From Internet Farming to Weapons of the Geek

The political education of apolitical technical people is extraordinary
Julian Assange, 2014

Gabriella Coleman
McGill University

Draft Paper for Current Anthropology special issue on New Media, New Publics. Please don't circulate, share, etc. Citations are incomplete.

In January 2015, after delivering a talk about the protest ensemble Anonymous at the University of Toronto, I went out to lunch with PW—a forty-something Dutch hacker now living in Canada, who I first met in 2002 while conducting a stint of research in Amsterdam. Given his expertise in cryptography and security, the conversation inexorably 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 historic and urgent 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, who has been intensely involved in the hacker scene for his whole adult life, did not skip a beat in tendering the following analysis: the political impacts of hackers would emerge diffusely, over an extended period of time, products of the types of technologies, like the internet itself, they work to build. To punctuate this point, he described hackers as "internet farmers." Just as the rise of agriculturalists ushered in massive changes by altering material relations to food supplies, so too would hackers and their technologists allies alter the course of human history by virtue of their technological artifacts. In other words, the impact of particular hacker individuals or organizations would be largely irrelevant—micro gestures within a broader, deterministic narrative 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 explicit activism or political tool building have long existed (Taylor and Jordan 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 five 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.

In particular, direct action and civil disobedience have surged in a variety of formats and styles, often related to leaks and exfiltration. We see lone leakers, like Chelsea Manning, and also leftist collectivist leaking endeavors such as Xnet in Spain. Other political engagements are threaded through software: for instance, protocols (like BitTorrent) and technical file sharing platforms like the Pirate Bay enable piracy and the legal sharing of cultural goods (Beyer 2014; McKelvey, forthcoming). 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 (Kelty 2008; Coleman 2013) and have inspired others, notably scientists, academics, and lawyers, to embolden arguments for access (Delfanti 2013). Across Europe, Latin America, and the

United States, anti-capitalist, leftist hackers run collectives—many doubling as anarchist associations—providing privacy-enhancing technical support and services for leftist crusaders aiming for systemic social transformations (Wolfson; Juris; Pickard). Anonymous, specializing in digital direct dissent, 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: 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 lawmaking, political tool building, and especially forms of direct action and civil disobedience so risky, scores of hackers are currently in jail or exile for their willingness to expose wrong-doing.

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 acts of civil disobedience? These are questions that beg for nuanced answers—beyond the blind celebration or denegration offered by popular characterizations of hacker politics.

This article will foremost provide an introductory inventory—a basic outline of the socio-cultural attributes and corollary historical conditions responsible for the intensification of hacker politics during the last five years. Probably the most important factor is a shared commitments to preserving autonomous ways of thinking, being, and interacting. Let's 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 85th web page— rarely does a week, or even a day, go by without offering small or large 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 emails before calling it a day. Distracted, I foolishly opened that 85th web page, prompting my computer, which runs a version of the Linux operating system, first to freeze, then go black, and finally reboot itself. Livid, I was fairly certain hours of work were about to be nuked into oblivion (I was right). Then this happened.

```
Oct 8 15:48:02 kernel: [27653668.999445] Out of memory: Kill process
12731 (redacted) score 318 or sacrifice child
```

"Sacrifice child?" I laughed, snapped a picture, and shared it on twitter. Clearly some developer had embedded this humorous message in an otherwise dry (and for the technically illiterate, likely incomprehensible) system log error message.[1] I was reminded: behind every piece of software is an auteur, a code writer with a distinctive creative style willing in some cases to implant humor into pieces of technology. Though already familiar with hacker humor—having dedicated an entire book chapter to the subject—my foul mood was replaced with exuberance: because this was the very first time I encountered a joke embedded in technology without hunting for one.

[1] The suggestion to sacrifice a child may seem like a random, and especially, mean-spirited message to send, one designed simply to shock the clueless user but to those familiar with Unix based operating system, this statement is actually technically accurate. To regain memory one has two choices: kill a specific process or kill what the more general process, which is referred to as a "child process," as it is a sub-processes of another parent one.

This sort of joke directs us to some unique and defining features common to hackers, at least when compared to other technologists—system administrators, programmers, security researchers—who like hackers, perform the same sort of labor and functions. Like hackers, all these technologists are quintessential craftspeople —tenaciously 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 especially 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 play between craft and craftiness, of respect for tradition and its complete, often wanton, disregard, is in itself not exclusive to hackers, or technologists. It is evident among a range of laborers and professionals guided by a crafting sensibility: from engineers to professors, from journalists to carpenters. Indeed, academics depend upon and reproduce convention by referencing the work of peers, but they also strive to advance novel and counter-intuitive arguments, and gain individual recognition in the doing.

What is unique to hackers is how outward display of craftiness has surpassed mere instrumentality to take on its own, robust life; craftiness and its associated attributes, such as guile, wit, and cleverness, are revered as much for their form as for their function. In contrast, for most craftspeople, craftiness is means to 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 aesthetic 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 it was acceptable, even welcome, for an audience member to interrupt a speaker in order to crack a joke (perhaps the only other groups 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 to me that hackers inject humor into every social situation and artifact, whenever they can: they joke and pun offline and online social interactions; 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, like the esoteric and minimalist programming language called BrainFuck. Hackers also have a long history of mischief making and pranking; according many, the term 'hacks' was first coined to describe a type of practical joke. Craftiness and humor have also been core to many of the hacker political battles addressed later in this essay. (For detailed analysis of the pervasiveness of cleverness and humor in hacker circles, see Goriunova, 2014; Montfor 2008; Coleman 2013).

Valorizing this craftiness even for non-instrumental uses, hackers invite levity and play into their activities and artifacts. But, perhaps even more importantly, they also maintain and hone it for even non-technical pursuits, the faculty: keeping it sharp and: ready-at-hand for when a truly stunning hack must be effected.

The Autonomous Mindset

Easiest way to get a hacker to do something: tell them they can't. Institutionalized oppositional defiance disorder (a hacker)

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

Emblematic of this ethos is the iconic "The Conscience of a Hacker," authored by a figure known as the "Mentor" and collectively redubbed as simply "A Hacker Manifesto" since its release. 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." While one might imagine a statement like this emerging 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 as a hacker: "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, behold many illicit components. The history of hacking is littered with examples of disobeyed norms, rules, and sometimes laws. These repeated subversive acts not only support anti-authoritarian attitudes directly but also, as The Hacker Manifesto attests, do so through 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 its cultural and technical legs in the late 1950s and early 1960s, rule breaking was often the essential condition to the access of any equipment. For phone freaks, rule breaking was simply unavoidable. Their entire raison d'être was the exploration of phone systems, and the connection 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 without fail every time they phreaked. The first freak arrests occurred in 1961 (Lapsley 2013: 59), although it would be another few decades before they—and their hacker cousins—felt the full brunt of the law (to be addressed later in the essay).

When compared to the freaks, university-based hackers rarely broke the law. But even among the small cadre of hacker-students who held computer privileges in prestigious universities, such as Carnegie Mellon, UCLA, Stanford, MIT, rules were frequently twisted—usually to land more time on their beloved computers. In his thorough account of the first generation MIT hackers, journalist Steven Levy characterizes the hacker proclivity to bend rules in this way:

> 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. When a hacker needed something to help him create, explore, or fix, he did not bother with such ridiculous concepts as property rights (1984: page).

These hackers willing to defy rules were partially shielded from punishment since they were, after all, affiliated as students. But a handful of pre-teen 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 conventions or rule, while in other cases, they clearly relish breaking the law, anti-authoritarianism is evident across varied hacking lineages. While craftiness emerges through technical practice, and rule bending and law breaking reinforce anti-authoritarianism, both mindsets now constitute the rhetorical repertoires that hackers use to self-describe themselves in writing and in everyday conversation.

Together, craftiness and anti-authoritarianism might be understood to cultivate an attitude that is profoundly individualistic, or even anti-social. 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 hyper socialized 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 (ever changing) guidelines of quality (Sennett 2009). Hacking is no exception to these craft dynamics.

Whether acknowledged or not by hackers themselves, all types of hacking embody profound forms of social entanglement and deep 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 and feelings of camaraderie are 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 endless numbers of developer and hacker conferences.

These are sites where hackers gather, deliberate, and work semi-autonomously from the mandates and demands of their day job. Taken together, they qualify as what scholars of social movements designate as "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 like 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 (examples might be a books 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 come to mind). What they all share is they are infused with logics of independence: participants run these spaces collectively and autonomously, outside the penumbra of the direct control and influence of dominant institutions, values, and ideologies, whether they be economic, political, cultural or some combination of the three. Indeed, a couple of the core technologies that constitute hacker free spaces, like Internet Relay Chat and mailing lists (and BBSes in earlier eras) are not only easy for hackers to set up, but, are non-commercial zones of freedom on an Internet almost thoroughly dominated today by private interests.[2]

Hackers cobble together the mediating, communication technologies that double as hacker

[2] There are some important differences, however, between most hacker and non-hacker free spaces: Compared to traditional free space venues, whose costs of renting or ownership are significant—downright exorbitant if they are located in cities like New York, London, Paris, Vancouver, 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 upkeep systems.

free spaces in radically 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 make 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, if not hundreds, of examples 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. Many of the technical engineers within Debian function as political architects, and together they have established the project as a federation, which functions something like a worker's cooperative. They have outlined intricate voting procedures for the purposes of governance, and articulated precise commitments and stipulations ratified in a series of legal and ethical charters and manifestos. Prior to enrollment, *all* prospective members are tested on their knowledge of the project's technical policies, legal commitments, and ethical norms (O'Neil 2009; Coleman 2013).

If Debian is configured as a sort of miniature society—and given its Social Constitution and Manifesto, having a very 19th century, Enlightenment feel to it—Anonymous, by contrast, is more opaque, and expansive, functioning more informally as a “scene” (Straw 200_). While increasingly recognizable as advocates for social justice and stewards of direct action—employing, as they have, a stable roster of tools and tactics, they refuse to establish an ideological common denominator, much less some universal set of ethical and political statements, like the sort Debian has ratified. Inhabiting a range of technologies—particularly Twitter accounts and a multitude of chat rooms, some public and some private, spread across the globe—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 five years. Still, most operations can be understood as somehow well organized, but given its dynamic geography, Anonymous eschews stabilization and routinization. Combine these characteristics with the fact that some hackers rely on partial secrecy, Anonymous is distinctive (and refreshing) for how it so fully resists concrete sociological mapping and thus categorization.

Where Debian proceeds from a set of rules, Anonymous is like an anti-algorithm: 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 hackers are nonetheless social to the extreme. Anonymous members communicate consistently—even if they don't know exactly who is on the other end—and Debian developers do too—with individuals carefully vetted by the project to which they are all devote themselves (to officially join the virtual project, a prospective developer must first get their cryptographic identity verified by another developer, in person).

In the case of Anonymous a crafty anti-authoritarianism is directed at the states and corporations that so often find themselves their targets. Yet rarely does this imply an antisociality that prevents them from working with with hacker colleagues. Likewise, even as Debian developers might maintain a suspicion of mainstream institutions, they suspend this tendency when it comes to their own institution, willing to trust their community's vetting processes and policies.

State Intervention as a Political Catalyst

So far we have considered three crucial components of a hacker subjectivity which help us grasp their political subjectivity: the playful valorization of craftiness, a culturally instantiated anti-authoritarianism, and a tendency to form tight bonds of fellowship around labor in free spaces. These features do not in themselves account for the hacker tendency towards political action. But by helping to reinforce and reproduce independent habits of thinking, skills suited to maintaining and governing technologies that enable autonomous congregation and action, and communities of mutual support, they form vital pillars capable of propping up the forms of collective, 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 partly and increasingly oriented in response to the problems of outsiders—and determined through a lens of social justice or defending civil liberties— the original catalyst that unites hackers in political action tends to emerge when the community itself is threatened. Thus the major, and perhaps unsurprising, trigger of hacker politicization has come about as a response to long standing and aggressive state and corporate hostility towards hackers and their technologies.

In this sense, the hacker public is also as an apt example of what Michael Warner identifies as a counterpublic—one which "maintain[s] at some level, conscious or not, an awareness of its subordinate status" (2002:56). 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 rise up and 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.

The transition from the analog phone network, following the divestiture of "Ma Bell," heralded the end of the golden age of phreaking. The practice was largely replaced in the 1980s 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—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, passed in the United States (Computer Fraud and Abuse Act in 1986), Australia (Crimes Legislation Amendment Act in 1989), and the United Kingdom (Computer Misuse Act in 1990).

Throughout the 1990s, law enforcement coordinated multi-state raids that targeted swaths of hackers and sought to shut-down the BBSes where they trafficked in secret knowledge and illicit information. Hackers were slapped with trumped up charges and fines that rarely matched the nature of the crime. Bruce Sterling, 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” (1992:104).

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 co-founder of the enormously popular e-zine *Phrack* (featuring hyperbolic, audacious, and relentlessly anti-authoritarian material, a healthy portion of which was expressly devoted to parodying the FBI). While Neidorf originally faced thirty-one 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 in fact available at the library for any member of the public to access. Charges were ultimately dropped—but only after a costly legal battle. So astounding was his plight, it helped spur the founding of what is now the largest non-profit for defending civil liberties in the digital realm, the Electronic Frontier Foundation, whose lawyers have by now defended scores of hackers against state prosecution.

Many subsequent cases were equally troubling for how state prosecution against hackers inched dangerously close to persecution. For instance, 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 nor cause any permanent damage. Nevertheless, because he was a “hacker,” the Department of Justice jailed him for four years in pre-trial confinement, followed by eight months in solitary confinement. Such harsh treatment was deemed necessary because law enforcement officials convinced the judge that Mitnick could “start a nuclear way by whistling into a pay phone.”

While a great majority of the 1990s and 2000s cases involved computer intrusion, these hackers rarely sought to profit from 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 naturally took a keen interest, dotting news headlines and television talk shows with tales of “mad hackers” and “real electronic Hannibal Lecters.”[3] Branded by the courts and the media as outlaws, the anti-authoritarianism harbored by hackers only intensified, and became marshaled in activist 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

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

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 (PGP), a piece of public encryption technology designed to enhance the privacy of regular citizens. Principally authored by cryptographer Phil Zimmerman, it's international release in 1991 constituted a daring act of civil disobedience, breaking international munition and patent laws predicated on the military uses of encryption (Levy 2001[1984]; Greenberg 2012). 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 tee-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 convinced 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 it's 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 re-published DeCSS online, printed the DeCSS co it received scant coverage in the mainstream media, and de on t-shirts. Some enacted even craftier forms of protest. One hacker, Seth Schoen, rewrote the program mathematically as a haiku, or to be more exact: as 256 haikus 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 the reader as follows:

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). As alliances were forged with civil liberties groups, lawyers, and librarians, what is now popularly known as the "digital rights movement" was more fully constituted (Postigo 2012).

Still, while the DeCSS legal imbroglio and it's activist outcomes became known to most every geek, hacker, civil liberties lawyer, and radical librarian at the time of its unfolding, it received scant coverage in the mainstream media, and it's 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 entitles and figures like 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’ release of the Collateral Murder war video in April of 2010, followed quickly by a large slab of diplomatic cables, set the course of hacker politics in a new direction, catapulting figures like Chelsea Manning—who was revealed to have leaked the content to WikiLeaks—to global prominence. Beginning in 2011, Antonymous' wily, media spectacular actions made it clear that this sudden gush of hacker 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 Swartz took his own life after he found him 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 upon them were of an unprecedented calibre: marshalling 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 Russia, respectively, due to 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 only demonizing the legal plights of these hackers, media outlets have instead publicized these cases widely, and sometimes sympathetically (Thorsen et al, 2013). Meanwhile, producers of popular cultural media now routinely portray these hackers as laudable heroes or anti-heroes. Television shows like Mr. Robot, House of Cards, The Good Wife, and Homeland feature prominent and powerful hacker characters. Films like *Black Hat* and the forthcoming *Snowden* offer similar treatments. And even independent documentary films explicitly sympathetic to these figures, such as Laura Poitras' 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 hacker—such as WikiLeaks' aggressive, direct action quest for radical press freedom or Anonymous contributions to all the major social revolutions transpiring in 2011—and the crackdowns against them, have drawn in hosts of sympathetic allies and bedfellows, extending the reach and impact of their original interventions into increasingly diverse domains. Spurred on by these exceptional events, many hackers previously wary of explicit political involvement—and many of their less technical but no less geeky cousins, too—have been drawn into full blown activist and political organizing.

The Liberal and Radical Politics of Hacking

Now that we have identified a few of the reasons that prompt 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 into broader political trends and traditions? If hackers aren't 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 as a general category might at least give us some hints. And here too we find more nuance than a blanket anti-authoritarianism might suggest. After all, code functions, in many ways, like a law unto itself.

Hacker's don't only hold an exhaustively antagonistic relationship to the law, but also at times a scholarly, even cooperative one. As I have argued elsewhere, a formal, homologous relationship exists between 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 like the law. 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, statutes, and ideas more generally.

Hackers have been known to use this facility with the law in the service of social change, both by diagnosing, avoiding, and arguing against laws they deem bad, and also, as in the case of free software, by detourning 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 (as property-rights, definitions of agrarian practice) 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 (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 to 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, 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. And there has never been anything like it in the world. 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.[4] (emphasis added)

[4] Excerpt from the documentary Citizen Four, directed by Laura Poitras (2014; Toronto: Praxis), Film.

For Snowden, the internet ought to be a medium to actualize unhampered exchange of ideas and permissive forms of free thinking. For those of a similar mind to Snowden, a concern for civil liberties is not separate or supplemental to a deep 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 puts it, is one shared by countless geeks (2008). The hacker commitment to civil liberties demonstrates a commitment to their own existence as an entity—what Chris Kelty defines as a recursive public: which includes the necessary liberties to pursue self-defined cultural and technical activity (2008).

Unsurprisingly, given the hacker interest in civil liberties, many hacker-led political endeavors mushrooming today also align with, and even directly bolster liberal or libertarian aspirations, aiming to reform existing political structures in the West. There are many such examples to choose from including the recent chartering of the Pirate Parties (Burkhart 201_), but the exemplary case is civic hacking, especially when these efforts at increasing transparency are directed at government itself. Civic hackers code tools and propose policies meant to increase government accountability by making data and processes more readily available (Schrock 2016, add others).

But other hackers, even whose products may advance the agenda of civil liberties, demonstrate a more radical disposition. Sometimes this takes the form of reforming or fundamentally challenging the institutions already in existence towards more liberatory ends. In effect, some hackers have carved out pockets of autonomy or alterity (Soderberg 2012; Wark 2004). Free software may be bought and sold in the market, but the product itself has been legally inoculated to prevent the dis-ease of alienation so common to capitalist labor relations. Anonymous, in so discouraging and criticizing fame seeking and social peacocking behaviors, enacts a critical practice of egalitarianism and solidarity (Coleman 2015); its ethics deviates sharply from the common practices of individualized branding and micro-celebrity flourishing on the same social media platforms used by Anonymous (Marwick 201_).

Elsewhere hacker politics take more resistive forms that are outright contrary or antagonistic to liberalism and capitalism. There are many such examples, past and present, of self-avowed anarchist, socialists, or Marxists hackers,who build tools and supporting systems for more radical, even revolutionary projects aiming at systemic change (see Wolfson 2015, also Coleman 2013, Pickard 201_; Juris 201). One of the most muscular of these endeavors undoubtedly is Indymedia—the big bang of online alternative media initiatives—having inspired countless copycats in its wake. Conceived by hackers directly involved in the yearlong planning efforts to stage a spectacular, large-scale demonstration during the 1999 Seattle-based World Trade Organization convention, these hacker-organizers accurately anticipated the mainstream media would hijack the representations of protest activity through tactics of simplification or distortion. These hackers implemented a novel content management system—unique at the time for making it easy to publish video and images online, years before the rise of web 2.0 platforms—so that protest organizers and rabble rousers could in effect bypass the media to become the media and cover what became known as the Battle of Seattle on their own terms.

At the height of its operations, the Indymedia technical team, spread across the globe, maintained over 250 (double-check number) journalism centers—no doubt one of the forces helping to propel the broader social justice movement outward across space and forward in time; in so doing a tight knit network of revolutionary hackers was also constituted—one that has continued to exist into the present, long after the counterglobalization movement has joined 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—the norm for Internet corporations offering so-called free services. This infrastructure is composed of a sizable roster of independently run internet service providers, many of which are also organized around consensus-based, anarchist principles. Roughly twenty eight across the world, their names bear the imprint of radical sensibilities: Riseup, 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 email and mailing list services to a user base that includes other technologists but is primarily composed of leftist political groups having little to do with the politics of technology.[5] For Riseup, technology is not an worthy as an end but rather as a conduit to "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," as its members have articulated it on their website.

My brief inventory of hacker projects simply demonstrates the ideological sensibilities underwriting hacker politics are far from unitary: just as we can locate liberal hackers and projects, so too can we just as easily identify radical interventions, both instances having measurable social impacts. To be sure, civil liberties can be considered as something of a universal among politically minded hackers, but even then such a blanket statement demands qualification. Even if civil liberties, being central components of liberal doctrine, are obviously and particularly consistent with liberal projects, leftist treatments of civil liberties, as the Riseup quote suggests (and as writers have started to explore in more detail[6]), frame free speech and privacy distinctly: not conceived as important for guaranteeing individual rights but instead treated as enablers for equality and justice. As to be expected —where the socialist and anarchist left is larger and more sturdy—Spain, Italy, Greece, Croatia, Argentina—so too are leftist hacker projects more present and robust.

[5] It now functions as one of largest non-profit internet service providers in the world (barring universities) and is member base nearly doubled after the Snowden revelations. blob:https %3A//share.riseup.net/b1e7e37a-4d4e-4d5f-809e-84410dca1ab9

[6] See Keizer 2012, for example.

These trends can be stated simply: the ideological division of political sensibilities among hackers generally mirrors and matches 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 the merely relying on accepted channels for debate or officially, legally-sanctioned domains of politics (notably the electoral, party system), are sufficient to catalyze change. Hacker tactics—as evinced in tool making, legal reformulation, leaking, whistleblowing, 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 in the realm of action with a smaller sub-set being illegal direct action.[7]

It would be overly simplistic to claim that the hacker's delivery of their politics through the channels of making and acting precipitates in any deterministic, law-like way from the craft and craftiness of hacking: the fact that hackers are avid makers and problem solvers with an anti-authoritarianism and crafty bent. It is simply a proclivity whose existence is connected loosely to the labor and cultural conditions of hacking.

Another such tendency can be gleaned by the type of political sociability encouraged by hackers. For many projects, it is evident that a pragmatic sets of judgments can trump ideologically defined ones in the following fashion: hackers exhibit a high degree of tolerance for working across ideological lines so that individuals who hold distinct political sensibilities can routinely collaborate without friction or sectarian in-fighting.

[7] Add Darin Barney.

Let me illustrate with an eminent case: Jeremy Hammond is a self-professed anarchist now serving a decade long stint in jail for his many acts of computer intrusion and corporate sabotage coordinated with hacker colleagues identifying as Anonymous. He is the sort of anarchist that, prior to joining forces with Anonymous, dedicated most of his adult existence to demolishing the liberal state aiming instead to engender a more egalitarian society through all sorts of non-technological form of anarchist and environmental politics. As a hacker, his interest had been naturally piqued by the faceless collective but initially he refused to contribute put off by Anonymous' tolerance of crass, and often racist language. But over time, his views started to shifts, as he judged the merits of Anonymous in terms of its growing hacking accomplishments/pedigrees. Ultimately his decision to join forces with Anonymous was based on a pragmatic calculus whereby tangible actions being executed and effected mattered more than Anonymous's lack of clearly articulated democratic visions and goals.

In my fifteen years of research on hackers I have seen similar logics and forms of reasoning at work numerous times. To be sure, notable exceptions abound: leftist technology collectives discussed above, tightly control membership due to issues of trust. Some degree of political infighting has erupted at the level of linguistic minutia—specific words—notably the terms free vs. open variably used to describe software libre—have bee the source of repeated contention since 1999 when the term “open” was coined by hackers seeking to attract investor funding. But for a striking number of endeavors, including Anonymous and especially the development of free software like Debian or specific tools, Tor and infrastructures like pirate sharing technologies—hackers don't expend a whole lot of energy on defining (and thus policing) the broadly-defined ideologies that participants should share. In some cases, this political agnosticism, as I have termed it elsewhere, follows from an impetus to narrowly configure project goals, often around technical or civil liberties terms alone. In other instances, like with Anonymous, a more radical form of ideological impurity can be gleaned: defining

Anonymous within clear political parameters would be tantamount to confining and strangling its very purpose and spirit.

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 spite of these differences, central to the contemporary intensification of hacker politics have been a handful of events—what historian Bill Sewell calls "critical events." These exceptional moments have been crucial in setting the politics of hacking on a new path not only for the ripples of change 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 catalogued above—beginning with WikiLeaks, followed by a burst of multi-year activity from Anonymous, and being capped off, finally, with Snowden's mega leak—have far surpassed them in terms of geopolitical weightiness.

Still it would not do to over-emphasize the importance of these critical events alone: without the shared, underlying socio-cultural dynamics and conditions inventoried in this piece, such events would have been less likely to manifest, or at least so explosively. The particular forms that contemporary hacker political activities take are necessarily heterogeneous but the conditions and attributes addressed here constitute a shared set of cultural practices, sensibilities, and even political tactics which 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 anthropologist James Scott used in his 1985 book of the same name to capture the unique nature of clandestine peasant politics. While the weapons of the weak embody tactics used by economically marginalized populations–small- scale illicit acts such as foot dragging and vandalism—that don't appear on their surface to be political, weapons of the geek is a form of politics exercised by a class of privileged and visible actors who often lie at the center of economic life.

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 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 anti-authoritarianism are not only commensurable with the types of direct action and law breaking tactics common to hacker politics today, but 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, must exist widely, reflected in the life histories of not a couple of individuals but a larger corpus of hackers. In fact, PW—the Toronto-based Dutch hacker who opens this essay so certain of the role played by technologies and events as political motivators—himself possesses a biography laden with the socio-cultural 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 affiliations: with a range of free spaces, informal hacker collectives, engineering associations, liberal non-profits, and policy orgs, flagging each with pride:

Working Group Chair, Document Editor, Participant

IETF [Internet Engineering Task Force]
2003– Present (12 years)
Participant in various IETF working groups related to security (ipsecme, dnsext, dnsop, dane, tls, saag, pkix, trans, etc). On of the co-authors on RFC 7250. Document Author and/or Editor of various drafts in dnsops and dane.

member
Electronic Frontier Foundation
2001 – Present (14 years)
Hat wielding proud member of the Electronic Frontier Foundation
Cryptographer

Cypherpunks
1997 – Present (18 years)
crypting

Co-Founder
HackLab.TO
July 2008 – Present (7 years)
Co-founder and current board member of HackLab Toronto Inc., which operates a community research lab / hacker space in Toronto.

Founding Member
The Libreswan Project
January 2012 – Present (3 years 6 months)
I am one of the core developers of libreswan, which forked from openswan 2.6.38 after a legal dispute.

member
Hippies from Hell [hacker] Collective
1997– 2007 (10 years).

Like PW, many hackers who are members of the weapons of the geek family hold multiple and dense relationships to each other through the medium of collective projects and free spaces. Had I featured someone else, say, avowedly leftist hackers, his list would likely include a smattering of technical projects but also anarchist technology collectives. Just as there are many ways to hack, so too are there many ways for hackers to enter the political arena. Geeks and hackers are not bound to a singular political sentiment or even format, and they certainly don’t 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: from collaborating together in autonomous spaces, and from their shared experiences pushing back against authoritarian crackdowns against specific instances of hacking, software, and now hacker-led interventions directed at broader social issues.

But the solid foundation upon which today's political ferment has been assembled/secured, might be a fragile thing. 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 tech entrepreneurship. While this ideology of production and development emerged from California, it has now diffused itself to major metropolitan centers across the globe, including New York City, Austin, Denver, Boston, Shanghai, London, and Berlin (Turner 2006; Barbrook and Cameron 1996; Marwick 201_; Neff 201_). Independent and autonomous hacker sensibilities, projects, and products have long been and are routinely co-opted by these economic forces, aesthetically adopted for corporate imperatives in hackathons (Irani) and developer conferences, or colonized outright by incentivizing individual professionalization and careerism (Delfanti and Soderberg 2015).

Just how this relationship will unfold remains to be seen. In a great many instances, financial freedom of employment can grant security and leisure time to engage in non-commercial projects. And there is 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 from another. But the more regions adopt the *particular* virulent strains of Bay Area technology culture—which requires significant investments of personal time—the greater the hazard it will be to the reproduction/future of hacker politics.

Still, despite this (and other) threats, what has been extraordinary about the last five 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 a insular, inward facing set of craft concerns. What this transformation—from securing an insular-facing form 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, either: but the dense accretion of all these things—stabilized by participation in free spaces, hacker collectives, and the greater hacker public—operating alongside anti-authoritarian habits of mind, access to technology, technical proficiency, a respect of the hack as form and function—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

Assange, Julian. 2014. Wikileaks. New York and London: OR Books.

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. Publicity and the Canadian State: Critical Communications Approaches. Kirsten Kozolanka (ed.). University of Toronto Press.

Bazzichelli, Tatiana. 2013. *Networked disruption: rethinking oppositions in art, hacktivism and the business of social networking*. 1st edition. Aarhus N, Denmark: Aarhus Universitet Multimedieuddannelsen

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

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

Borsook, Paulina. 2000. *Cyberselfish: a critical romp through the terribly libertarian culture of high tech*. New York: PublicAffairs.

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

Chan, Anita Say. 2014. *Networking peripheries: technological futures and the myth of digital universalism*. Cambridge, MA: The MIT Press.

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

Coleman, E, and Alex Golub. 2008. Hacker practice. *Anthropological Theory* 8(3): 255–277.

———. 2014. *Hacker,* hoaxer, whistleblower, spy: the many faces of Anonymous. London: Verso.

Comaroff, Jean and John Comaroff. 2003. Reflections on liberalism, policulturalism, and ID-ology: citizenship and difference in South Africa. *Social Identities.* 9(3): 445-474.

Crawford, Matthew. 2010. *Shop class as soulcraft: an inquiry into the value of work*. New York: Penguin.

Dreyfus, Suelette. 1997. Underground: tales of hacking, madness and obsession on the Electronic Frontier. *Boroondara, Australia:* Reed Books Australia.

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

Gregg, Melissa and Carl DiSalvo. 2013. The trouble with white hats. *The New Inquiry*, November 21. http://thenewinquiry.com/essays/the-trouble-with-white-hats/.

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. Forthcoming. Hackathons and the making of entrepreneurial citizenship. *Science, Technology, and Human Values*.

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

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

Kelty, Christopher M. 2008. *Two Bits: the cultural significance of Free Software*. Durham, NC: Duke University Press.

Kubitschko, Sebastian. Forthcoming. Hackers' media practices: demonstrating and articulating expertise as interlocking arrangements. *Convergence: The International Journal of Research into New Media*.

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

Levy, Steven. 2001 [1984]. *Crypto: how the code rebels beat the government saving privacy in the digital age*. 1st edition. London: Penguin Books.

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

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. Forthcoming. "We like copies, just don't let the others fool you: the paradox of The Pirate Bay." *Television and New Media*.

Montfort, Nick. 2008. Obfuscated code. In *Software Studies a Lexicon*, Matthew Fuller, ed. Cambridge, MA: MIT Press.

Nissenbaum, Helen. 2004. Hackers and the contested ontology of cyberspace. *New Media and Society (6)2:195-217.*

O'Neil, Mathieu. 2009. *Cyberchiefs: autonomy and authority in online tribes*. 1st edition. London: Pluto Press.

Orr, Julian E. 1996. *Talking about machines: an ethnography of a modern job*. 1st edition. Ithaca, NY: ILR Press.

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

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

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

Söderberg, Johan. 2008. *Hacking Capitalism: The Free and Open Source Software Movement*. London: Routledge.

Schrock, Andrew Richard. Forthcoming. Civic hacking as data activism and advocacy: A history from publicity to open government data.*New Media & Society*.

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

———. 2012. *Two cheers for anarchism.* Princeton, NJ: Princeton University Press.

Sennett, Richard. 2009. *The Craftsman*. 1 edition. New Haven, CT: Yale University Press.

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

Sterling, Bruce. 1992. *The hacker crackdown: law and disorder on the Electronic Frontier*. New York: Bantam Books.

Takhteyev, Yuri. 2012. *Coding places: software practice in a South American city*. Cambridge, MA: The MIT Press.

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

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

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 Books.