Digital Keywords

A Vocabulary of Information Society and Culture

Edited by
Benjamin Peters

Princeton University Press
Princeton and Oxford

Contents

15

Hacker

Gabriella Coleman

In the 1950s a small group of MIT-based computer enthusiasts, many of them model train builders/tinkerers, adopted the term *hacker* to differentiate their freewheeling attitude from those of their peers. While most MIT engineers relied on convention to deliver proven results, hackers courted contingency, disregarding norms or rules they thought likely to stifle creative invention. These hackers, like the engineers they distinguished themselves from, were primarily students, but a handful of outsiders, some of them preteens, were also deemed to possess the desire and intellectual chops required to hack and were adopted into the informal club; in the eyes of this group, hackers repurposed tools in the service of beauty and utility, while those students "who insisted on studying for courses" were considered "tools" themselves (Levy 1984, 10).

Since this coinage sixty years ago, the range of activity wedded to the term *hacking* has expanded exponentially. Bloggers share tips about "life hacks" (tricks for managing time or overcoming the challenges of everyday life); corporations, governments, and NGOs host "hackathon" coding sprints (Gregg and DiSalvo 2013; Irani 2015); and the "hacktivist," once a marginal political actor, now stands at the center of geopolitical life (Jordan and Taylor 2004; Beyer 2014; Sauter 2014; Coleman 2014).

Since the early 1980s, the hacker archetype has also become a staple of our mass media diet. Rarely does a day pass without an article detailing an enormous security breach at the hands of shadowy hackers, who have ransacked corporate servers to pilfer personal and lucrative data. Alongside these newspaper headlines, hackers often feature prominently in popular film, magazines, literature, and TV (Alper 2014; Schulte 2013).

Despite this pervasiveness, academic books on the subject of hacking are scant. To date the most substantive historical accounts have been penned by journalists (Levy 1984; Sterling 1992; Lapsley 2013; Greenberg 2012), while academics have written a handful of sociological, anthropological, and philosophical books—typically with a media studies orientation (Thomas 2002; Wark 2004; Kelty 2008; Coleman 2013, 2014). Surveying the popular, journalistic, and academic material on hackers, one discovers that few words in the English language evoke such a bundle of simultaneously negative and positive—even sexy—connotations: mysterious, criminal, impulsive, brilliant, chauvinistic, white knight, digital Robin Hood, young, white, male, politically naive, libertarian, wizardly, entitled, brilliant, skilled, mystical, monastic, creepy, creative, obsessive, methodological, quirky, asocial, pathological.

Some of these associations carry with them a kernel of truth, especially in North America and Europe: conferences are populated by seas of mostly white men; their professionalizable skills, which encompass the distinct technical arts of programming, security research, hardware building, and system/network administration, land them mostly in a middle-class or higher tax bracket (they are among the few professionals who can scramble up corporate ladders without a college degree); and their much-vaunted libertarianism does, indeed, thrive in particular regions like Silicon Valley, the global start-up capital of the world, and select projects like the cryptocurrency Bitcoin.

Yet many other popular and entrenched ideas about hacking are more fable than reality. Hackers, so often tagged as asocial lone wolves, are in fact highly social, as evidenced by the hundreds of hacker or developer cons that typically repeat annually and boast impressive attendance records (Coleman 2010). Another misconception concerns the core political sensibility of the hacker. Many articles universalize a libertarianism to the entirety of hacking practitioners in the West. Whether appraising them positively as freedom fighters or deriding them as naive miscreants, journalists and academics often pin the origins of their practice on an anti-authoritarian distrust of government combined with an ardent support for free market capitalism. This posited libertarianism is most

often mentioned in passing as simple fact or marshaled to explain everything from their (supposedly naive) behavior to the nature of their political activity or inactivity (Borsook 2000; Golumbia 2013).

What is the source of this association, and why has it proved so tenacious? The reasons are complex, but we can identify at least two clear contributing factors. First, many hackers, especially in the West, do demonstrate an enthusiastic commitment to anti-authoritarianism and a variety of civil liberties. Most notably, hackers advocate privacy and free speech rights—a propensity erroneously (if perhaps understandably) flattened into a perception of libertarianism. While these sensibilities are wholly compatible and hold affinities with a libertarian agenda, the two are by no means coconstitutive, nor does one necessarily follow from the other.

The second source propping up the myth of the libertarian hacker concerns the framing and uptake of published accounts. Certain depictions of particular aspects of hacking or specific geographic regions wherein libertarianism does, indeed, dominate are routinely represented as, and subsequently taken up as, indicative of the entire hacker culture (Turner 2006).[1] This is only magnified by the fact that Silicon Valley technologists, many of whom promulgate what Richard Barbrook and Andy Cameron have named the "Californian ideology"—"a mix of cybernetics, free market economics, and counter-culture"—are so well resourced that their activities and values, however specific, circulate in the public more pervasively than those at work in other domains of hacker practice (1996). There is no question that the California ideology remains salient (Morozov 2013; Marwick 2013)—but it by no means qualifies as a singular hacker worldview homogeneous across regions, generations, projects, and styles of hacking.

This disproportionately fortified stereotype of the libertarian hacker, along with the paucity of historical studies and contemporary research regarding other values and regional logics at work in hacking, forms the terrain from which scholars of hackers currently work and write. But this seems, slowly, to be changing. Increasingly, scholars are tracing the genealogies of hacking practices, ethics, and values to heterodox, multiplicitous origins (Jordan 2008; Coleman and Golub 2008). For instance, the inception of the "hacker underground"—an archipelago of tight-knit crews

who embrace transgression, enact secrecy, and excel in the art of computer intrusion—can be traced to the phone phreaks: proto-hackers who, operating both independently and collectively, made it their mission to covertly explore phone systems for a variety of reasons that rarely involved capital gain (Lapsely 2013). Conversely, "free software" hackers are far more transparent in their constitution and activities as they utilize legal mechanisms that aim to guarantee perpetual access to their creations (Coleman 2012). Meanwhile, "open-source" hackers, close cousins to their equivalents in the free software movement, downplay the language of rights, emphasizing methodological benefits and freedom of choice in how to use software over the perpetual freedom of the software itself; as a result, open-source ideology maintains an affinity with neoliberal logics, while free software runs directly against this current (Berry 2008). Another engagement still is displayed by "the crypto-warriors," covered in great detail by journalist Andy Greenberg, who concern themselves with technical means for securing anonymity and privacy (2012). Their reasons and ideologies differ, but they align in the desire for and development of tools that might ensure these ends.

So while libertarianism is an important worldview to consider, especially in various regions and particular projects, it fails to function effectively as a thread to connect different styles and genres of hacking. However, this doesn't mean we can't consider other commitments around which hackers do, indeed, seem to share a common grounding.

The Craftiness of Craft

Hacking, across its various manifestations, can be seen as a site where craft and craftiness converge: building a 3D printer that can replicate itself; stealing a botnet—an army of zombie computers—to blast a website for a political distributed denial-of-service (DDoS) campaign; inventing a license called copyleft that aims to guarantee openness of distribution by redeploying the logic inherent to copyright itself; showcasing a robot that mixes cocktails at a scientific-geek festival devoted entirely to, well, the art of cocktail robotics; inventing a programming language called Brainfuck

which, as you might infer, is designed to humorously mess with people's heads; the list goes on. The alignment of craft and craftiness is perhaps the best location to find a unifying thread that runs throughout the diverse technical and ethical worlds of hacking.

To hack is to seek quality and excellence in technological production. In this regard, all hackers fit the bill as quintessential "craftspeople," as defined by sociologist Richard Sennett: "Craftsmanship names an enduring, basic human impulse, the desire to do a job well for its own sake" (2009). In the twentieth century, with the dominance of Fordist styles of factory labor and other bureaucratic mandates, crafting has suffered a precipitous decline in Western mainstream economies, argues Sennett. Among hackers, however, this style of laboring still runs remarkably deep and strong (Hannemyr 2009).

Even if craftspeople tend to work in solitude, crafting is by definition a collectivist pursuit based on shared rules of engagement and standards for quality. Craftspeople gather in social spaces, like the workshop, to learn, mentor each other, and establish guidelines for exchange and making. Among hackers this ethic has remained intact, in part because they have built the necessary social spaces—mailing lists, code repositories, free software projects, hacker and maker spaces, Internet chat relays—where they can freely associate and work semiautonomously, free from the imperatives and mandates of their day jobs (Shrock 2014).

Large free and open-source projects are even similar to the guilds of yore, where fraternity was cultivated through labor. Free and Open Source Software (F/OSS) institutions are supported by brick-and-mortar infrastructures (servers, code repository) along with sophisticated and elaborate organizational mechanisms. The largest such project is undoubtedly Debian—boasting over a thousand members who maintain the twenty-five thousand pieces of software that together constitute the Linux-based operating system. In existence now for twenty-one years, Debian is a federation sustained by procedures for vetting new members (including tests of their philosophical and legal knowledge regarding free software), intricate voting procedures, and a yearly developer conference that functions as a sort of pilgrimage (Coleman 2013; O'Neil 2009).

Craft and all the social processes entailed—the establishment of rules, norms, pedagogy, traditions, social spaces, and institutions—nevertheless coexist with countervailing, but equally prevalent, dispositions: notably individualism, antiauthoritarism, and craft*iness*. Hackers routinely seek to display their creativity and individuality and are well known for balking at convention and bending (or simply breaking) the rules. If a hacker inherits a code base she dislikes, she is likely to simply reinvent it. One core definition of a hack is a ruthlessly clever and unique prank or technical solution. By extension its creator is also designated as unique.

Craftiness is foremost an aesthetic disposition, finding expression in a plethora of practical engagements that include wily pranks and the writing of code—which is sometimes sparsely elegant and at other times densely obfuscated (Monfort 2008). Its purest manifestation, I have argued elsewhere, lies in the joking and humor so common to the hacker habitat (Coleman 2013, and see the collection in Gorinova 2014). "Easter eggs" provide the classic example: clever and often nonfunctional jokes are commonly integrated into software instructions or manuals.

Hacking is not the only crafting endeavor straddling this line between collectivism and individualism, between tradition and craftiness; the tensions between these poles are apparent among academics who depend upon conventional referencing of peers' work while simultaneously striving to advance clever, novel, counterintuitive arguments and individual recognition. Craftspeople who build and maintain technologies must be similarly enterprising, especially when improvising a fix for something like an old engine or obsolete photocopying machine (Orr 1996). Indeed, the craft-vocation of the security hacker requires what we might describe as intellectual guile. When lecturing to my class one security researcher described the mentality: "You have to, like, have an innate understanding that [a security measure is] arbitrary, it's an arbitrary mechanism that does something that's unnatural and therefore can be circumvented in all likelihood." Craftiness, then, can be seen as thinking outside the box, or circumvention of inherent technological limitations in pursuit of craft. But we can also understand craftiness as exceeding mere instrumentality. Among hackers, the

performance of this functional aspect becomes an aesthetic pursuit, a thing valued in and of itself.

The Power and Politics of Hacking

The interplay between craft and craftiness can be treated as something of a hacking universal, then. But it would be wrong to claim that these two attributes are alone capable of sparking political awareness or activism, or even that all hacking qualifies as political, much less politically progressive. Indeed, for a fuller accounting of the politics of hacking it is necessary to consider the variable cultures and ethics of hacking that underwrite craft and craftiness. Hacker political interventions must also be historically situated, in light of regional differences (Chan 2014; Takhteyev 2012), notable "critical events" (Sewell 2005)—like the release of diplomatic cables by the whistle-blowing hacker organization WikiLeaks—and the broader socioeconomic conditions that frame the labor of hacking (Wark 2004).

Indeed, there is little doubt that commercial opportunities fundamentally shape and alter the ethical tenor and political possibilities of hacking. So many hacker sensibilities, projects, and products are motivated by, threatened by, or easily folded into corporate imperatives (Delfanti and Soderberg 2015). Take, for instance, the hacker commitment to autonomy. Technology giant Google, seeking to lure top talent, instituted the "20 percent policy" (Tate 2013). The company affords its engineers, many of whom value technical sovereignty as part of their ethos, the freedom to work one day a week on their own self-directed projects. And Google is not unique; the informal policy is found in a slew of Silicon Valley firms like Twitter, Facebook, Yahoo, and LinkedIn. Of course, critics rightly charge that this so-called freedom simply translates into even longer and more grueling work weeks. Corporations advertise and institutionalize "hackathons" as a way to capitalize on the feel-good mythology of the hacker freedom fighter—all while reaping the fruits of the labor performed therein. In high-tech Chinese cities like Shanghai, where hacker spaces are currently mushrooming, ethics of openness have been determined to bolster entrepreneurial

goals beyond those of any individual or unaffiliated collective (Lindtner and Li 2012; Lindtner 2015).

It is nevertheless remarkable that hackers, so deeply entwined in the economy, have managed to preserve pockets of meaningful social autonomy and have frequently instigated or catalyzed political change. Hacking, especially the transgressive art of computer intrusion, to be sure has long exhibited a powerful, albeit latent, political subtext (Soderberg 2012; Wark 2004). But in the past five years, activist-motivated hacking has significantly enlarged its scope and continues to demonstrate nuanced and diverse ideological commitments. Many of these commitments cannot be reduced to "libertarianism," that ideology universalized by many observers as the crux of hacker politics. For one, civil disobedience has surged in a variety of formats and styles, often in relation to leaks and exfiltration. We see lone leakers, like Chelsea Manning, and also collectivist and leftist leaking endeavors, perhaps best exemplified by Xnet in Spain. Other political engagements, similarly irreducible to libertarian values alone, center on collective engagements at the level of software: hackers have recently coded up protocols (like BitTorrent) and technical platforms (like The Pirate Bay) to enable peer-to-peer file sharing and anticopyright piracy (Beyer 2014; McKelvey 2015); since the 1980s, free software hackers have embedded their collectively produced programs with legal stipulations that have powerfully tilted the politics of intellectual property law in favor of access (Kelty 2008; Coleman 2013); Across Europe, Latin America, and the United States, anticapitalist hackers run small but well-functioning collectives that offer privacy-enhancing technical support and services for leftist crusaders; Anonymous, a worldwide protest ensemble specializing in digital direct dissent, has established itself as one of the most populist manifestations of contemporary geek politics—requiring no technical skills to contribute (Coleman 2014); and finally, on the more liberal front, civic and open government hackers throughout North and South America have sought to improve government transparency by creating open standards and applications that facilitate data access and sharing (Gregg and DiSalvo 2013; Schrock forthcoming). Julian Assange, one of the most prominent activist hackers, has recently

highlighted the rather dramatic turn to activism and political engagement among geeky technologists. "The political education of apolitical technical people is extraordinary" (2014, 116), he noted during an interview.

If the past five years are any indication, this is a trend that we can expect to grow. What, then, are the sociological and historical conditions that have helped secure and sustain this vibrant sphere of hacker-led political action, especially in light of the economic privilege they enjoy?

Part of the answer lies in craft and the "workshops," like Internet Relay Chat (IRC), mailing lists, and maker spaces, where hackers collectively labor. Taken together they constitute what anthropologist Chris Kelty defines as a recursive public: "a public that is vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its own existence as a public; *it is a collective independent of other forms of constituted power and is capable of speaking to existing forms of power through the production of actually existing alternatives*" (2008). What Kelty highlights with his theory of recursive publics is not so much its politics but its *power*—a point also extended in a different manner by McKenzie Wark in *A Hacker Manifesto* (2004). Hackers hold the knowledge—and thus the power—to build and maintain the technological spaces that are partly, or fully, independent from the institutions where they otherwise work for pay. These autonomous zones are where they labor, but also the locales where hacker identities are forged and communities emerge to discuss values deemed essential to the practice of their craft.

Taken from another disciplinary vantage point, these spaces qualify as what sociologists of social movements call "free spaces," historically identified in radical book shops, bars, block clubs, tenant associations, and the like. Generally these are "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). The vibrancy of hacker politics is contingent on the geeky varieties of such free spaces.

It is important to emphasize, however, that while recursive publics or free spaces do not, in and of themselves, guarantee the

emergence of hacker political sensibilities, they remain nevertheless vital stage settings for the possibility of activism; however, regional differences figure prominently. For instance, much of the hacker-based political activism emanates from Europe. Compared to their North American counterparts (especially those in the United States), European hackers tend to tout their political commitments in easily recognizable ways, often aligning themselves with politically mandated hacker groups and spaces (Bazzichelli 2013). The continent boasts dozens of autonomous, anticapitalist technology collectives, from Spain to Croatia, and has a developed activist practice that fuses art with hacking (Maxigas 2012). One of the oldest collectives, the German-based Chaos Computer Club (established in 1981), has worked to shape technology policy in dialogue with government for over a decade (Kubitschko 2015). A great majority of the participants populating the insurgent protest ensemble Anonymous are European. Perhaps most tellingly, the first robust, formalized, geek political organization, the Pirate Party, was founded in Sweden (Burkart 2014).

Not all hackers are seeking, however, to promote social transformation. But we can nevertheless consider how many of their legal and technical artifacts catalyze enduring and pervasive political changes regardless of intent.

Craft autonomy figures heavily in this unexpected dynamic, one that can be observed, perhaps most clearly, in the production of F/OSS. Productive autonomy and access to the underlying structures of code are enshrined values in this community, and politics seems to be a natural outcome of such commitments. Irrespective of personal motivation or a project's stated political position, F/OSS has functioned as a sort of icon, a living example from which other actors in fields like law, journalism, and education have made cases for open access. To give but one example, Free Software licensing directly inspired the chartering of the Creative Commons nonprofit, which has developed a suite of open-access licenses for modes of cultural production that extend far beyond the purview of hacking (Coleman and Hill 2004). Additionally, F/OSS practices have enabled radical thinkers and activists to showcase and advocate the vitality, persistence, and possibility of nonalienated labor (Hardt and Negri 2005).

Like F/OSS hackers, those in the underground also strive for and enact craft autonomy with interesting political effects—but here autonomy is understood and enacted differently. Often referred to as blackhats, these hackers pursue forbidden knowledge. Lured as they are by the thrills offered by the subversion of owning and exploring systems, their politics—whether explicit or not—are foremost rooted in transgression for pushing legal, technical, and ethical boundaries. Many of their literary artifacts, such as textfiles and zines, go a step further, actively mocking FBI agents and thus state power (Thomas 2002; Coleman 2012).

Their acts also serve pedagogical purposes, and many have emerged from these illegal, underground nooks into the realm of academic or corporate security research. Their hands-on experiences locating vulnerabilities and sleuthing systems are easily transferrable into efforts to fortify—rather than penetrate—technical systems. Predictably, the establishment of a profitable security industry is seen by some underground hackers as a threat to their autonomy: some critics deride their fellow hackers for selling out to the man (Anonymous 2012). A much larger number don't have a problem with the aim of securitization per se, but nevertheless chastise those attracted to the field by lucrative salaries rather than a passionate allegiance to quality. In one piece declaring the death of the hacker underground, a hacker laments: "Unfortunately, fewer and fewer people are willing, or indeed capable of following this path, of pursuing that ever-unattainable goal of technical perfection. Instead, the current trend is to pursue the lowest common denominator, to do the least amount of work to gain the most fame, respect or money" (Anonymous 2008).

A major, and perhaps unsurprising, motivator of hacker politicization comes in the wake of state intervention. The most potent periods of hacker politicization (at least in the American context) are undoubtedly those following arrests of underground hackers like Craig Neidorf (Sterling 1992) or Kevin Mitnick (Thomas 2002). The criminalization of software can also do the trick; hacker-cryptographer Phil Zimmerman broke numerous munitions and intellectual property laws when he released PGP (Pretty Good Privacy) encryption to the world—a fact governments did not fail to notice or act upon (Levy 2001). But this act of civil disobedience

helped engender the now firmly established hacker notion that software deserves free speech protections (Coleman 2009).

In many such instances, the pushback against criminalization spills beyond hacker concerns, engaging questions of civil liberties more generally. Activists outside the hacker discipline are inevitably drawn in, and the political language they deploy results in a sort of positive feedback loop for the hackers initially activated. We saw this precise pattern with the release and attempted suppression of DeCSS, a short program that could be used to circumvent copy and regional access controls on DVDs. In the United States, hackers who shared or published this code were sued under the Digital Millennium Copyright Act, and its author was subsequently arrested in Norway. State criminalization led to a surge of protest activity among hackers across Europe and North America as they insisted upon free speech rights to write and release code, indisputably cementing the association between free speech and code. 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).

See in this volume: activism, community, digital, forum, geek, internet, mirror, participation

See in Williams: anarchism, capitalism, collective, creative, culture, democracy, expert, liberation, originality, status

Note

1 For instance, Turner's excellent account about the Silicon Valley regions is taken up to argue for a more general libertarianism.

References

Alper, Meryl. 2014. "'Can Our Kids Hack It with Computers?' Constructing Youth Hackers in Family Computing Magazines." *International Journal of Communication* 8: 673–98.

Anonymous. 2008. "The Underground Myth." *Phrack Inc.* 0x0c, no. 0x41 (November).

———. 2012. "Lines in the Sand: Which Side Are You On in the Hacker Class War." *Phrack Inc.* 0x0e, no. 0x44 (April).

Assange, Julian. 2014. *WikiLeaks*. New York: OR Books.
Barbrook, R., and A. Cameron. 1996. "The California Ideology." *Science as Culture* 6(1): 44–72.
Bazzichelli, Tatiana. 2013. *Networked Disruption: Rethinking Oppositions in Art, Hacktivism and the Business of Social Networking*. Aarhus N, Denmark: Aarhus Universitet Multimedieuddannelsen.
Berry, David. 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: MIT Press, 2014.
Chan, Anita Say. 2014. *Networking Peripheries: Technological Futures and the Myth of Digital Universalism*. Cambridge, MA: MIT Press.
Coleman, Gabriella. 2009. "Code Is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers." *Cultural Anthropology* 24(3): 420–54.
———. 2010. "The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld." *Anthropological Quarterly* 83(1): 47–72.
———. 2012. "Phreaks, Hackers, and Trolls and the Politics of Transgression and Spectacle." In *The Social Media Reader*, edited by Michael Mandiberg. New York: New York University Press.
———. 2013. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.
———. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso.
Coleman, E. Gabriella, and Alex Golub. 2008. "Hacker Practice." *Anthropological Theory* 8(3): 255–77.
Coleman, Gabriella, and Mako Hill. 2004. "How Free Became Open and Everything Else under the Sun." *MC Journal* 7(3) (July).
Delfanti, Alessandro, and Johan Soderberg. 2015. "Hacking Hacked! The Life Cycles of Digital Innovation." *Science, Technology & Human Values* 40: 793–98.
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.
Gregg, Melissa, and Carl DiSalvo. 2013. "The Trouble with White Hats." *New Inquiry*, November 21. http://thenewinquiry.com/essays/the-trouble-with-white-hats/.
Hannemyr, Gisle. 1999. "Technology and Pleasure: Considering Hacking Constructive." *First Monday* 4(2) (February 1). http://journals.uic.edu/ojs/index.php/fm/article/view/647.

Hardt, Michael, and Antonio Negri. 2005. *Multitude: War and Democracy in the Age of Empire*. Reprint ed. New York: Penguin Books.
Irani, Lili. 2015. "Hackathons and the Making of Entrepreneurial Citizenship." *Science, Technology & Human Values* 40(5): 799–824.
Jordan, Tim. 2008. *Hacking: Digital Media and Technological Determinism*. Cambridge: Polity Press.
Jordan, Tim, and Paul Taylor. 2004. *Hacktivism and Cyberwars: Rebels with a Cause?* Routledge.
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 Press.
Lavy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. Garden City, NY: Anchor Press/Doubleday.
———. 2001. *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*. London: Penguin Books.
Lindtner, Silvia. 2015. "Hacking with Chinese Characteristics: The Promises of the Maker Movement against China's Manufacturing Culture." *Science, Technology & Human Values* 40: 854–79.
Lindtner, Silvia, and David Li. 2012. "Created in China." *Interactions* 19(6): 18.
Marwick, Alice E. 2013. *Status Update: Celebrity, Publicity, and Branding in the Social Media Age*. New Haven, CT: Yale University Press.
Maxigas. 2012. "Hacklabs and Hackerspaces—Tracing Two Genealogies." *Journal of Peer Production*, no. 2. http://peerproduction.net/issues/issue-2/peer-reviewed-papers/hacklabs-and-hackerspaces.
McKelvey, Fenwick. 2015. "We Like Copies, Just Don't Let the Others Fool You: The Paradox of The Pirate Bay." *Television and New Media*. 16(8): 734–50.
Montfort, Nick. 2008. "Obfuscated Code." In *Software Studies: A Lexicon*, edited by Matthew Fuller. Cambridge, MA: MIT Press.
Morozov, Evgeny. 2013. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs.
O'Neil, Mathieu. 2009. *Cyberchiefs: Autonomy and Authority in Online Tribes*. New York: Pluto Press.
Orr, Julian E. 1996. *Talking about Machines: An Ethnography of a Modern Job*. 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: MIT Press.
Sauter, Molly. 2014. *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic.
Schrock, Andrew Richard. 2014. "'Education in Disguise': Culture of a Hacker and Maker Space." *InterActions: UCLA Journal of Education and Information Studies* 10(1) (January 1). http://escholarship.org/uc/item/0js1n1qg.

———. Forthcoming. "Civic Hacking as Data Activism and Advocacy: A History from Publicity to Open Government Data." *New Media and Society*.
Schulte, Stephanie Ricker. 2013. *Cached: Decoding the Internet in Global Popular Culture*. New York: New York 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.
Soderberg, Johan. 2012. *Hacking Capitalism: The Free and Open Source Software Movement.* London: Routledge.
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: MIT Press.
Tate, Ryan. 2013. "Google Couldn't Kill 20 Percent Time Even If It Wanted To." *Wired*, August 21. http://www.wired.com/2013/08/20-percent-time-will-never-die/.
Thomas, Douglas. 2002. *Hacker Culture*. Minneapolis: University of Minnesota 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.