerational *dis*agreement among the cypherpunks regarding transparency for the powerful. It was therefore only with the later generations of cypherpunks that the basic principle of cypherpunks ethics would take on its full normative meaning.

The cypherpunks originally formed in response to attempts by the United States government to monopolize cryptography by keeping it out of the hands of the public. In January 1991, Senator Joe Biden, head of the Senate Judiciary Committee, cosponsored an anti-terrorism bill that would make it illegal for citizens to use unbreakable encryption to secure and protect their electronic documents and communications. As the legislation said, all telecommunications providers and device manufacturers "shall ensure that communication systems permit the government to obtain the plaintext contents of voice, data, and other communications when appropriately authorized by law" (qtd. in Levy 2001: 195). Shortly after this proposed legislation was made public, a group of cryptology enthusiasts in the San Francisco Bay Area decided to organize in opposition to the United States government's attempts to suppress the public availability of digital crypto. As a result, the cypherpunk movement was born (Levy 2001; Greenberg 2012). Throughout the 1990s, the cypherpunks joined with other activists to challenge the government's attempts to monopolize crypto, intentionally and repeatedly provoking state backlash by finding and distributing classified government documents about cryptology (Levy 2001). The government frequently attempted to prosecute or silence the cypherpunks and other like-minded crypto advocates, but in the end, all charges were dropped when a district court ruled that encryption software is code, code is speech, and speech is protected by the First Amendment. "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" (qtd. in Levy 2001: 302).

Given the cypherpunks' role in the Crypto War, it should come as no surprise that one half of their normative framework calls for "privacy for the weak." Cypherpunks commonly explain the threat to privacy in the digital age by comparing it to the late-eighteenth century, when the Framers of the US Constitution lived (Castronovo 2013). Back then, they say, it was possible for two people to walk to the edge of town and have a private conversation, thereby making it extremely difficult for anyone to surveil them (Castronovo 2013). In the digital age, however, when almost all communication and economic transactions take place over networked computer systems, nothing is private—unless one uses encryption. Thus, in "A Cypherpunk's Manifesto," Eric Hughes (2001: 81 argues that cryptography is a necessary tool for defending privacy in "the electronic age." As Hughes (2001: 81) defines it, "privacy is the power to selectively reveal oneself to the world." Unfortunately, he observes, "when my identity is revealed by the underlying mechanism of the transaction"—as is the case with digital transactions and communications—"I have no privacy. I cannot selectively reveal myself; I must always reveal myself" (Hughes 2001: 82). When an individual uses encryption, however, they are empowered because their ability to selectively reveal themselves to the world is restored. Because "we cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence," Hughes (2001: 82) insists, "we must defend our own privacy if we expect to have any." From its inception to its present incarnations, participants in the cypherpunk movement have generally shared a concern about privacy in the age of electronic communication.

The cypherpunk concern for privacy has been widely acknowledged, but because most commentators focus solely on the cypherpunks' advocacy for privacy, the cypherpunk call for "transparency for the powerful" has been underappreciated. There is also far more disagreement among cypherpunks about transparency than there is about privacy. To understand the normative meaning of transparency for the powerful as the cypherpunks conceive it, it is helpful to contrast two conceptions of this norm: Tim May's crypto anarchist conception of transparency and Julian Assange's justice-oriented conception of transparency.

In Tim May's (2001a) view, the cypherpunk movement is about promoting what he calls "crypto anarchy," a type of libertarian or anarcho-capitalist philosophy that identifies the widespread use of crypto as the beginning of the end of nation-state governments. May (2001a) argues that digital crypto promises to undermine the stability of nation-states in three ways. First, encrypting communication impedes the government's ability to surveil communications and censor information, which means that governments would no longer be able to control thought or speech. Second, cryptocurrencies undermine the government's control over money and impedes the government's power to collect taxes. A third reason for the eventual collapse of government, May (2001b: 74) argues, is the fact that "liquid markets in information" would "make secrets much harder to keep." In May's conception, most of these information markets would be economically motivated, meaning that information including government secrets would be sold to the highest bidders, but some of the information markets would attract whistleblowers and journalists. Not only could whistleblowers use encryption to disclose documents anonymously, May (2001b: 69) writes, but "the CIA can't stop newsgroups, sites, or Web pages that give away its secrets." For May, transparency for the powerful primarily means transparency for governments, though corporations that foolishly leave their documents unencrypted could become victims of corporate espionage. Nevertheless, he is clear that crypto does not entail transparency all around. Capturing the cypherpunk slogan nicely in one passage, he writes: "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 not 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: 90–91). In the end, May essentially understands transparency descriptively, as a basic fact about the implications of the widespread use of cryptography.

While May's (2001a) conception of cypherpunk transparency focuses largely on governments and provides space for the selling of secret documents, Julian Assange (2016) sees transparency for the powerful as a means of pursuing justice. On one hand, Assange does not differentiate governments, corporations, intelligence agencies, and major political parties, for he sees them all on a spectrum of organizations and institutions that attempt to gain as much power for themselves as possible. On the other hand, he eschews the idea of information black markets where secret documents are bought and sold, for in his view, the purpose of disclosing secret documents is not individual or organizational financial gain but justice, accountability, and knowledge (Assange 2011). Assange therefore understands transparency not in terms of market forces but in terms of modifying institutions in ways that make them potentially more just. Furthermore, as a key figure among third-generation cypherpunks, Assange adds a normative dimension to transparency that is missing from the thought of first-generation cypherpunks like May. Despite Assange's disagreement with May regarding how transparency will play out in practice, he nevertheless agrees that encryption is the technological basis for the social and political practice. By building an encrypted submission and publishing system, as Assange (2016) did with WikiLeaks, it becomes possible for whistleblowers to enforce transparency for the powerful without being detected, thus redistributing information and thereby redistributing power.[4]

In this context, it becomes possible to see why some criticisms of the cypherpunks are misleading if not misguided. First, we can see why Brin's (1998) criticism of the cypherpunks misunderstands the nature of the movement. Bossewitch and Sinnreich (2012: 231) argue that, because Brin (1998) naïvely treats all data

[4] Chelsea Manning was discovered and arrested because she confessed her actions in a chatroom and her confidant eventually reported her to the FBI (Zetter and Poulson 2010). To my knowledge, no other source of WikiLeaks' has ever been discovered, with perhaps one exception. See Anderson (2020).

collection as equal, he "fails to adequately account for the differential access to analytic processing power available to different individuals and organizations in making sense—and use—of this data." Lacking any account of power dynamics, they add, Brin (1998) problematically equivocates "privacy" and "secrecy" and therefore misunderstands the cypherpunks' claims. 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 view as an emerging "transnational surveillance dystopia" (Assange et al. 2012: 5). For the cypherpunks, therefore, privacy and secrecy are distinguished by power relations, and transparency corresponds to secrecy only.[5]

Second, we can see why attempts to lump cypherpunks in with mainstream crypto advocacy movements in fact distorts the broader visions of the movement. Some crypto advocates have been criticized for prioritizing the concerns of middle-class whites in Western societies over colonized and otherwise racially subjugated peoples, the people who experience the most directly violent and deadly results of datafication and surveillance (Gürses, Kundnani, and Van Hoboken 2016). On this view, the problem is that most mainstream Western crypto advocacy movements only oppose *their* government spying on *them*, while maintaining a deferential attitude toward standard imperial and colonial foreign policy practices.

While this critique could certainly apply to privacy-oriented, first-generation cypherpunks, especially May, whose thought unmistakably reflects a commitment to Western chauvinism (Greenberg 2012: 91–92), third-generation cypherpunks take a far more cosmopolitan, anti-imperialist approach to crypto advocacy. Such cypherpunks reject relying upon a "western eye" (Assange 2016: 144) when approaching global political issues, and they have expressed unequivocal criticism of drone wars, regime change operations, global mass surveillance, and imperial attempts to maintain and expand coercive spheres of influences (Assange et al. 2012; Assange 2015). For his own part, Assange has explicitly argued that crypto is an essential tool for anticolonial national movements. "Cryptography can protect not just the civil liberties and rights of individuals," Assange (2013) argues, "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." In this context, then, it becomes possible to appreciate the global meaning and application of "privacy for the weak, transparency for the powerful," the central principle of cypherpunk ethics.

The normative claims of the cypherpunks, then, entail a two-part principle through which individual privacy is defended and institutional transparency is pursued. While crypto can be used to reinforce privacy for the weak, as the first-generation cypherpunks advocated, it can also be used to promote transparency for the powerful, as later generations of cypherpunks have insisted. This normative framework emerged from the concrete political engagement of crypto advocates three decades ago and continues to provide a foundation for the global data activism of the cypherpunk movement.

Cypherpunk Epistemology as Data Activism

Given its use of information technology and software to challenge the contemporary power distribution in society, it should come as no surprise that, outside surveillance studies, the cypherpunk movement and its participants are commonly understood under the rubric of "hackers" and "hacking" (Coleman and Golub 2008; Villena Saldaña 2011; Marechal 2013; Dewi Horstmann 2020; Di Salvo 2020). The cypherpunks certainly share the playful and creative disposition of the original hacker cultures (Levy 2010; Assange et

[5] The cypherpunk conceptions of secrecy and privacy thus differ from the conceptions offered in Sissela Bok's (1982) influential conception.

al. 2012), but reducing the cypherpunks to "hackers" distorts our understanding of the movement in several ways. First, the term "hacker" is a highly contested and sometimes polarizing term that now has too many different meanings to too many different audiences, so calling the cypherpunks "hackers" may confuse more than clarify. Second, the cypherpunk movement drew its original inspiration from cryptographers and not hackers, two groups that were originally quite separate (Levy 2001). Third, most studies of the cypherpunks as hackers treat the issues of privacy and transparency as mutually exclusive, thereby failing to understand privacy and transparency as two sides of the same cypherpunk coin.

To move beyond the vagaries of the cypherpunk-as-hacker approach, we should instead situate the cypherpunks under a technical definition of data activism. Stefania Milan and Lonneke van der Velden (2016) argue that contemporary data activism can be defined by three key features: (1) it responds to the datafication of surveillance and society; (2) it advocates a hands-on approach; and (3) it both engages and appropriates digital surveillance and data technologies. Taken together, Milan and van der Velden (2016: 69) state that these features of data activism result in "alternative epistemologies" able to map new narratives of "our datafied social reality." They argue that this "conceptual map" provides a means for understanding technology-focused social movements in a more dynamic way. Based on its origins, its dispositions, and its principles, the cypherpunk movement embodies this conception of data activism, offering a *cypherpunk epistemology* where crypto occupies a central role in negotiating digitally mediated social relations.

First, Milan and van der Velden (2016: 61) state that there has been a "fundamental paradigm shift brought about by datafication." Since the late 1980s, scholars have documented the shift away from the mid-twentieth century trimodal conception of physical surveillance, psychological surveillance, and data surveillance (Westin 1967) to a combined pattern of datafication and digitization that subsumes those three modes under the rubric of dataveillance (Clarke 1988) and digital surveillance (Graham and Wood 2003). In the twentieth century, digital data surveillance has superseded or incorporated almost all older forms audio/video and electromagnetic databasing. Metadata is now a primary mode of surveillance, and its collection is driven by an ideology that data is a raw material waiting to be harvested (van Dijck 2014). Given this context, Milan and van der Velden (2016) suggest that data activists are in large part motivated by their awareness of the ubiquity of digital data surveillance.

The cypherpunks express a keen awareness of digital data surveillance, an awareness that can be traced genealogically back to the roots of the movement. David Chaum—who has been called "the prophet and godfather of digital anonymity" (Greenberg 2012: 65) and "the ultimate cypherpunk" (Levy 2001: 213)—was a mathematician and cryptographer whose writings influenced and in part inspired the formation of the cypherpunk movement. In the early 1980s, Chaum (1985: 1030) was concerned about the traceability of personal communications and transactions in national and global computerized systems, arguing 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." Importantly, Chaum's reaction to the early trend of datafication was catalyzed by his reading of David Burnham's *The Rise of the Computer State* (2014), which presciently warned of the dangers of massive computerized bureaucracies and databases that enable the tracking of every individual's actions. "The loss of privacy," Burnham (2014: 9–10) writes, "is a key symptom of one of the fundamental social problems of our age: the growing power of large public and private institutions in relation to the individual citizen," specifically the use of "computers and data bases and computerized communication networks" and the ways in which powerful institutions use these technologies to "influence what we think is important." The cypherpunks' advocacy of strong crypto, therefore, emerged from the paradigm shift caused by datafication and a growing perception of digital data surveillance.

Second, Milan and van der Velden (2016: 62) argue that data activists take a hands-on approach, making sure not only to theorize but also to *act*, because they are inspired by "notions of access to information, code tinkering, collaboration, and world improvement through technical fixes." This hands-on disposition is distinctly expressed in Hughes' cypherpunk manifesto. "Cypherpunks write code," Hughes (2001: 82–83) famously writes. "The Cypherpunks are actively engaged in making the networks safer for privacy." Indeed,

cypherpunks created many digital tools using encryption, including anonymous email systems, digital currencies, and other privacy and anonymity programs. Because "privacy extends only so far as the cooperation of one's fellows in society," Hughes (2001: 82–83) explains that cypherpunk "code is free for all to use." Not only did the cypherpunks write code, then, they also distributed it for others to use, a practice that remains a cypherpunk standard to today (Assange et al. 2012).

Third, and most importantly, Milan and van der Velden (2016) observe that data activists both engage and appropriate digital surveillance and data technologies. For Milan and van der Velden (2016: 65–66), data activism is polysemic *and* holistic: polysemic because it incorporates "discrete but complementary means to achieving political goals" and holistic because it is nuanced enough to recognize "the harmful and productive qualities of the 'big data' phenomenon." Thus, data activism simultaneously involves both re-active data activism and pro-active data activism. Re-active data activism describes defensive activity, such as using "encryption or anonymity networks to resist monitoring by state[s] and corporations," while pro-active data activism describes offensive activity, such as relying on data as a means of "supporting alternative narratives of the social reality, questioning the truthfulness of other representations, denouncing injustice, and advocating for change" (Milan and van der Velden 2016: 67). Though these two strategies would seem contradictory to analyses like those offered by Brin (1998), Milan and van der Velden (2016: 67) insist that they are complementary because "both take information as a constitutive force in society capable [of shaping] social reality."

The cypherpunk slogan "privacy for the weak, transparency for the powerful" perfectly embodies the synthesis of re-active and pro-active responses of data activism to datafication. When the cypherpunks advocate the use of encryption to achieve privacy for the weak, they are taking a re-active approach to their activism. End-to-end encrypted messaging applications, encrypted email accounts, virtual private networks (VPNs), Tor browser, and Bitcoin all embody the defense mode of data activism. Likewise, when cypherpunks advocate for the use of encryption to achieve transparency for the powerful, they are taking a pro-active approach to their activism. Since the 1990s, cypherpunks have theorized *and* built a number of crypto-based transparency platforms, such as Tim May's BlackNet and John Young's cryptome.org (Greenberg 2012), yet Assange's WikiLeaks may represent the most matured manifestation of this offensive mode of data activism. In the case of WikiLeaks, secure encrypted submission drop boxes make it possible to protect whistleblowers in a way that was not possible before the internet, thereby reducing the chances that a whistleblower will be caught and thus lowering what Assange (2016) calls the "courage threshold." And because large, powerful institutions cannot function without massive digital bureaucracies (Assange 2016), Assange (2006, 2015) argues that the mere threat of documents leaking forces such institutions to enact an endless series of defensive measures, reducing the ability of these institutions to carry out secretive, harmful policies.

Milan and van der Velden (2016) explain that their conception of data activism is a spectrum, with re-active and pro-active data activism on opposite ends. Some movements, they note, can synthesize the two ends of the spectrum, but they do not explore the ways in which the cypherpunks stand as a paradigmatic example of data activism so conceived. By understanding the cypherpunks as data activists in this way, we not only better understand the nuances of cypherpunk ethics but also better understand what it means to bring re-active and pro-active data activism together in a coherent approach to social and technological engagement.

Furthermore, while other movements may also be properly classified as data activism in this sense, cypherpunk epistemology is distinctive in at least one sense: its emphasis on crypto. Many social movements can and do rely on cryptography to preserve the integrity of their communications and to achieve other ends, but the cypherpunks are clear that the movement follows from the technology (Assange et al. 2012). Importantly, this emphasis on crypto suggests that cypherpunk epistemology taps into the logic of electronic communication in ways that other alternative epistemologies may not. In his analysis of the telegraph, the first electronic medium, James Carey (2009: 157, 162) argues that "the telegraph was not only a new tool of commerce but also a thing to think with, an agency for the alteration of ideas," a creation that reworked "the nature of awareness itself." By extension, the telegraph created the conditions for the transformation of

encrypted communication. As the historian of cryptology David Kahn (1967: 189) unequivocally observes, "The telegraph made cryptography was it is today." Taken together, Carey (2009) and Kahn's (1967) insights suggest that crypto is a fundamental part of human awareness in the electronic age. To the extent that the computer is an extension of the telegraph, as Carey (2009) suggests, cypherpunk epistemology stands out among other forms of data activism by giving crypto a central technological and ethical role in the movement's activism.

As a form of data activism, then, cypherpunk epistemology understands the datafication of social relations and responds with practical pro-active and re-active, offensive and defensive, strategies of resistance. As such, cypherpunk epistemology represents a form of what Matthew Zaia (2019) has called oppositional and participatory surveillance consciousness. Cypherpunk epistemology is oppositional because it contests power relations by going up against surveillance, and it is participatory because it engages the digital technologies that make contemporary surveillance possible, turning those technologies into technologies of resistance.

Cypherpunk Sousveillance: Rethinking WikiLeaks

WikiLeaks founder Julian Assange was one of the original contributors to the cypherpunk mailing list and today remains one of the most prominent spokespersons of the later generations of the movement (Manne 2011; Greenberg 2012; Assange et al. 2012). When Assange (2016) created WikiLeaks, he was motivated by the cypherpunk demand for transparency for the powerful. As Assange (2011: 79) explains, "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." WikiLeaks, therefore, embodies a practice of *cypherpunk sousveillance*. Cypherpunk sousveillance agrees with more classical theories of sousveillance that relations of power (Mann and Ferenbok 2013) and authority (Ali and Mann 2013) are central to surveillance and sousveillance, but it also joins more contemporary forms of sousveillance in moving beyond the traditional audio/video mode of sousveillance (Mann 2002), exploring the use of digital networks and databases to promote new modes of watching the watchers. In the transition from audio/video sousveillance to various forms of digital data sousveillance, theorists have focused on the *content* of sousveillance while neglecting the *form* of sousveillance. Cypherpunk sousveillance revitalizes our attention to sousveillance form in the context of contemporary digital data sousveillance.

Theories of classic forms of audio/video sousveillance are clear that both the content and the form of sousveillance are important aspects of the practice. With classic sousveillance, the sousveiller uses audio/video technology in response to audio/video surveillance, the resulting situation pits camera against camera (Mann, Nolan, and Wellman 2003). This practice has been commonly used against law enforcement, a practice called "cop watching" (Schaefer and Steinmetz 2014). In such a situation, the sousveiller collects information about the recorded officer (or other subject) and can then later use the contents of the data as part of the evidentiary basis for claims against power, such as in court proceedings (Ali and Mann 2013). Sometimes sousveillance reveals information about surveillance practices (Mann, Nolan, and Wellmann 2003), and other times it simply provides general knowledge about powerful, surveilling institutions (Ali and Mann 2013).

In addition to providing *content* to the sousveiller, the *form* of audio/video sousveillance imposes upon its subjects a new media environment in which they are compelled to alter their behavior. In the context of cop watching, Ajay Singh (2017) argues that citizens do not necessarily wait until police brutality is in progress to record police actions but that in many instances such sousveillance is anticipatory. In a policing environment he calls the Prolepticon, Singh (2017: 678) observes, "as cellphone-enabled citizens continue to anticipate negative police encounters and film the actions of law enforcement, with footage remaining in control of the citizen[s] who then use the internet to propagate these videos around the world, they are creating an environment where officers no longer know if they are being surveilled, leading police to become

self-disciplining subjects." In Singh's (2017) Prolepticon, it is not the content of the video recordings of the police that are important; instead, it is the very omnipresence of the camera-equipped smart phone that is important. When the police do not know when, where, or by whom they may be recorded, they must always assume that they may be being recorded. Thus, they are more likely to refrain from behavior that they do not want recorded and shared.

With the rise of datafication, dataveillance, and databases, new digital forms of this type of sousveillance have emerged alongside classical audio/video sousveillance. These forms of digital data sousveillance have been theorized regarding the contents of what the sousveillance reveals. Fernando van der Vlist (2017), for example, has drawn upon the documents disclosed by Snowden to offer a "critical cartography" of the United States' surveillant assemblage, revealing the ways in which public and private partnerships constitute the basis for contemporary digital dataveillance. Colin Burke (2020) has similarly mapped the United States surveillant assemblage, drawing upon documents disclosed by WikiLeaks to demonstrate a method he calls "digital sousveillance." Finally, Shaul Duke (2019: 500) argues that data sousveillance—which he calls "database-driven empowering surveillance"—is an effective tool for marginalized groups to monitor the activities of their political opponents. This practice includes "all those initiatives that focus on building a database of the surveillance-acquired data and disseminating information to provoke a change." Though Duke (2019) prefers the term "empowering surveillance" to "sousveillance," the idea is similar: that databases can be used to watch the powerful from below. By moving beyond the audio/video mode of sousveillance pioneered by Mann (2002), van der Vlist (2017), Burke (2020), and Duke (2019) show that it is possible to use the contents of digital data sousveillance to understand and, perhaps, neutralize surveillance and other forms of oppressive power in the digital age.

As a platform informed by cypherpunk ethics, WikiLeaks represents a form of cypherpunk sousveillance that uses digital data sousveillance to collect documents and databases to distribute those documents to the global public. Like other forms of digital data sousveillance, WikiLeaks enables the analysis of sousveillance *content* to map surveillance assemblages and to understand the often-secret actions of the powerful. Similar to the work called for by van der Vlist (2017) and Burke (2020), some of WikiLeaks' publications, such as the Vault 7 collection, permit the mapping of the surveillance capabilities of the state. Vault 7—which includes "thousands of pages describing sophisticated software tools and techniques used by the [Central Intelligence Agency] to break into smartphones, computers and even Internet-connected televisions" (Shane, Rosenberg, and Lehren 2017)—reveals to the global public previously unknown points of data and device vulnerability, empowering individuals to change their security and privacy practices in response to new information about their surveillance environment. Likewise, similar to the work called for by Duke (2019), other WikiLeaks publications, such as the Iraq War Logs, the Afghan War Diary, and US State Department cables, permit publics to understand how powerful state actors and military personnel conduct their affairs behind closed doors, providing a chance for democratic oversight (Benkler 2011; Assange 2015). WikiLeaks therefore practices data sousveillance to provide citizens and publics around the world with information about their surveillance situation and with general information about powerful actors.

But there is another perhaps even more important sense in which WikiLeaks represents cypherpunk sousveillance, for sousveillance does not merely inform us about surveillance or report data on elites' activity, it also intervenes to alter power relations at the system level through its very *form*. Similar to the Proleptic cop watching described by Singh (2017), for instance, WikiLeaks provides an anticipatory platform for whistleblowers. While WikiLeaks does receive and publish documents about a wide array of abuses on an ongoing basis, according to Assange (2006), the sousveillance enabled by WikiLeaks turns every insider into a potential source, leaker, or whistleblower. To paraphrase Singh (2017), WikiLeaks seeks to create an environment where political and economic elites no longer know if they are being surveilled, leading them to become self-disciplining subjects.

To understand the implications of WikiLeaks' intervention, we can draw upon Steve Mann's (2002) discussion of open-systems, closed-systems, and feedback loops. Following the September 11 terrorist

attacks, the US government implemented a series of national security measures that simultaneously increased government secrecy and government surveillance. These steps were taken, of course, in the name of stopping terrorism. Mann (2002), however, argues that the government took the wrong perspective on terrorism. For while the government was convinced that it was an apparent lack of surveillance that allowed the 9/11 terrorists to slip past intelligence agencies, Mann (2002) argues that terrorism is a response to a seemingly unaccountable government. Whereas the government believed that privacy enabled terrorists, Mann (2002) argues that secrecy inspired terrorists. So, to make the government even more secret was to exacerbate the problem. Without proper external feedback, an increasingly secretive government will only continue to consolidate power unchecked. As Mann (2002) puts it, "Secret organizations often run open-loop, without the normal feedback mechanisms that provide important checks and balances… It is not privacy that is the cause of the problem. It is not the unphotographed, unfingerprinted, unsurveilled citizens who are to blame, but, rather, it is the larger pressure cooking machinery that needs to be stopped." Mann (2002) suggests that the mere act of effectively "watching back," so to speak, changes the operation of the system by modifying the feedback.

In a similar manner, Assange (2006) argues that secrecy is the primary cause of all government corruption, wrongdoing, and authoritarianism, and that by creating a condition of seemingly omnipresent sousveillance, it is possible to reduce secrecy and therefore the harms that result from corruption. Assange (2006) defines "conspiracy" as the making of secret plans and jointly committing harmful actions; based on this definition, all harmful government and corporate policies that are enabled by secrecy are conspiratorial. Governments keep their harmful, nefarious plans secret because if the public were to find out about and disapprove of the plans, then the plans could be stopped before they are implemented. But as Assange (2006) observes, modern governments require massive bureaucracies to properly function, and because bureaucracies in the digital age keep their records on computer networks, it becomes increasingly easy for insiders to disclose large document caches. While Assange's hacker ethic forbids the stealing of documents (Dreyfus and Assange 2012: 79; Assange 2011: 93), it does not preclude the creation of an encrypted whistleblowing platform. "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: 131). When documents are leaked from powerful institutions, the otherwise open loop closes in two ways. On one hand, there is the *content*: publics can read the documents and express their disapproval of the revealed plans, potentially preventing those plans from being enacted (Assange 2016). On the other hand, there is the *form*: because it never knows when it is being watched from its own insiders, the institution itself constricts its internal communication networks, undermining its own ability to properly function and thus undermining its ability to carry out nefarious plans (Assange 2006; Bady 2010; Brunton 2011).

Cypherpunk sousveillance, then, makes two important contributions to the theory and practice of sousveillance. First, as discussed above, in the transition from audio/video sousveillance to digital data sousveillance, theorists have tended to increasingly focus on content rather than form. Cypherpunk sousveillance redirects our attention back to the form of digital data sousveillance and allows us to see how Singh's (2017) Prolepticon can be expanded beyond audio/video modalities. Second, because of the central role of crypto in cypherpunk ethics and cypherpunk epistemology, cypherpunk sousveillance also shows us that crypto need not be understood solely for its privacy-enhancing functions. Ali and Mann (2013) suggest that crypto and "veillance" are unrelated, but the cypherpunks show that crypto can be used to promote sousveillance through the construction of encrypted whistleblowing and publishing platforms.

Battle of the Black Holes: NSA and Google vs. Cypherpunks

Cypherpunk *ethics* offers a normative framework for engaging digital surveillance technologies; cypherpunk *epistemology* reflects a form of data activism that combines pro-active and re-active strategies to challenge existing distributions of surveillance, information, and power; and cypherpunk *sousveillance*, as a product of the first two, provides a method of putting the cypherpunk call for transparency for the powerful into practice. Taken together, the cypherpunk worldview provides a novel perspective on our

contemporary surveillance situation because the basic principles and practices called for by the cypherpunks mirror the principles and practices of the most powerful public and private surveillance institutions: the NSA and Google. Using Bossewitch and Sinnreich's (2012) notion of "information flux," it becomes possible to see that the NSA and Google both strive to be what they call "black holes," which means they work to collect as much data *about* others as possible while simultaneously working to prevent emitting any data *to* others. In a world dominated by such institutions, the cypherpunks provide an appropriate response, for in practicing "privacy for the weak, transparency for the powerful," they advocate the use of crypto to simultaneously protect one's individual data while collecting data about large, powerful organizations. In this sense, cypherpunk ethics provides individuals with concepts, practices, and tools necessary to navigate the world in a time of mass digital data collection.

Adapting the notion of flux—defined as "the rate of flow of 'stuff' passing through a given surface"—Bossewitch and Sinnreich (2012) argue that contemporary information flows can be conceived of as fluxes. They note that, in recent decades, the volume of information flowing across networked spaces has increased exponentially, but because these flows are multidirectional—passing to, from, and between individuals, organizations, and systems—it is necessary to understand how each entity in an information network relates to the network. Studying a whole information network—such as the total aggregate information flows within a country like the United States—would allow us to understand the net direction of information movement. To do so, we would need to understand which entities emit and collect information and to what degree. Importantly, Bossewitch and Sinnreich (2012: 227) argue that determining information flux helps us understand "the emerging knowledge/power dynamics" under contemporary surveillance regimes and within a networked society.

Bossewitch and Sinnreich (2012) explain that there are three modes of information flux: neutral, positive, and negative. They note that these terms are not normative; the terms simply describe the types of flow and, in some cases, a negative information flux can be good, and a positive information flux can be bad. *Neutral flux* describes a state of affairs in which all parties have equal and open access to all information, a situation of "perfect transparency."[6]

For Bossewitch and Sinnreich (2012), in our contemporary surveillance situation, the two most important fluxes are positive and negative. *Positive flux* describes a state of affairs in which one person or institution leaks or emits more information than it collects, meaning that other actors have relatively greater access to information than this person or institution. *Negative flux* describes a state of affairs in which one person or institution collects more information than it leaks or emits, meaning that this person or institution has relatively greater access to information than other actors. If information is power, then those persons and institutions who desire power will attempt to maintain the strongest possible negative flux. Some actors will attempt to be what Bossewitch and Sinnreich (2012: 11–12) call a "voracious collector," an actor that pursues an intensive information-gathering strategy without necessarily trying to prevent themselves from emitting any data. However, other actors who desire even more power will attempt to become what Bossewitch and Sinnreich (2012: 232) call a "black hole," an actor that "attempts to collect and analyze as much information as possible from the outside, while leaking as little as possible." In a sense, information black holes parallel the notion of data activism, for to become a black hole, a person or institution must simultaneously seek out information (pro-active) and defend their own data (re-active). In Bossewitch and

[6] This situation of neutral flux describes a social situation reminiscent of Brin's (1998) transparent society or Ali and Mann's (2013) Veillance society (or a situation of equiveillance [Mann and Ferenbok 2013]). Jean-Gabriel Ganascia (2010) has argued that we have already achieved this type of transparent society. While it is true that personal computers and smart devices decenter the power to watch to a degree, this view fails to consider the net information flux of overall information systems. While I reject the notion that we have achieved a transparent society, I would also argue that even the call for a transparent society not only misunderstands power dynamics but also dangerously undermines personal privacy, the benefits of which and the threats to which have been detailed by scholars for a half century (Westin 1967; Benn 1971; Greenwald 2014; Sloan and Warner 2015; Zuboff 2019).

Sinnreich's (2012) conception, a black hole is both polysemic *and* holistic because it uses discrete but complementary strategies to increase its power and reinforce its position within an information system.

The black hole strategy is best embodied in the world's two most powerful surveillance institutions: the NSA and Google. The NSA is a black hole of information flux because it wants to know everything about every person and organization outside of its walls while simultaneously defending its own extreme secrecy—an *absolute* negative flux. On one hand, documents disclosed by Edward Snowden revealed that one of the NSA's surveillance mottos is "Sniff It All, Know It All, Collect It All, Process It All, Exploit It All" (qtd. in Greenwald 2014: 97). Glenn Greenwald (2014: 94) captures the NSA's desire to know everything: "The agency is devoted to one overarching mission: to prevent the slightest piece of electronic communication from evading its systemic grasp." On the other hand, the NSA has always been highly secretive about its internal operations, a disposition that has inspired jokes that NSA stands for "No Such Agency." Not only was the NSA created by a secret executive order, the US government denied its existence for the first ten years it was operational (Bamford 1982). Famously surrounded by "the Triple Fence," the NSA headquarters at Fort Meade is a paradigmatic representation of organizational secrecy. As Steven Levy (2001: 15) writes, "the triple-depth electrified and barbed-wire fence surrounding its headquarters was not only a physical barrier but a metaphor for the NSA's near fanatical drive to hide information about itself and its activities." While Snowden's disclosures demonstrate that not even NSA-level secrecy can prevent all data leaks, the NSA nevertheless strives to become a black hole, attempting to achieve an absolute negative information flux in which all information comes in and no information goes out.

Google, the NSA's private sector surveillance sibling, also strives for black hole status. While we might be tempted to think that Google imitates the NSA, the reverse is in fact true. As Shoshana Zuboff (2019) notes, after 9/11, the NSA sought Google's assistance with their surveillance objectives and tried to imitate the Silicon Valley giant. Motivated by the need for advertising revenue, Google became aggressive in its data acquisition, collecting anything and everything it could about its users; this surveillance capitalism model eventually pushed Google to expand beyond search, offering email, browsers, operating systems, and smart phones, all of which would allow Google to swallow up massive amounts of data about user activity. In a sense, Google is the "Sniff It All, Know It All, Collect It All" institution of the private sector. Also like the NSA, Google is highly secretive, especially about its algorithms, for the company's ability to collect data—often without users' knowledge—is the key to its financial success. Commenting on the company's secrecy, former Google executive Douglas Edwards states, Larry Page "opposed any path that would reveal our technological secrets or stir the privacy pot and endanger our ability to gather data" (qtd. in Zuboff 2019: 89). Rather than offer users the chance to provide informed consent for its data gathering, Google instead opted to work in "total secrecy" (Levine 2018). Like the NSA, Google is not necessarily completely impervious to leaked information, but it shares the drive to become an information black hole by maintaining the strongest possible negative information flux.

In relation to the information black holes created by these two enormous surveillance institutions (among others), cypherpunk ethics advocates a simple response: *become a black hole yourself*. The cypherpunk slogan "privacy for the weak, transparency for the powerful" calls for citizens and activists to not only defend their own individual privacy but also to collaborate on privacy-enhancing and transparency-enforcing projects. The principles of cypherpunk ethics allow individuals to learn about, understand, and use technological tools in order to create for themselves a negative flux of information, helping them respond to their surveillance surroundings by simultaneously protecting their personal or organizational data (re-active) and gathering all possible data about their networked environments (pro-active). Translating cypherpunk ethics into the technical language of the NSA, we might say that "privacy for the weak" corresponds to the NSA's practice of communications security (COMSEC), while "transparency for the powerful" corresponds to the NSA's practice of signals intelligence (SIGINT) (Bamford 1982: 57). While the NSA is both collecting all unencrypted communications of others and ensuring that its own communications are protected with the strongest encryption possible, the cypherpunks call for individuals to reverse this practice, turning it back upon the governmental and corporate institutions that seek to consolidate power.

While privacy is an obvious and well-established concern of the cypherpunks (Levy 2001; Greenberg 2012), that concern takes on new meaning when placed in conjunction with cypherpunk sousveillance. Assange (2011: 22), for example, has argued that WikiLeaks is "an intelligence agency of the people," and in this sense, it mirrors the work of the NSA but from the position of the powerless. For Assange, the primary difference between WikiLeaks and traditional state intelligence agencies is that the former publishes—meaning it makes public the results of its investigations—while the latter does not (Scahill 2017). This distinction is crucial because if WikiLeaks is indeed an intelligence agency of the people, if it is indeed an organization that practices cypherpunk sousveillance, then it is one means by which whistleblowers, journalists, and activists can challenge black holes like the NSA, Google, and other public and private institutions, contesting the power dynamics of our modern surveillance society and achieving accountability for the powerful. As the embodiment of pro-active data activism, WikiLeaks seeks to play a role in preventing powerful surveilling institutions from achieving the absolute negative information flux they seek.

To be sure, just as the NSA and Google cannot achieve absolute negative flux, neither can individuals. But achieving an absolute negative flux is not the purpose of cypherpunk ethics. If cypherpunks advocate the protection of privacy, and if privacy is the ability to freely and selectively reveal oneself to the world, then an absolutely negative flux is not merely impossible but also undesirable, for it would entail breaking off normal human relationships, a result that is anathema to the cypherpunk ethos. Nevertheless, cypherpunk ethics does at least offer what Bossewitch and Sinnreich (2012) argue is needed, namely, a simple model for understanding how practical engagement with technology and networked communication systems can help individuals exercise their agency over information flows and manipulate them in the service of restoring fair power balances.

This discussion of information flux and black holes allows us to construct a more dynamic conception of the relationship between surveilling institutions and resisting social movements. Journalist Yasha Levine (2018: 203–204), for example, describes the cypherpunk movement as the mirror image of the public-private surveillance apparatus in the US, writing:

> The cypherpunk vision of the future [is] an inverted version of the military's cybernetic dream pursued by the Pentagon and Silicon Valley: instead of leveraging global computer systems to make the world more transparent and predictable, cypherpunks wanted to use computers and cryptography to make the world opaque and untrackable. It was a counterforce, a cybernetic weapon of individual privacy and freedom against a cybernetic weapon of government surveillance and control.

While this explanation is somewhat insightful, it is limited. When we conceive of the relation between Pentagon and Silicon Valley institutions and the social movements that challenge their power in terms of information flux, we see that there is not an "inverted" relation. Instead, we see that the contest over information flows occurs between various entities who attempt to impose some control over the overall flux. The Pentagon and Silicon Valley are concerned about more that transparency, for they desire transparency for *others* and secrecy for *themselves*. Likewise, the cypherpunks are not merely concerned with privacy for the weak; they also seek transparency for the powerful. The battle is not between transparency and privacy. The battle is a competition between black holes who seek to impose a regime of information flux conducive to their interests.

Conclusion

Twenty years ago, David Lyon (2001: 33) wrote that "Surveillance is diffusing decisively into society at large, although it should be noted that this does not mean that the capacity to answer back has now exceeded the power of state surveillance upon its citizens." Ten years ago, Kate Shilton (2010: 147) argued that the ability to answer back still had not been achieved, but she added that "the emergence of participatory sensing," the use of data to empower individuals and movements against governments and corporations, "brings us closer to such a possibility." Yet today, it seems as though we are still quite far off from the

ability to meaningfully "answer" the surveillance assemblage. In this paper, I have argued that the cypherpunk movement provides, in the words of Bossewitch and Sinnreich (2012), a simple and effective model of resistance and participation. Cypherpunk ethics offers a normative principle calling for privacy for the weak and transparency for the powerful. Cypherpunk epistemology presents cryptography as an effective means for simultaneously pursuing the re-active and pro-active data activism that the movement's normative principle requires. Cypherpunk sousveillance is a practice designed to realize the pro-active aim of transparency for the powerful, while emphasizing benefits or effects of *both* the form and content of digital data sousveillance. Taken together, the cypherpunk worldview calls for individuals to become (or at least approximate) information black holes, the mirror image of the dominant government and corporate nodes in the surveillance assemblage.

This paper also contributes to several areas of scholarship in surveillance studies and beyond. First, this paper extends previous scholarship on WikiLeaks, surveillance, and sousveillance by articulating the cypherpunk content form which WikiLeaks grows (Fuchs 2011; Andrejevic 2014; Mortesen 2014). Second, this paper revives discussions of sousveillance form in the content of contemporary digital data sousveillance, which is important because the contents of sousveillance documents are often subject to highly debated and competing interpretations (Mortesen 2014; Reilly 2015). Third, this paper expands surveillance studies discussions of cryptography, pushing the conversation beyond crypto's role in achieving privacy and raising important insights about crypto's possible roles in sousveillance (Leistert 2012; Verde Garrido 2015). Fourth, this paper shows that the cypherpunk model of data activism successfully synthesizes transparency activism and privacy activism into a meaningful whole, providing a possible model for scholars and other activists do to the same. Finally, Lee Wilkins and Renita Coleman (2004) argue that practitioners build their moral worlds through action *and* reflection, which means that theory and practice inform each other. By considering the ideas and theories of activists like the cypherpunks, scholars can more effectively reflect on and question the dominant narratives and ways of knowing that structure their own epistemic milieu (Milan and van der Velden 2016).

The cypherpunk paradigm "privacy for the weak, transparency for the powerful" offers a compelling strategy of response to the contemporary use of surveillance by powerful institutions, and cypherpunks provide technological, moral, epistemic, and practical means of achieving the world they envision.

References

Ali, Mir Adnan, and Steve Mann. 2013. The Inevitability of the Transition from a Surveillance-Society to a Veillance-Society: Moral and Economic Grounding for Sousveillance. Presented at *The IEEE International Symposium on Technology and Society, Ontario, CA, June 27–29,* 243–254. Piscataway, NJ: IEEE.

Anderson, Patrick. 2020. Privacy for the Weak, Transparency for the Powerful: The Cypherpunk Ethics of Julian Assange. *Ethics & Information Technology* 23: 295–308.

Andrejevic, Mark. 2014. WikiLeaks, Surveillance, and Transparency. *International Journal of Communication* 8: 2619–2630.

Assange, Julian. 2006. Conspiracy as Governance. *Cryptome.org*, December 3. http://archive.fo/kr8Pr [accessed February 10, 2022].

———. 2011. Of the People and For the People. *New Statesman*, April 5.

———. 2013. How Cryptography is a Key Weapon in the Fight Against Empire States. *The Guardian*, July 9. https://archive.ph/Mbsx4 [accessed February 10, 2022].

———. 2014. Who Should Own the Internet? *New York Times*, December 4. https://archive.fo/vxLJd [accessed February 10, 2022].

———. 2015. Introduction: WikiLeaks and Empire. In *The WikiLeaks Files: The World According to US Empire*, by WikiLeaks, 1–19. New York: Verso.

———. 2016. *When Google Met WikiLeaks*. 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.

Bady, Aaron. 2010. Julian Assange and the Computer Conspiracy: "To Destroy this Invisible Government." *zunguzungu* (blog), November 29. http://archive.fo/4nIaQ [accessed February 10, 2022].

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

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.

Benn, Stanley I. 1971. Privacy, Freedom, and Respect for Persons. In *Privacy and Personality*, edited by R. L. Ciochon, 1–26. New York: Routledge.

Bok, Sissela. 1982. *Secrets: On the Ethics of Concealment and Revelation*. New York: Pantheon Books.
Bossewitch, Jonah, and Aram Sinnreich. 2012. The End of Forgetting: Strategic Agency Beyond the Panopticon. *New Media & Society* 15 (2): 224–242.
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.
Burke, Colin. 2020. Digital Sousveillance: A Network Analysis of the US Surveillant Assemblage. *Surveillance & Society* 18 (1): 74–89.
Burnham, David. 2014. *The Rise of the Computer State: The Threat to Our Freedoms, Our Ethics and Our Democratic Process*. New York: Random House.
Carey, James. 2009. *Culture as Communication: Essays on Media and Society*. Revised edition. New York: Routledge.
Castronovo, Russ. 2013. Ben Franklin and WikiLeaks. *Critical Inquiry* 39 (3): 425–450.
Chaum, David. 1985. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM* 28 (10): 1030–1044.
Clarke, Roger. A. 1988. Information Technology and Dataveillance. *Communications of the AMC* 31(5): 498–512.
Coleman, E. Gabriella, and Alex Golub. 2008. Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism. *Anthropological Theory* 8 (3): 255–277.
Dewi Horstmann, Nina. 2020. The Power to Selectively Reveal Oneself: Privacy Protection among Hacker-activists. *Ethnos*: https://doi.org/10.1080/00141844.2020.1721549.
Di Salvo, Philip. 2020. *Digital Whistleblowing Platforms in Journalism: Encrypting Leaks*. Cham, CH: Palgrave Macmillan.
Dreyfus, Suelette. 2012. Introduction to *Underground*, Second Edition. In *Underground*, Suelette Dreyfus and Julian Assange, xi–xix. Edinburgh, UK: Canongate Books.
Dreyfus, Suelette, and Julian Assange. 2012. *Underground*. Edinburgh, UK: Canongate Books.
Duke, Shaul A. 2019. Database-Driven Empowering Surveillance: Definition and Assessment of Effectiveness. *Surveillance & Society* 17 (3/4): 499–516.
Fuchs, Christian. 2011. WikiLeaks: Power 2.0? Surveillance 2.0? Criticism 2.0? Alternative Media 2.0? A Political-Economic Analysis. *Global Media Journal: Australian Edition* 5 (1): http://archive.fo/8s73J.
Ganascia, Jean-Gabriel. 2010. The Generalized Sousveillance Society. *Social Science Information* 49 (3): 489–507.
Graham, Stephen, and David Wood. 2003. Digitizing Surveillance: Categorization, Space, Inequality. *Critical Social Policy* 23 (2): 227–248.
Greenberg, Andy. 2012. *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information*. New York: Dutton.
Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*. New York: Picador.
Gürses, Seda, Arun Kundnani, and Joris Van Hoboken. 2016. Crypto and Empire: The Contradictions of Counter-Surveillance Advocacy. *Media, Culture & Society* 38 (4): 576–590.
Haggerty, Kevin. D., and Richard V. Ericson. 2000. The Surveillant Assemblage. *British Journal of Sociology* 51 (4): 605–622.
Holden, Joshua. 2017. *The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption*. Princeton, NJ: Princeton University Press.
Hughes, Eric. 2001. A Cypherpunk's Manifesto. In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 81–84. Cambridge, MA: MIT Press.
Kahn, David. 1967. *The Codebreakers: The Story of Secret Writing*. New York: Macmillan Publishing.
Lee, Ashlin. 2015. Integrating Subjects: Linking Surveillance Experiences to Social Patterns Using Ethno-Epistemic Assemblages. *Surveillance & Society* 13 (3/4): 385–399.
Leistert, Oliver. 2012. Resistance against Cyber-Surveillance within Social Movements and How Surveillance Adapts. *Surveillance & Society* 9 (4): 441–456.
Levine, Yasha. 2018. *Surveillance Valley: The Secret Military History of the Internet*. New York: Public Affairs.
Levy, Steve. 2001. *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*. New York: Penguin.
———. 2010. *Hackers: Heroes of the Computer Revolution—25th Anniversary Edition*. Cambridge, MA: O'Reilly Media.
Lyon, David. 2001. *Surveillance Society*. Buckingham, UK: Open University Press.
Mann, Steve. 2002. Sousveillance, Not Just Surveillance, in Response to Terrorism. *Metal and Flesh* 6 (1): 1–8.
———. 2020. Wearables and Sur(over)-Veillance, Sous(under)-Veillance, Co(So)-Veillance, and MetaVeillance (Veillance of Veillance) for Health and Well-Being. *Surveillance & Society* 18 (2): 262–271.
Mann, Steve, and Joseph Ferenbok. 2013. New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World. *Surveillance & Society* 11 (1/2): 18–34.
Mann, Steve, Jason Nolan, and Barry Wellmann. 2003. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society* 1 (3): 331–355.
Manne, Robert. 2011. The Cypherpunk Revolutionary. *The Monthly*, February 16. http://archive.fo/kwI60 [accessed February 10, 2022].
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, Aaron K., Rosamunde E. van Brakel, and Daniel J. Bernhard. 2009. Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework. *Surveillance & Society* 6 (3): 213–232.
May, Timothy. 2001a. The Crypto Anarchist Manifesto. In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 61–64. Cambridge, MA: MIT Press.

———. 2001b. Crypto Anarchy and Virtual Communities. In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 65–80. Cambridge, MA: MIT Press.

Milan, Stefania, and Lonneke van der Velden. 2016. The Alternative Epistemologies of Data Activism. *Digital Culture and Society* 2 (2): 57–74.

Moore, Adam D. 2011. Privacy, Security, and Government Surveillance: WikiLeaks and the New Accountability. *Public Affairs Quarterly* 25 (2): 141–156.

Mortensen, Mette. 2014. Who is Surveilling Whom? Negotiations of Surveillance and Sousveillance in Relation to WikiLeaks' Release of the Gun Camera Tape *Collateral Murder*. *Photographies* 7 (1): 23–27.

Reilly, Paul. 2015. Every Little Helps? YouTube, Sousveillance and the "Anti-Tesco" Riot in Stokes Croft. *New Media & Society* 17 (5): 755–771.

Scahill, Jeremy. 2017. WikiLeaks vs. the CIA. *Intercepted*, April 19. https://archive.md/ODOuv [accessed February 10, 2022].

Schaefer, Brian P., and Kevin F. Steinmetz. 2014. Watching the Watchers and McLuhan's Tetrad: The Limits of Cop-Watching in the Internet Age. *Surveillance & Society* 12 (4): 502–515.

Schneier, Bruce. 1996. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. Second edition. New York: John Wiley & Sons.

Shane, Scott, Matthew Rosenberg, and Andrew W. Lehren. 2017. WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents. *New York Times*, March 7. https://archive.fo/nY9Hs [accessed February 10, 2022].

Shilton, Kate. 2010. Participatory Sensing: Building Empowering Surveillance. *Surveillance & Society* 8 (2): 131–150.

Singh, Ajay. 2017. Prolepticon: Anticipatory Citizen Surveillance of the Police. *Surveillance & Society* 15 (5): 676–688.

Sloan, Robert H., and Richard Warner. 2015. The Harm in Merely Knowing: Privacy, Complicity, Surveillance, and the Self. *Journal of Internet Law* 19 (1): 3–14.

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.

van der Vlist, Fernando N. 2017. Counter-Mapping Surveillance: A Critical Cartography of Mass Surveillance Technology After Snowden. *Surveillance & Society* 15 (1): 137–157.

van Dijck, José. 2014. Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology. *Surveillance & Society* 12 (2): 197–208.

Verde Garrido, Miguelángel. 2015. Contesting a Biopolitics of Information and Communications: The Importance of Truth and Sousveillance after Snowden. *Surveillance & Society* 13 (2): 153–167.

Villena Saldaña, David. 2011. Julian Assange: periodismo, científico, conspiración y ética hacker. *Quehacer* 181: 58–69.

Westin, Alan. F. 1967. *Privacy and Freedom*. New York: Atheneum.

Wilkins, Lee, and Coleman, Renita. 2004. *The Moral Media: How Journalists Reason About Ethics*. Mahwah, NJ: Lawrence Erlbaum Associates.

Zaia, Matthew. 2019. Exploring Consciousness: The Online Community's Understanding of Mobile Technology Surveillance. *Surveillance & Society* 17 (3/4): 533–549.

Zetter, Kim, and Kevin Paulson. 2010. U.S. Intelligence Analyst Arrested in WikiLeaks Video Probe. *Wired*, June 6. https://archive.fo/gsvu5 [accessed February 10, 2022].

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.