From Internet Farming to Weapons of the Geek

by Gabriella Coleman

Hackers and their projects have become routine, authoritative, and public participants in our daily geopolitical goings-on. There are no obvious, much less given, explanations as to why a socially and economically privileged group of actors, once primarily defined by obscure tinkering and technical exploration, is now so willing to engage in popular media advocacy, traditional policy- and law-making, political tool building, and especially forms of direct action and civil disobedience so risky that scores of hackers are currently in jail or exile for their willingness to expose wrongdoing. Why and how have hackers managed to preserve pockets of autonomy? What historical, cultural, and sociological conditions have facilitated their passage into the political arena, especially in such large numbers? Why do a smaller but still notable fraction risk their privilege with acts of civil disobedience? These are questions that beg for nuanced answers—beyond the blind celebration or denigration offered by popular characterizations of hacker politics. In this article I will provide an introductory inventory—a basic outline of the sociocultural attributes and corollary historical conditions—responsible for the intensification of hacker politics during the last 5 years.

In January 2015, after delivering a talk about the protest ensemble Anonymous, I went out to lunch with PW—a 40-something Dutch hacker now living in Canada whom I first met in 2002 while conducting research in Amsterdam. Given his expertise in cryptography, the conversation naturally drifted to the subject of Edward Snowden—a former government contractor who exposed the NSA's secret surveillance programs. PW, long involved in the battle for privacy, benefited from the following situation: many hackers experienced Snowden's act of whistle-blowing as a wake-up call. Scores of technologists were spurred to pursue a privacy agenda through the communal development of encryption tools.

Over lunch I asked him what he thought about the contemporary state of hacker politics. PW—intensely involved in the hacker scene for his whole adult life—did not skip a beat in tendering the following analysis: the political effects of hackers would emerge diffusely over an extended period of time, products—just as the Internet itself is—of the types of technologies they work to build. To punctuate this point, he described hackers as "Internet farmers." Just as the rise of agriculturalists massively altered human material relations to food supplies, so too would hackers and their technologists' allies alter the course of human history through their technological artifacts. The effect of particular hacker individuals or organizations would be largely irrelevant—microgestures within broader, deterministic forces driven by technological development itself.

But this explanation was just for context. He continued by expressing surprise at the current state of affairs whereby both individual hackers and hacker organizations—many of which were intimately familiar to him—increasingly assume prominent geopolitical roles in sculpting our immediate history. As he offered his commentary, I nodded in agreement: by this point I had been researching the politics of hacking for many years, and while strong pockets of activism or political tool building have long existed (Jordan 2008; Jordan and Taylor 2004), these were but small corners of activity in a vast territory.

Today the landscape has dramatically changed, and in a very short period of time. In the past 5 years, hackers have significantly enlarged the scope of political projects, demonstrating nuanced and diverse ideological commitments that cannot be reduced to the libertarianism so often presupposed as the essence of a hacker ideology (Golumbia 2013). In particular, direct action or civil disobedience have surged in a variety of formats and styles, often related to freezing websites through distributed denial of service campaigns (Sauter 2014) or to whistle-blowing. We see lone leakers, such as Chelsea Manning, and also leftist collectivist leaking endeavors, such as Xnet in Spain. Other political engagements are threaded through software: for instance, protocols (such as BitTorrent) and technical file-sharing platforms (such as the Pirate Bay) enable the sharing of cultural goods (Beyer 2014; McKelvey 2014). Hackers conceptualize these platforms distinctly to suit a range of ideological agendas: from anarchist to socialist, from liberal to libertarian. Since the 1980s, free software hackers have embedded software with legal stipulations that have powerfully tilted the politics of intellectual property law in favor of access

Gabriella Coleman is Associate Professor in the Department of Art History and Communication Studies at McGill University (853 Sherbrooke Street West, Montreal, Quebec H3A 0G5, Canada [gabriella.coleman@mcgill.ca]). This paper was submitted 24 VIII 15, accepted 27 VII 16, and electronically published 22 XI 16.

0011-3204/2017/58S15-0009$10.00. DOI: 10.1086/688697

(Coleman 2013; Kelty 2008) and have inspired others—notably scientists, academics, and lawyers—to embolden arguments for access (Delfanti 2013). Across Europe, Latin America, and the United States, anticapitalist hackers run collectives—many doubling as anarchist associations—providing privacy-enhancing technical support and services for leftist crusaders aiming for systemic social transformations (Wolfson 2014). Anonymous has established itself as one of the most populist manifestations of contemporary geek politics; while no technical skills are required to contribute, the entity has used the attention gained by high-risk hacking trysts to deliver its most powerful messages (Coleman 2015).

Plainly, hackers can no longer be viewed as exotic experts: they have become authoritative and public participants in our daily geopolitical goings-on. There are no obvious, much less given, explanations as to why a privileged group of actors, once primarily defined by obscure tinkering and technical exploration, is now so willing to engage in popular media advocacy, traditional policy- and law-making, political tool building, and especially forms of direct action and civil disobedience so risky that scores of hackers are currently in jail or exile for their willingness to expose wrongdoing.

Working technologists are economically rewarded in step with doctors, lawyers, and academics—and yet these professions seem to produce far fewer politically active practitioners. Why and how have hackers, who enjoy a significant degree of social and economic privilege, managed to preserve pockets of autonomy? What historical, cultural, and sociological conditions have facilitated their passage into the political arena, especially in such large numbers? Why do a smaller but still notable fraction risk their privilege with daring acts of civil disobedience? These are questions that beg for nuanced answers—beyond the blind celebration or denigration offered by popular characterizations of hacker politics.

This article will provide an introductory inventory—a narrative sketch of the sociocultural attributes and historical conditions responsible for the intensification of hacker politics during the last 5 years. Probably the most important factor is a shared commitment to preserving autonomous ways of thinking, being, and interacting. Let us see how they are secured.

The Craft and Craftiness of Hacking

Computers can be a daily source of frustration for user and technologist alike. Whether a catastrophic hard drive crash—which, without a backup, can feel like a chunk of one's life has been yanked away by dark, mysterious forces—or a far more mundane search engine freeze—after having foolishly opened an eighty-fifth web page—rarely does a week or even a day go by without offering a computer malfunction. I found myself in this situation one day in October 2015. At the tail end of a long day, I was replying to a slab of e-mails. Distracted, I foolishly opened that eighty-fifth web page. My computer, which runs a version of the Linux operating system, first froze, then went dark, and finally rebooted itself. Livid, I was fairly certain hours of work were about to be nuked into oblivion (I was right). Then this happened.

```
Oct 8 23:48:02 kernel: [27653668.999445] Out of memory:
Kill process 12731 (redacted) score 318 or sacrifice child
```

"Sacrifice child?" I laughed and snapped a picture. Some developer had implanted this humorous message in an otherwise dry (and for the technically illiterate, likely incomprehensible) system log error message.[1] I was reminded that behind every piece of software is an auteur with a distinctive style. Though already familiar with hacker humor—having dedicated a book chapter to the subject (Coleman 2013)—my foul mood was replaced with elation: this was the first time I encountered a joke embedded in technology without hunting for one.

This sort of joke directs us to some unique features common to hackers, at least when compared with other technologists—system administrators, programmers, cryptographers, security researchers—who, like hackers, perform the same sort of labor. Like hackers, all these technologists are quintessential craftspeople driven by the pursuit of quality and excellence (Sennett 2009). The hacker adds something more into the mix: a fastidious and explicit impulse for craftiness. To improve and secure computer technologies, hackers approach solutions not only with technical know-how and ability but also with some degree of agility, guile, and even disrespect. To quote an effective description offered by a security hacker during an interview, "You have to, like, have an innate understanding that technology is arbitrary, it's an arbitrary mechanism that does something that's unnatural and therefore can be circumvented, in all likelihood."

This oscillation between craft and craftiness, of respect for tradition and its wanton disregard, is in itself not exclusive to hackers or technologists. It is common among a range of laborers guided by a crafting sensibility: from engineers to professors, from journalists to carpenters (Orr 1996). Indeed, academics depend on and reproduce convention by referencing the work of peers, but they also strive to advance novel and counterintuitive arguments and gain individual recognition in the doing. What is unique to hackers is how an outward display of craftiness has surpassed mere instrumentality to take on its own, robust life; craftiness and its associated attributes, such as wit and guile, are revered as much for their form as for their function. In contrast, for most craftspeople, craftiness is a means to

[1] The suggestion to sacrifice a child may seem like a random and especially mean-spirited message to send, one designed to shock the clueless user. To those familiar with Unix-based operating systems, however, this statement is technically accurate. In extreme memory-constrained scenarios, the Linux Kernel out of Memory Management (OOM) routine that makes an algorithmic determination to stop a process (by sending a "kill" signal) was done in this case to a subprocess (known as a "child process"). Choosing what process to sacrifice is a bit of a dark art and causes processes to "die," potentially losing work, as a trade-off for regaining access to the system again.

an end—one tool, often exercised tacitly, among others (Collins 2010; Polyani 1967). For hackers, the performance of craftiness has long attained the status of an explicit pursuit, a thing valued in and of itself.

The most evident trace of the hacker quest for and adoration of craftiness is the sheer abundance of humor among them. No ethnography would be complete without considering it—a conclusion I arrived at when, sitting at a hacker conference, it dawned on me that it was acceptable, even welcome, for an audience member to interrupt a speaker in order to crack a joke (perhaps the only other group willing to spontaneously defy social decorum in similar ways are comedians or drunk people). Once tuned in to the frequency of hacker humor, it became clear that hackers inject humor into every social situation and artifact: there is a long tradition of inserting small snippets of wit into code and documentation; and they even embed hidden puzzles (what they call Easter eggs) in code for the amusement of those scrutinizing their work. Sometimes, technical cleverness regiments an entire technical artifact, such as the esoteric and irreverently named programming language BrainFuck. Hackers also have a long history of mischief making and pranking; according to many, the term "hacks" was first coined to describe a type of practical joke (Peterson 2011). Crafty humor is evident in some of the hacker political battles addressed later in this essay. (For detailed analysis of the pervasiveness of cleverness and humor in hacker circles, see Coleman 2013; Goriunova 2014; Montfort 2008). Valorizing this craftiness even for noninstrumental uses, hackers invite levity and play into their activities. Perhaps even more importantly, they also hone a crafty mindset for even nontechnical pursuits, keeping it sharp and ready at hand for when a truly stunning hack is needed.

The Autonomous Mind-Set

> *Easiest way to get a hacker to do something: tell them they can't.* (Institutionalized Oppositional Defiance Disorder [a hacker])

Craftiness depends on a vigilant criticality, a willingness to scrutinize, always with a mind on identifying inconsistencies or upending convention. Perhaps unsurprisingly, another characteristic that might be identified as common to hackers is a dogged antiauthoritarianism, which manifests itself as a profound skepticism toward institutions and other forms of entrenched power. While it might be tempting to see this as merely another journalistic cliché, this attitude is genuinely encoded deep in the hacker cultural DNA. It is as apparent in their flippant, casual conversation as it is in their manifestos, zines, and text files.

Emblematic of this ethos is the iconic "The Conscience of a Hacker," authored by a figure known as the "The Mentor" and collectively redubbed "A Hacker Manifesto." Published in 1986, it ends with a defiant confession: "Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for" (The Mentor 1986). While one might imagine a statement such as this as the hyperbolic expression of an angst-ridden, middle-class alienation, the truth is that whatever his economic background, The Mentor wrote it at a particular juncture of his life: "The following was written shortly after my arrest."

The Mentor's biography is uncommon: most hackers never face arrest. But the fact remains that many aspects of hacking, past and present, are littered with examples of disobeyed norms, rules, and sometimes laws. These repeated subversive acts not only support antiauthoritarian attitudes directly but also, as "The Hacker Manifesto" attests, do so through its memorialization in the copious archives of hacker literary and political writings. Indeed, illicit subversion must be understood as an originary condition of hacking itself. When phreaking (originally called freaking) and hacking established their cultural and technical legs in the late 1950s and early 1960s, rule breaking was often essential to gaining access to any equipment. For phone freaks, rule breaking was simply unavoidable. Their entire raison d'être was the exploration of phone systems and to link up with other phone enthusiasts in the doing; even if profit or malice were rarely part of their calculus, they nevertheless violated state and federal laws every time they phreaked. The first freak arrests occurred in 1961 (Lapsley 2013:59), although it would be another few decades before their hacker cousins felt the full brunt of the law.

When compared with the freaks, university-based hackers rarely broke the law. But even among the small cadre of hacker-students enrolled in universities—such as Carnegie Mellon; the University of California, Los Angeles; Stanford; and MIT—rules were frequently twisted—usually to land more time on their beloved computer. In his account of the first-generation MIT hackers, journalist Steven Levy characterizes the hacker proclivity to bend rules:

> To a hacker, a closed door is an insult, and a locked door is an outrage. Just as information should be clearly and elegantly transported within a computer, and just as software should be freely disseminated, hackers believed people should be allowed access to files or tools which might promote the hacker quest to find out and improve the way the world works. (Levy 2010 [1984]:86)

These hackers were partially shielded from punishment because they were, after all, affiliated as students. But a handful of preteen and teenage computer enthusiasts, too young to attend university, also joined the informal club of technologists—at times by sneaking illegally into the facilities at night, a practice which earned them the fitting title of "computer rats."

Collectivism and the Autonomous Spaces of Hacking

Despite differences in degree and typology of insubordination—in some instances, hackers disobey convention while in other cases, they relish breaking laws—antiauthoritarianism is evident across varied hacking lineages. While craftiness emerges through technical practice and rule bending or law breaking reinforce antiauthoritarianism, both mind-sets now constitute the rhetorical repertoires that hackers use to describe themselves.

Together, craftiness and antiauthoritarianism might be understood to cultivate an attitude that is profoundly individualistic or even antisocial. No doubt it is from isolating and extrapolating these characteristics that the myth of sweeping hacker libertarianism emerges. But the relationship between hackers and individualism is more complex than these two characteristics might suggest. As any sustained observation of hackers is quick to reveal, hacking is, in most instances, a hypersocialized activity. Cooperation, fellowship, mutual aid, and even institution building are quotidian to the hacker experience—even among the most subversive, rule-breaking practitioners.

Even if craftspeople tend to work in solitude—and hackers most definitely do, and as the stereotype goes, heavily caffeinated and late into the night—many aspects of crafting are collectivist. Skilled workers gather in social spaces, such as conferences or workshops, to learn, mentor, and establish (everchanging) guidelines of quality (Sennett 2009). Hacking is no exception to these dynamics. Whether acknowledged or not by hackers themselves, all types of hacking embody profound forms of social entanglement and feelings of communion. These elements are established by a mutual adoration of technical pursuits and the pragmatic need to secure the help of others; crucially, the collective development of technology is bolstered by social spaces, and hackers have long had and continue to build and inhabit many of these—mailing lists and image boards, code repositories, free software projects, hacker and maker spaces, Internet chat relays, and developer and hacker conferences.

These are sites where hackers gather, deliberate, and work semiautonomously from the mandates and demands of their day jobs. They qualify as what scholars of social movements designate "free spaces." Usefully defined by one sociologist as "settings within a community or movement that are removed from the direct control of dominant groups, are voluntarily participated in, and generate the cultural challenge that precedes or accompanies political mobilization" (Polletta 1999:1), scholars of such spaces have tended to examine locales such as independent book shops, women-only gatherings, bars, block clubs, tenant associations, and union halls.

Free spaces are "free" not because they are open to everyone. While some are inviting to all (e.g., a book shop or a public chat channel), others spaces are regulated—some loosely, others tightly—to control access and membership (a union hall or free software project). They are free for being infused with logics of independence: participants run these spaces collectively and autonomously, outside the penumbra of the direct control or even influence of dominant institutions or values whether they be economic, political, cultural, or some combination of the three. Indeed, a couple of the core technologies that constitute hacker free spaces, such as Internet Relay Chat and mailing lists (and BBSes in earlier eras), are not only easy for hackers to set up but are noncommercial zones on an Internet almost dominated today by private interests.[2]

Hackers cobble together the communication technologies that double as hacker free spaces in distinct ways: some spaces, like those that facilitate free software projects, are structured and transparently documented institutions, while others, like those that serve Anonymous, function as opaque, elastic, and far-flung networks. Juxtaposing these two examples makes it clear that hacker spaces—and thus hacker sociality—are by no means monolithic. And yet both examples also function to dispel the myth that hackers are individualist, or against institutions.

While there are dozens to choose from, one of the most notable examples of a structured hacker organization is the Debian Project. Founded in 1993, it boasts a thousand members who maintain the 25,000 pieces of software that together constitute a Linux-based operating system. Some of the technical engineers within Debian double as political architects, and they have established the project as a federation, which functions something like a guild or workers' cooperative. They have outlined intricate voting procedures for the purposes of governance and have articulated commitments and stipulations ratified in a series of legal and ethical charters and manifestos. Before enrollment, all prospective members are tested on their knowledge of the project's technical policies, legal commitments, and ethical norms (Coleman 2013; O'Neil 2009).

If Debian is configured as a sort of miniature society—and given its social constitution and manifesto, having a very nineteenth-century, Enlightenment feel to it—Anonymous, by contrast, is more opaque, but expansive, functioning more informally as a "scene" (Straw 2014). While increasingly recognizable as advocates for social justice and stewards of direct action, they refuse to establish an ideological common denominator much less universally applicable ethical statements of the sort Debian has ratified. Spread across the globe and inhabiting a range of technologies—Twitter accounts and a multitude of chat rooms, some public and some private—Anonymous is a dynamic, moving target. Many Anonymous-based nodes and collectives, whether small teams, larger networks, or simply groups of loosely connected Twitter accounts, form, disband, and regroup in new ways in the course of weeks or months. Others have existed in relatively stable shape now for 5 years. Still, most operations can be understood as some-

[2] There are some important differences between most hacker and nonhacker free spaces. Compared with traditional free-space venues, whose costs of renting or ownership are significant—downright exorbitant if they are located in cities such as New York, London, Paris, Vancouver, or Sydney—online-based hacker free spaces can be maintained at a comparatively modest cost, usually boiling down to fees for Internet access and labor to maintain systems. A longer account would have to address the material qualities of software because they help ensure the sheer abundance of free spaces among hackers.

how well organized, but given its dynamic geography, Anonymous eschews stabilization. Combine these characteristics with the fact that some hackers rely on partial secrecy, and Anonymous is distinctive (and refreshing) for how it resists extensive sociological mapping and thus categorization.

Where Debian proceeds from a set of rules, Anonymous is like an antialgorithm: hard to predict and difficult to control. They appear more akin to a cipher than a solution. Yet at both these poles and everywhere in between, these participants are social to the extreme. Anonymous members communicate consistently (even if they do not know exactly who is on the other end—and Debian developers do, too) with individuals carefully vetted by the project (to officially join the virtual project, a prospective developer must first get their cryptographic identity verified by another developer, in person).

State Intervention as a Political Catalyst

So far we have considered three crucial components of hacker subjectivity that help us grasp their political subjectivity: the valorization of craftiness, the cultural cultivation of antiauthoritarianism, and the sustenance of fellowship around labor in free spaces. These features do not in themselves account for the hacker tendency toward political action. But by helping to reinforce and reproduce independent habits of thinking, skills suited to maintaining and governing technologies that enable both autonomous congregation and action and communities of mutual support, they form vital pillars capable of propping up the forms of political action that flourish in the community today.

Yet while these components set the stage for action, the thing still missing is a script—and a problem to set the action in motion. While hacker politics today are increasingly oriented in response to the problems of outsiders, the original catalyst that unites hackers in political action tends to emerge when the community itself is threatened (Coleman 2016). Thus, the major, and perhaps unsurprising, trigger of hacker politicization has come about as a response to aggressive state and corporate hostility toward hackers and their technologies. In this sense, the hacker public is also an apt example of what Michael Warner (2002) identifies as a counterpublic—one that "maintain[s] at some level, conscious or not, an awareness of its subordinate status" (56). Here we can understand "subordinate" to mean simply that hackers, their activities, and their artifacts have frequently had their existence challenged by state forces more powerful than themselves. But more to the point, hackers have been quick to sound a high-pitched awareness of this subordinate status whenever the state or the market comes barreling down on them. Their response, typically, has been to fight back. In the short history of hackerdom, such challenges have appeared with a remarkable frequency. Below I will highlight a tiny fraction of such events.

By the 1980s phreaking was largely replaced by the avid exploration of computer networks, instantiating what is commonly referred to as the hacker underground. With the availability of cheaper modems and personal computers, those willing to engage in the risky sport of computer trespass swelled, as did the technical watering holes—the free spaces of the era—that these nascent hackers built to congregate, swap information, and store contraband. Chief among these were Bulletin Board Systems (BBSes), text-based computer hubs reachable via a modem and phone. As the hacker underground grew more tentacles, its members ran increasingly afoul of the law (Dreyfus 1997; Sterling 1992). Crucially, arrests and subsequent prosecutions were enabled by new statutes with stiff penalties directed specifically at computer users and passed in the United States (Computer Fraud and Abuse Act in 1986),[3] Australia (Crimes Legislation Amendment Act in 1989), and the United Kingdom (Computer Misuse Act in 1990).[4]

Throughout the 1990s, law enforcement coordinated multistate raids that targeted swaths of hackers and sought to shut down the BBSes. Hackers were slapped with trumped up charges and fines that rarely matched the nature of the crime. Bruce Sterling (1992), who chronicled the 1990s American clampdown, described it in no uncertain terms as "a crackdown, a deliberate attempt to nail the core of the operation, to send a dire and potent message that would settle the hash of the digital underground for good" (104).

The most infamous of the 1990s US-based arrests concerned the case of Craig Neidorf. Known in hacker circles by the handle Knight Lightning, Neidorf was a cofounder of the popular e-zine *Phrack* (featuring hyperbolic and relentlessly antiauthoritarian material, a healthy portion of which was expressly devoted to parodying the FBI). While Neidorf originally faced 31 years in jail for circulating an AT&T technical memorandum about the nation's 911 emergency phone call system, it was later revealed that the document was available at the library for any member of the public to access. Ultimately charges were dropped—but only after a costly legal battle. So astounding was his plight that it helped spur the founding of what is now the largest nonprofit for defending civil liberties in the digital realm, the Electronic Frontier Foundation.

Many subsequent cases were as troubling for how state prosecution against hackers resembled persecution (Thomas 2003). In the early 2000s hacker and phreak Kevin Mitnick engaged in multiple, indisputable crimes of computer trespass—online explorations that did not benefit him financially or cause any permanent damage. Nevertheless, because he was a "hacker," the Department of Justice jailed him for 4 years in pretrial confinement followed by 8 months in solitary confinement. Such harsh treatment was deemed necessary because law enforcement officials convinced the judge that Mitnick could "start a nuclear war by whistling into a pay phone."[5]

While a great majority of the 1990s and 2000s cases involved computer intrusion, these hackers rarely sought to profit from

[3] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213, codified as amended at 18 U.S.C. §103 (1986).

[4] Computer Misuse Act, 1990, c.18. Crimes Legislation Amendment Act, 1989, No. 108.

[5] Cited in Mills (2008).

their illicit jaunts into computer networks much less damage any equipment or data. Typically, their most substantial crime was hoarding technical data or defrauding the phone companies to make the free calls needed to explore more networks. As a dozen high-profile cases plodded through the court system, journalists wrote or spoke about "mad hackers" and "real electronic Hannibal Lecters."[6] Branded by the courts and the media as outlaws, the antiauthoritarianism harbored by hackers only intensified and became marshaled in campaigns like the "Free Kevin" movement, which devoted itself to exposing the plights of incarcerated hackers.

Only a narrow band of hackers are willing to break the law for the thrill of exploratory joy riding (and then, the ability to boast about the journey to their peers). Most hackers are law-abiding citizens, some with little sympathy for the legal woes of their security-breaching colleagues. But when the conditions needed to write or distribute software are jeopardized—or software is itself targeted for censure or criminalization—they can be spurred to action, even direct action.

Take the case of Pretty Good Privacy, a piece of public encryption technology designed to enhance the privacy of regular citizens. Principally authored by cryptographer Phil Zimmerman, its international release in 1991 constituted a daring act of civil disobedience, breaking international munition and patent laws predicated on the military uses of encryption (Greenberg 2012; Levy 2001, 2010 [1984]). The 1993 FBI criminal investigation of Zimmerman for possible "munitions export without a license" triggered developments in both the then nascent idea that software deserves free speech protections and also the more general idea that publishing software could constitute an act of revolt. Discussed widely on multiple online forums, hackers registered their support for public encryption by crossing international borders wearing T-shirts printed with legally protected encryption source code. As he was pursued by US law enforcement, a crafty solution was devised to dramatically increase his chances for successfully challenging the export control laws he had broken: along with publishing the source code online, MIT Press was persuaded to publish the software blueprints as a book, thus ensuring that the international sale of the printed code would be protected under the First Amendment. Eventually, the FBI mysteriously dropped all charges and has to this day declined any explanation for the sudden change of heart.

A similar pattern of aggressive state intervention occurred between 1999 and 2001 with the release and attempted suppression of DeCSS, a short program designed to bypass access protection on commercial DVDs, enabling them to be played on Linux operating systems or outside of their specified region. This time, the hacker-based protests were more widespread. Following the arrest of Norwegian teenager Jon Johansen for his involvement in its development, some hackers in the United States who shared or published the code were sued under the Digital Millennium Copyright Act—a copyright statute passed in 1998 forbidding the cracking of digital rights management. This criminalization led to a then unprecedented surge of protest activity among hackers, particularly free software developers, across both Europe and North America. In addition to street demonstrations, many began to share the code as a knowing provocation, a form of civil disobedience: they republished DeCSS online, rewrote the original program in different computer languages, and printed the DeCSS code on T-shirts. Some enacted even craftier forms of protest. One hacker, Seth Schoen (2001), rewrote the program mathematically as a haiku, or, to be more exact, as 465 individual haiku strung together into one epic poem. Meant for the judges overseeing the legal cases, Schoen passionately defended what he dually described as "controversial math" and poetry. His text implores,

> Reader, see how yet
> technical communicants
> deserve free speech rights;
>
> see how numbers, rules,
> patterns, languages you don't
> yourself speak yet,
>
> still should in law be
> protected from suppression,
> called valuable speech!

Although this poem was authored individually, it joined a more collective insistence that free speech rights pertain also to acts of writing, releasing, and sharing code (Coleman 2013).

Still, while the DeCSS legal imbroglio and its activist outcomes became known to most every geek, hacker, civil liberties lawyer, and radical librarian at the time of its unfolding, constituting what is now popularly known as the "digital rights movement" (Postigo 2012), it received scant coverage in the mainstream media, and its implications never really found purchase in the broader public consciousness. That type of colossal media coverage would only emerge a decade or so later, as names and figures such as WikiLeaks, Chelsea Manning, Julian Assange, Anonymous, Aaron Swartz, and Edward Snowden came to the fore. Alternatively supported by their hacker brethren and despised by many in power, these figures nonetheless became household names across the Western world.

WikiLeaks's release of the "Collateral Murder" war video in April of 2010, followed by a large slab of diplomatic cables, set the course of hacker politics in a new direction, catapulting figures such as Chelsea Manning—who was revealed to have leaked the content to WikiLeaks—to global prominence. Beginning in 2011, Anonymous's wily media-spectacular actions made it clear that this sudden gush of direct action and political activity would continue to flow for years.

Yet just like the previous generation of hackers, these figures were not spared the attention of authorities. Chelsea Manning was sentenced to 35 years of US military imprisonment; Aaron

[6] "Geraldo Rivera Browbeats Craig Neidorf," RDFRN, http://www.rdfrn.com/totse/en/hack/legalities_of_hacking/geraldo.html (accessed June 23, 2015).

Swartz took his own life after he found himself threatened with a ludicrous 35-year prison sentence for downloading academic articles; and scores of Anonymous activists, such as Jeremy Hammond, faced arrest and imprisonment for a range of hacking charges. Indeed, sometimes the powers brought to bear on them were of an unprecedented calibre, marshaling geographically extensive state forces, as in the cases of WikiLeaks and Edward Snowden. Both Julian Assange and Edward Snowden currently sit in an exiled legal limbo, in Ecuador's London embassy and in Russia, respectively, because of the coordinated efforts of multiple Western states to prosecute them.

Yet in one regard the response today has been markedly different. Rather than ignoring or demonizing the legal plights of these hackers, media outlets have instead publicized these cases widely and sometimes sympathetically (Thorsen, Sreedharan, and Allan 2013). Meanwhile, producers of popular cultural media now routinely portray these hackers as laudable heroes or antiheroes. Television shows such as *Mr. Robot*, *House of Cards*, *The Good Wife*, and *Homeland* feature prominent and powerful hacker characters. Films such as *Who Am I* offer similar treatments. And documentary films sympathetic to these figures, such as Laura Poitras's Academy Award–winning *Citizenfour*, are now capable of earning the West's highest cultural honours. This dual push of cultural celebration and authoritarian crackdown seems only, thus far, to have swelled the ranks of hacker activists, maintaining the state antagonism that prompts reaction while elsewhere popularly celebrating those who react.

Ever since, the most overt protests or fights engaged by hackers—such as WikiLeaks's aggressive quest for radical press freedom or Anonymous's contributions to all the major social revolutions transpiring in 2011—have drawn in hosts of sympathetic allies and bedfellows, extending the reach of their original interventions into increasingly diverse domains. Spurred on by these exceptional events, many hackers previously wary of political involvement—and many of their less technical but no less geeky cousins, too—are involved in full-blown activist and political organizing.

The Liberal and Radical Politics of Hacking

Now that we have identified the circumstances that prompt some hackers to take a political stand, it is worth considering the tone and tenor of this political engagement itself. When hackers do act, what is it they are fighting for? And how does it link with broader political trends and traditions? If hackers are not the libertarians they are so often painted as, what are they? Social anarchists? Rebels without a cause? Reformist liberals? There is no single answer to this question, but an examination of the way hackers engage with the law might at least give us some hints. And here, too, we find more nuance than a blanket antiauthoritarianism might suggest. After all, code functions, in many ways, as a law unto itself.

Hackers do not only hold an exhaustively antagonistic relationship to the law but also at times a scholarly, even cooperative one. As I have argued elsewhere, a homologous relationship exists between the craft of writing code and intuiting legal texts: the modes of reasoning required to write code are similar to those needed for parsing a formal, rule-based system such as the law (Coleman 2013). While many hackers hold nothing but contempt for the unjust laws and prosecutorial abuses of which they are often the target, they nevertheless display enormous interest in and facility with legal principles and statutes.

Hackers have been known to use this dexterity with the law in the service of social change both by diagnosing, avoiding, and arguing against laws they deem bad and, as in the case of free software, by detouring existing laws to assure their productive freedom. But the faculty can be seen as more broadly useful still. While the following excerpt by historian E. P. Thompson describes the saturation of the law in eighteenth-century English society, it could equally be applied to the more general state of the Western world today.

> I found that law did not keep politely to a "level" but was at every bloody level; it was imbricated within the mode of production and productive relations themselves . . . and it was simultaneously present in the philosophy of Locke; it intruded brusquely within alien categories, reappearing bewigged and gowned in the guise of ideology; . . . it was an arena of politics and politics was one of its arms; it was an academic discipline, subjected to the rigour of its own autonomous logic; it contributed to the definition of self-identity both of rulers and of ruled; above all, it afforded an arena for class struggle, within which alternative notions of law were fought out. (Thompson 1978:96)

For hackers, the law is more than a friend or a foe: it is their reality. And this tight relation between hacking and the law has afforded an arena for many instances of struggle and avoidance, even if not always class related. Hackers both fight for alternative notions of the law and insist on the realization of cherished legal principles that they believe have been corrupted. One class of legal precepts in particular, those of civil liberties—privacy and free speech—have settled so deeply into the cultural and technical sinews of hacking that much of their advocacy is almost inseparable from the idea of the hacker itself.

We can see this civil liberties acculturation at work in Edward Snowden's justification for releasing NSA documents detailing the pervasive citizen surveillance deployed by the American and British governments. Hiding out in a Hong Kong hotel room, in an interview with journalist Glenn Greenwald he explained,

> I remember what the Internet was like before it was being watched. . . . You could have children from one part of the world having an equal discussion . . . where they were sort of granted the same respect for their idea in conversation with experts in a field from another part of the world on any topic. . . . It was free and unrestrained. And we've seen the chilling of that and the cooling and the changing of that

> model toward something in which people self-police their views. . . . It has become an expectation they are being watched. It limits the boundaries of their intellectual exploration. And I am more than willing to *risk imprisonment* than the curtailment of my intellectual freedom.[7]

For Snowden, the Internet ought to be a medium to actualize unhampered exchange of ideas and free thinking. For those of a similar mind to Snowden, a concern for civil liberties is not separate or supplemental to an engagement with these technologies: it is constitutive of the experience itself. Snowden may be exceptional, insofar as he took on enormous risk to expose the current depth of surveillance, but his vision of the Internet as a "a moral order," as Chris Kelty (2008) puts it, is one shared by countless geeks. The hacker commitment to civil liberties demonstrates a commitment to their own existence as an entity—what Kelty (2008) defines as a recursive public, which includes the necessary liberties to pursue self-defined cultural and technical activity.

Given the hacker interest in civil liberties, many of contemporary hacker-led political endeavors also align with and even directly bolster liberal or libertarian aspirations. There are many such examples, including the chartering of Pirate Parties, designed to partake in liberal democratic politics (Beyer 2014; Burkart 2014) or the watchdog functions of associations such as the German-based Chaos Computer Club, who routinely work with journalists in various capacities (Kubitschko 2015). The exemplary case of such a liberal agenda is civic hacking, which aims to develop tools that can solve problems inherent to the current Western political order. While this sometimes means enhancing local services, it also involves attempts to increase government transparency and accountability by making data and processes more readily available (Schrock 2016).

Other hackers rely on civil liberties to incubate a more radical disposition, working to carve out pockets of autonomy or alterity (Söderberg 2007; Wark 2004). Adherents of free software, for instance, are able to build software in commercial or noncommercial settings without ever losing control of the material they produce. Anonymous, in discouraging and criticizing fame seeking and social peacocking, enacts a critical practice of egalitarianism and solidarity (Coleman 2015), maintaining a critical space in popular social media platforms for those whose ethics deviate sharply from the logic of individualized branding (Marwick and boyd 2011).

Elsewhere hacker politics take more resistive forms that are outright contrary or antagonistic to liberalism and capitalism. There are many such examples of self-avowed anarchist, socialist, and Marxist hackers who build tools and support systems for more radical forms of autonomy and sometimes advance revolutionary projects aimed at systemic change (see Juris 2008; Milan 2013; Wolfson 2014). One of the most muscular of these endeavors is Indymedia, a robust alternative media initiative that has inspired countless copycats in its wake. Conceived by hackers involved in planning the large-scale demonstrations during the 1999 World Trade Organization convention in Seattle, these hacker-organizers anticipated that the mainstream media would hijack the representations of protest activity through tactics of simplification or distortion. They opted to develop an entirely alternative media system rooted in a novel content management system that allowed them to embed videos and photos into their online reports years before pundits (incorrectly) celebrated web 2.0 companies for inventing such functionality. With these tools it was hoped that protest organizers and rabble-rousers could bypass the media to become the media.

At the height of its operations, the Indymedia technical team, spread across the globe, maintained over a couple hundred journalism centers. These material forces helped propel the broader social justice movement outward across space and forward in time. And in so doing, a tight-knit network of revolutionary hackers was constituted—one that has continued to exist into the present, long after the counterglobalization movement was itself relegated to the annals of protest history.

This hacker-cohort has since erected an alternative technical backbone to the commercial Internet, one built on a principled refusal to monitor its users in the manner now normal for Internet corporations offering supposedly free services (Milberry 2014). This infrastructure relies on a sizable roster of independently run Internet service providers, many of which are organized around consensus-based, anarchist principles. Around 28 exist across the world, and their names bear the imprint of radical sensibilities: cybrigade, squat.net, systemausfall.org, flag.blackened.net, hackbloc.org, mutualaid.org, riseup.net, resist.ca, entodaspartes.org, MayFirst, and so on. The largest of this cluster is the US-based Riseup. Chartered by some of the same hackers who founded Indymedia, the collective provides secure e-mail and mailing list services to a user base that is made up of both technologists and leftist organizations whose political agenda is often not anchored in technology itself. Riseup members state that technology is not an end in itself but rather an "aid in the creation of a free society, a world with freedom from want and freedom of expression, a world without oppression or hierarchy, where power is shared equally."[8]

These engagements show that the ideological sensibilities that animate hacker politics are diverse: just as we can locate liberal hackers and projects, so too can we identify radical hackers and projects and see how both engender social change. While a commitment to civil liberties can be seen as something of a universal among politically minded hackers, the reasons for this commitment can vary. While liberals treat civil liberties as the essential condition of individual rights and mainstream political participation (or access, or voice), radical hackers see civil liberties such as free speech and privacy as the gateway

[7] Excerpt from the documentary *Citizenfour*, directed by Laura Poitras (2014, Toronto: Praxis), emphasis added.

[8] "About us," Riseup.net, https://help.riseup.net/about-us.

to more substantive projects that aim to enable equality and justice.[9] And as one might expect, wherever the socialist and anarchist left is more represented in society—such as in Spain, Italy, Greece, Croatia, and Argentina—so too are leftist hacker projects more present and robust (Bazzichelli 2013; Corsin Jimenez and Estalella 2016; Maxigas 2012). Some of these characteristics can be explained simply. The ideological division of political sensibilities among hackers often mirrors dominant and regional political patterns, but only up to a point. Other characteristics related to hacker tactics and political sociability are more particular and imminent to the sphere of hacking itself.

While making information publicly available and debating it are undeniably supported by most hackers, many projects—notably WikiLeaks and Anonymous—challenge the core liberal fantasy that status quo channels of debate and official, legally sanctioned domains of politics (notably the electoral party system) are sufficient to catalyze change. Hacker tactics—as evinced by tool making, legal reformulation, leaking, whistle-blowing, and especially direct action hacking—demonstrate a more forthright, hands-on engagement with politics than might be implied by their embrace of civil liberties. Indeed, time and again, hacker interventions exceed liberal publicity and enter squarely into the realm of action—sometimes even principled illegal direct action.[10]

Hackers also distinguish themselves by their avid embrace of political intersectionality: hackers exhibit a high degree of tolerance for working across ideological lines. In many projects, pragmatic judgments often trump ideological ones—leading to situations where, say, an anticapitalist anarchist might work in partnership with a liberal social democrat without friction or sectarian infighting. Let me illustrate with an eminent case: self-professed anarchist hacker Jeremy Hammond is now serving a decade-long stint in jail for acts of computer intrusion and corporate sabotage coordinated with colleagues under the mantle of Anonymous. Hammond dedicated most of his adult existence to demolishing capitalism and the liberal state, aiming to engender a more egalitarian society through all sorts of anarchist and environmental political endeavors, often in ways that had nothing to do with technology. But as a hacker, his interest was piqued by the activist activities of Anonymous. Initially he refused to contribute, put off by the crass and often racist language tolerated among the Anonymous ranks. But over time his views shifted as he began to judge the merits of Anonymous in terms of its hacking accomplishments and not its style of discourse. Ultimately, his decision to join forces with Anonymous was based on a pragmatic calculus: the actions being executed mattered more than the absence of clearly articulated democratic visions and goals.[11]

In my 15 years of research on hackers I have seen similar logics and forms of reasoning at work numerous times. To be sure, notable exceptions abound: many of the leftist technology collectives discussed above restrict membership because of issues of trust. And political infighting has at times erupted over linguistic minutia—as in the Free and Open Source Software movement, where one contingent accuses another of having adopted the term "open" as an alternative to "free" in the late 1990s as a way to attract funding from investors made nervous by more explicit political language (Berry 2008).

But in a striking number of endeavors—in activism, in piracy, in software development, and beyond—hackers avoid defining (and thus policing) the broadly defined ideologies that all their participants must share (see Postill 2014 for a discussion of pragmatism and political hacking). While, as in the case of Debian, they frequently define policies, codes of conduct, and even requisite skills and knowledge, rarely does this extend to the level of political belief. In some cases, this political agnosticism, as I have termed it elsewhere (Coleman 2013), follows from a drive to configure project goals narrowly, often around technical or civil liberties goals alone. In other instances, as with Anonymous, a more radical form of impurity is perceptible: defining Anonymous within delineated political parameters would be tantamount to confining and strangling its very purpose and spirit.

It would be overly simplistic to claim that the distinct forms that hacker politics assume—the tendency for hackers to supplement publicity with deeds and their accentuated willingness to work across ideological differences—follow in any deterministic way from the craft and craftiness of hacking, from the fact that hackers are avid makers and problem solvers with an antiauthoritarianism and crafty bent, but it would be equally simplistic to entirely discount them in our accounting of the contemporary shape of hacker politics.

Conclusion: Weapons of the Geek

We have seen that hackers perform politics in a variety of ways, engaging in politics for a variety of purposes, with a variety of ends in mind: from liberal, civic engagements designed to enhance government statecraft to anarchic attempts to develop software and communities that exist outside of the capitalist economy and its concomitant liberal political institutions. In

[9] See Keizer (2012) for a defense of privacy on socialist grounds.

[10] Darin Barney (2013) convincingly argues that WikiLeaks, so identified with a liberal project of publicity, in fact sharply deviates from a liberal logic, instead relying on tactics that exceed debate and also threaten the very core of liberal governance. A distinct though related—and perceptive—argument has been posed by Johan Söderberg (2013), who notes that even though hackers are wedded to theories of technological determinism, they nevertheless still engage in collective action to fight for change. He not only highlights the disjuncture between deterministic ideas and hacker political practices but also examines how theories of determinism can form the very impetus for action.

[11] As a graduate student rightly reminded me during a workshop, pragmatism itself can work ideologically; indeed, it can be thus posed as a core hacker political sensibility. It is still worthwhile to highlight how this embrace of pragmatism, however it is defined, allows for some hackers to work together in spite of holding different political goals and aims.

spite of these differences, central to the contemporary intensification of hacker politics have been a handful of events—what historian Bill Sewell (2005) calls "critical events." These exceptional moments have been crucial in setting the politics of hacking on a new path not only for the changes they immediately trigger but also for their ability to serve as models for emulation. The early days of hacking saw a smattering of such episodes, but the most recent ones cataloged above—beginning with WikiLeaks, followed by a burst of multiyear activity from Anonymous, and being capped off, finally, with Snowden's megaleak—have far surpassed them in terms of geopolitical weightiness.

Still, it would not do to overemphasize the importance of these critical events alone: without the shared sociocultural conditions inventoried in this piece, such events would have been less likely to manifest themselves, or at least so explosively. The particular forms that contemporary hacker political activities take are necessarily heterogeneous, but the attributes addressed here constitute a shared set of cultural practices, sensibilities, and even political tactics that are helpful to consider under a general rubric: "weapons of the geek." This is a modality of politics that obviously sits in direct contrast to the "weapons of the weak," a term the political scientist and anthropologist James Scott (1985) used in his book of the same name to capture the unique nature of clandestine peasant politics. While weapons of the weak embody tactics used by economically marginalized populations—small-scale illicit acts, such as foot dragging and vandalism—that do not appear on their surface to be political, weapons of the geek encompass a range of political interventions—recognized as such—and exercised by a class of privileged and visible actors who often lie at the center of economic life.[12]

To those familiar with Scott's work, connecting hackers with some of the poorest and most exploited members of society—with the subaltern—may strike one as ironic or just plain misguided. But what Scott's work on weapons of the weak so masterfully displayed was that political formations of resistance often exhibit both a logic and artistry tied to concrete material and historical conditions. As craftspeople, hackers develop independent habits of critical thinking, build autonomous communities and infrastructures, and engage with law to reform or even negate it in ways to assert their rights to be hackers; closely related, craftiness and antiauthoritarianism are not only commensurable with the types of direct action and law-breaking tactics common to hacker politics today but also help explain why a portion of hackers are willing to take on such risk in the first place.

But for these conditions and characteristics to exert influence, they must exist widely, reflected in the life histories not of a handful of individuals but a larger mass of hackers. In fact, PW—the Toronto-based Dutch hacker discussed in the opening of this essay who was so certain of the role played by technologies and events as political motivators—himself possesses a biography laden with the sociocultural cues and attributes covered in this essay. This is evident even from a glance at his LinkedIn page, where along with his many professional work experiences, he lists a diverse set of volunteer affiliations, with a range of free spaces, informal hacker collectives, engineering associations, liberal nonprofits, and policy organizations:

> Working Group Chair, Document Editor, Participant of IETF [Internet Engineering Task Force]
>
> member, Electronic Frontier Foundation
>
> Cryptographer, Cypherpunks
>
> Co-Founder, HackLab.TO
>
> Founding Member, The Libreswan Project
>
> member, Hippies from Hell [hacker] Collective

Like PW, many hackers of the weapons of the geek family hold multiple relationships to each other through collective projects and free spaces; in his case, PW has participated in a number of these groups for over a decade. Nevertheless, had I featured someone else, say, an avowedly leftist hacker, her list would likely include a smattering of technical projects but also leftist hack labs or anarchist technology collectives. Geeks and hackers are not bound to a singular political sentiment or even format, and they certainly do not agree on how social change should proceed. But what they all have in common is that their political tools, and to a lesser degree their tactical sensibilities—their willingness to work across political lines and for a smaller number, their willingness to engage in risky illegal acts of direct action—emerge from the concrete experiences of their craft.

Still, under less auspicious conditions, the bloom of hacker politics of today could tomorrow wilt and wither away. One of the many threats to hacker politicization comes in the form of a particular breed of commercial culture: that of Silicon Valley–style entrepreneurship. While this ideology of development emerged from California, it has now diffused itself to major metropolitan centers across the globe, including New York, Austin, Denver, Boston, Shanghai, London, and Berlin (see Barbrook and Cameron 1996; Marwick 2013; Neff 2012; Turner 2006). Autonomous hacker sensibilities and projects have long been and are routinely co-opted by these economic forces, aesthetically adopted for corporate imperatives in hackathons (Irani 2015), or colonized outright by incentivizing individual professionalization and careerism (Delfanti and Söderberg 2015).

Just how this relationship will unfold remains to be seen. In a great many instances, steady employment can grant security

[12] For a thoughtful and detailed discussion of how distinct political tactics of hackers, including leaking, breaching, pirating, and DDoSing, interface with different modalities of power, see Rosado-Murillo and Kelty (2017).

and leisure time to engage in noncommercial projects. And there is a revered tradition among leftist hackers to poach time at work to build and maintain autonomous hacker infrastructure—an easy enough feat to pull off, because managers lacking technical training are unable to tell the difference between one green matrix and another. But the more regions that adopt the particular strains of Bay Area technology culture—which requires significant investments of personal time and paints capitalist-based technological work as politically progressive—the greater the hazard it will be to the reproduction of hacker politics.

Still, despite this (and other) threats, what has been extraordinary about the last 5 years especially is that a sizeable number of hackers increasingly recognize that their rights—and the rights of others—will not be protected unless they engage in wilful political action of the sort that exceeds an inward-facing set of concerns. What this transformation—from securing an inward-facing form of craft autonomy to a more robust outward-facing sphere of political activities—shows us that events are not enough, technologies are not enough, commitments to technology are not enough, individuals are not enough, and free spaces and communities are not enough: what is needed is the dense accretion of all these things. It is the ensemble of all these pieces that constitutes the resources and infrastructure suited to nourishing a desire for and ability to act politically—if and when the right historical circumstances arise.

References Cited

Barbrook, Richard, and Andy Cameron. 1996. The California ideology. *Science as Culture* 6(1):44–72.

Barney, Darin. 2013. Publics without politics: surplus publicity as depoliticization. In *Publicity and the Canadian state: critical communications approaches*. Kirsten Kozolanka, ed. Pp. 72–88. Toronto: University of Toronto Press.

Bazzichelli, Tatiana. 2013. *Networked disruption: rethinking oppositions in art, hacktivism and the business of social networking*. Aarhus: Aarhus Universitet Multimedieuddannelsen.

Berry, David M. 2008. *Copy, rip, burn: the politics of copyleft and open source*. London: Pluto.

Beyer, Jessica L. 2014. *Expect us: online communities and political mobilization*. Oxford: Oxford University Press.

Burkart, Patrick. 2014. *Pirate politics: the new information policy contests*. Cambridge, MA: MIT Press.

Coleman, E. Gabriella. 2013. *Coding freedom: the ethics and aesthetics of hacking*. Princeton, NJ: Princeton University Press.

———. 2015. *Hacker, hoaxer, whistleblower, spy: the many faces of Anonymous*. London: Verso.

———. 2016. Hackers. In *Digital keywords: a vocabulary of information society and culture*. Ben Peters, ed. Pp. 158–172. Princeton, NJ: Princeton University Press.

Collins, Harry. 2010. *Tacit and explicit knowledge*. Chicago: University of Chicago Press.

Corsin Jimenez, Alberto, and Adolfo Estalella. 2016. Ethnography: a prototype. In *Obstruction and intervention*. Rane Willerslev, Lotte Meinert, and George Marcus, eds. Special issue, *Ethnos*, doi:10.1080/00141844.2015.1133688.

Delfanti, Alessandro. 2013. *Biohackers: the politics of open science*. London: Pluto.

Delfanti, Alessandro, and Johan Söderberg. 2015. Hacking hacked! the life cycles of digital innovation. *Science, Technology, and Human Values* 40:793–798.

Dreyfus, Suelette. 1997. *Underground: tales of hacking, madness and obsession on the electronic frontier*. Boroondara, Australia: Reed.

Golumbia, David. 2013. Cyberlibertarians: digital deletion of the left. *Jacobin*, December 4. https://www.jacobinmag.com/2013/12/cyberlibertarians-digital-deletion-of-the-left/.

Goriunova, Olga, ed. 2014. *Fun and software: exploring pleasure, paradox and pain in computing*. New York: Bloomsbury Academic.

Greenberg, Andy. 2012. *This machine kills secrets: how WikiLeakers, cypherpunks, and hacktivists aim to free the world's information*. New York: Dutton Adult.

Irani, Lili. 2015. Hackathons and the making of entrepreneurial citizenship. *Science, Technology, and Human Values* 40(5):799–824.

Jordan, Tim. 2008. *Hacking: digital media and technological determinism*. Cambridge: Polity.

Jordan, Tim, and Paul A. Taylor. 2004. *Hacktivism and cyberwars: rebels with a cause?* London: Routledge.

Juris, Jeffrey S. 2008. *Networking futures: the movements against corporate globalization*. Durham, NC: Duke University Press.

Keizer, Garret. 2012. *Privacy*. New York: Picador.

Kelty, Christopher M. 2008. *Two bits: the cultural significance of free software*. Durham, NC: Duke University Press.

Kubitschko, Sebastian. 2015. Hackers' media practices: demonstrating and articulating expertise as interlocking arrangements. *Convergence: The International Journal of Research into New Media* 21(3):388–402.

Lapsley, Phil. 2013. *Exploding the phone: the untold story of the teenagers and outlaws who hacked Ma Bell*. New York: Grove.

Levy, Steven. 2001. *Crypto: how the code rebels beat the government, saving privacy in the digital age*. London: Penguin.

———. 2010 (1984). *Hackers*. Sebastopol, CA: O'Reilly Media.

Marwick, Alice, and danah boyd. 2011. To see and be seen: celebrity practice on Twitter. *Convergence: The International Journal of Research into New Media Technologies* 17(2):139–158.

Maxigas. 2012. Hacklabs and hackerspaces: tracing two genealogies. *Journal of Peer Production* 2. http://peerproduction.net/issues/issue-2/peer-reviewed-papers/hacklabs-and-hackerspaces/.

McKelvey, Fenwick. 2014. We like copies, just don't let the others fool you: the paradox of the Pirate Bay. *Television and New Media* 16(8):734–750.

Mentor, The. 1986. The conscience of a hacker. *Phrack Magazine*, January. http://phrack.org/issues/7/3.html#articleMontfort.

Milan, Stefania. 2013. *Social movements and their technologies*. London: Palgrave.

Milberry, Kate. (Re)making the Internet: free software and the social factory hack. In *DIY citizenship: critical making and social media*. Matt Ratto and Megan Boler, eds. Cambridge, MA: MIT Press.

Mills, Elinor. 2008. Social engineering 101: Mitnick and other hackers show how it's done. *CNET*, July 21. http://www.cnet.com/news/social-engineering-101-mitnick-and-other-hackers-show-how-its-done/.

Montfort, Nick. 2008. Obfuscated code. In *Software studies: a lexicon*. Matthew Fuller, ed. Pp. 193–199. Cambridge, MA: MIT Press.

Neff, Gina. 2012. *Venture labor: work and the burden of risk in innovative industries*. Cambridge, MA: MIT Press.

O'Neil, Mathieu. 2009. *Cyberchiefs: autonomy and authority in online tribes*. London: Pluto.

Orr, Julian E. 1996. *Talking about machines: an ethnography of a modern job*. Ithaca, NY: ILR.

Peterson, T. F. 2011. *Nightwork: a history of hacks and pranks at MIT*. Cambridge, MA: MIT Press.

Polletta, Francesca. 1999. "Free spaces" in collective action. *Theory and Society* 28(1):1–38.

Polyani, Michael. 1967. *The tacit dimension*. New York: Anchor.

Postigo, Hector. 2012. *The digital rights movement: the role of technology in subverting digital copyright*. Cambridge, MA: MIT Press.

Postill, John. 2014. Freedom technologists and the new protest movements: a theory of protest formulas. *Convergence: The International Journal of Research into New Media Technologies* 20(4):402–418.

Rosado-Murillo, Luis Felipe, and Christopher M. Kelty. 2017. Hacking und hackers. In *Digitalisierung: Theorien und Konzepte für die Empirische Forschung*. Gertraud Koch, ed. Konstanz: UVK Press. Forthcoming.

Sauter, Molly. 2014. *The coming swarm: DDOS actions, hacktivism, and civil disobedience on the Internet*. New York: Bloomsbury Academic.

Schoen, Seth, 2001. *How to decrypt a DVD: in haiku form. (Thanks, Prof. D. S. T.)*. https://www.cs.cmu.edu/~dst/DeCSS/Gallery/decss-haiku.txt.

Schrock, Andrew Richard. 2016. Civic hacking as data activism and advocacy: a history from publicity to open government data. *New Media and Society* 18(4):581–599.

Scott, James. 1985. *Weapons of the weak: everyday forms of peasant resistance*. New Haven, CT: Yale University Press.

Sennett, Richard. 2009. *The craftsman*. New Haven, CT: Yale University Press.

Sewell, William H. 2005. *Logics of history: social theory and social transformation*. Chicago: University of Chicago Press.

Söderberg, Johan. 2007. *Hacking capitalism: the free and open source software movement*. London: Routledge.

———. 2013. Determining social change: the role of technological determinism in the collective action framing of hackers. *New Media and Society* 15(8):1277–1293.

Sterling, Bruce. 1992. *The hacker crackdown: law and disorder on the electronic frontier*. New York: Bantam.

Straw, Will. 2014. Some things a scene might be. *Cultural Studies* 29(3):476–485.

Thomas, Douglas. 2003. *Hacker culture*. Minneapolis: University of Minnesota Press.

Thompson, E. P. 1978. *Poverty of theory*. London: Monthly Review.

Thorsen, Einar, Chindu Sreedharan, and Stuart Allan. 2013. WikiLeaks and whistle-blowing: the framing of Bradley Manning. In *Beyond WikiLeaks: implications for the future of communications, journalism and society*. Benedetta Brevini, Arne Hintz, and Patrick McCurdy, eds. Pp. 101–122. New York: Palgrave Macmillan.

Turner, Fred. 2006. *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. Chicago: University of Chicago Press.

Wark, McKenzie. 2004. *A hacker manifesto*. Cambridge, MA: Harvard University Press.

Warner, Michael. 2002. *Publics and counterpublics*. New York: Zone.

Wolfson, Todd. 2014. *Digital rebellion: the birth of the cyberleft*. Urbana-Champagne: University of Illinois Press.