2 (Re)making the Internet: Free Software and the Social Factory Hack

Kate Milberry

With the emergence of global justice movement(s) in the mid-1990s, tech activists began remaking the Internet in the image of the just society they pursue. Using free and open source software (FOSS), tech activists continue to build the digital infrastructure of the "newest social movements," developing *technologies of resistance* to support activists online. The newest social movements are contemporary, broadly anti-capitalist social movements that organize loosely around anarchist politics, informed by emancipatory theory (Day 2005). By designing values into technology that are consonant with movement goals, tech activists engage in prefigurative politics. This self-reflexivity invokes the spirit of critical making as both an activity and a site for deepening a transformative sociotechnical praxis. In deploying FOSS across an increasingly commercialized and privatized web, tech activists enact their politics at both a technological and social level. Drawn from the free software and global justice movements, these values—including freedom, decentralization, heterarchy, autonomy, self-determination, collaboration, collectivism, and mutual aid—challenge capitalist norms that dominate the social factory both online and offline. This chapter considers the transformative potential of critical making as emancipated labor when it is manifest in tech activism. It locates critical making in the tradition of emancipatory theory and explores how tech activists hack the social factory, reconnecting society and technology by remaking the Internet into a more humane and democratic communication medium.

Tech Activism as Critical Making

Tech activists are hackers, coders, and self-described geeks who subscribe to the politics of the Free Software movement yet are committed to the goals of the newest social movements. These goals include gender and racial equality, economic justice, environmental sustainability, and labor and human rights, all of which they believe contribute to a freer, more just society. Tech activists build the online communication systems and software that support the broader movements to which they belong. Their prefigurative politics manifest as critical making when tech activists infuse unmet user needs, such as participatory democracy, consensus-based decision making, and security culture into the software design and development process. They further enact the values and skills necessary for deepening democracy offline through the FOSS mode of production, which relies on a set of social relations that challenge capitalist norms (Dunbar-Hester, chapter 4, this volume). Thus tech activists both anticipate and actualize the values they build into their technologies. This brand of critical making is therefore a means to an end, as well as an end in itself. It is also intentional: tech activists understand the political nature of technology as well as the sociality of its production. In producing technology that embeds new social relations, ones not founded on exploitation, exclusivity, scarcity, and profit, tech activists are remaking the Internet after the image of the better world they seek. Emancipatory theory and critical making come together in the work of tech activists as they intervene in the digital infrastructure, reconceptualizing the Internet as a contested terrain as well as a space and a tool of social critique, engagement, and change.

Species-Being, Hacking, and Emancipated Labor

The current strain of tech activism is the third wave of an historical trajectory that has its roots in hacking, which first emerged in the 1960s as a digital counterculture. Hacking in its original manifestation evokes the spirit of “species being”—that distinctively human capacity for self-determined activity that is realized in the productive or creative work of human beings. Species-being is fulfilled through emancipated labor, which Marx (1964) distinguishes from labor under capitalism. This he called “wage slavery” or estranged labor: the sale of one’s physical capacities for the minimum amount required to survive. Emancipated labor is rather a “process of genuine activity” in which a person develops him- or herself. Here work is not only a means to an end “but an end in itself, the meaningful expression of human energy; hence work is enjoyable” (Fromm 1961, 41).

First-generation computer hackers were graduate students building the early Internet at MIT’s Artificial Intelligence Lab. They were distinguished by their spirit of adventure, exploration, and play; they were fans who appreciated “the options, fun, excitement and fiendish fascination of computers” (Nelson 1987, 5). These early hackers “were permeated with the values of individual freedom, of independent thinking, and of sharing and co-operation" that also characterized the radical student movement of the day (Castells 2001, 24). They developed the habit of sharing source code based upon a firm belief that information should be free (Stallman 2002). Freedom is at the core of the hacker ethic (Levy 1984), which would become the philosophical and practical foundation of free and open source software.

Hacking and the FOSS mode of software development offer a contemporary example of Marx's emancipated labor. For Marx, labor is not merely the production of a commodity, or the reproduction of the physical existence of workers. Rather labor is something much more important: it is the means by which people fulfill their humanity, their species-being: "The nature of individuals . . . depends on the material conditions determining their production" (Marx and Engels 1970, 42). Thus the production and reproduction of the technical infrastructure are inextricably and dialectically bound to social life. As a genuine activity that expresses one's self, the FOSS mode of production engenders social relations that contradict the property relations that underpin modern capitalism. As a means of fulfilling one's human potential, the FOSS mode of production fosters relations of freedom, which are incorporated into the labor process at the same time as they are embedded in the outcome of that process: free and open source software. Hacking, the foundational activity of FOSS production, is commonly referred to as joyful (Himanen 2001), fun (Raymond 2001), playful (Levy 1984; Torvalds 2001) and humorous (Stallman 2002). It is often done for free, and always freely shared. FOSS as a labor process, therefore, belongs to a "much broader undercurrent revolting against . . . commodified labour and needs satisfaction" (Soderberg 2008, 44).

Emancipatory Theory and the Radical Potential of Critical Making

The possibilities for critical making as a strategy for social change appear when it is rooted in the emancipatory theory. Critical theory of technology, or critical constructivism, considers technology as a terrain of contestation and intervention by users, rather than a mysterious black box, the exclusive territory of designers (Feenberg 1991). It builds from critical theory, which provides the analytic and normative bases for social inquiry intended to reduce domination and increase freedom, "to liberate human beings from the circumstances that enslave them" (Horkheimer 1982, 244). Critical constructivism questions the social fixity of technology and looks for human interventions into the technical infrastructure of capitalism, and for the subsequent subversion (or affirmation) of dominant social values and interests that congeal there. The result of such interventions is a critical (re)making of the material world. Critical constructivism helps us understand how free and open source software increases user freedom and satisfies unfulfilled needs through hacking computer code. The FOSS mode of production inculcates a new set of social relations that challenges the capitalist mode of production upon which contemporary society is founded. In doing so, it offers a transformative vision of the future.

In critical theory's long tradition of social engagement, Feenberg (2002) calls for the creation of a politics of technological transformation that will rebuild society from its material base. In reclaiming technology from ownership and control by the technocapitalist class, the citizenry will, in dialectic fashion, become conscious of technology as both means of oppression *and* democratization. From here, the objective is to generalize the democratic tendencies of "technology for the people" to the political and economic structures of domination. The Internet as a technology-in-the-making, and the technological hack of writing free code as a constitutive part of this process, uncovers just such a possibility: that of translating critical making from the technical base to the sociopolitical realm, thereby transforming a technological practice into a social praxis of liberation. This recalls the "caring for" aspect of critical making necessary for the reconnection of society and technology (Ratto 2009), and for the humanization of technology in order to reduce human want, misery, cruelty, and violence.

Technologies of Resistance

Tech activists have heeded the call for a politics of technological transformation in building *technologies of resistance* intended to support grassroots struggle online, remaking the Internet as a more democratic and humane communication medium in the process. Such a transformation is possible because the Internet remains a flexible technology that has yet to reach closure; rather it is daily being made and remade by users and developers, as well as corporations and governments. How, then, will it concretize? What technical affordances will be baked into the architecture of the Internet; what social constraints will be laid over the top of the network? This is a social as well as a technological contest, one in which tech activists have been central. "Activist designers, software developers and digital artists have leveraged the malleability of IT and the openness of network protocols to develop utilities that are expressive of particular political commitments" (Howe and Nissenbaum 2009, 431).

Since the development of Active, the open publishing platform for Indymedia in 1999, tech activists have been rebuilding the application layer of the Internet. Concurrently, the forces of corporate and state enclosure have sought ever greater control of the Internet through cyber-surveillance on the one hand and legislation on the other (Milberry and Clement, forthcoming). Based entirely on FOSS, technologies of resistance are imbued with a prefigurative politics of emancipation. They seek to assist activists in their social justice work by providing secure communications and enhancing privacy and anonymity online. For example, email encryption is necessary for activists, who are often under surveillance by the state (Leistert 2012). The cryptographic software, *GNU Privacy Guard* (GnuPG), is a free implementation of PGP (Pretty Good Privacy), the original email encryption protocol developed by American antinuclear activist Philip Zimmerman. PGP employs public key encryption, where users have a secret key that matches a public key. Use of these keys protects the authenticity, confidentiality, and integrity of a message by creating a digital signature with the private key, which can then be verified by the public key. Zimmerman published his public key encryption software package for free on the Internet, believing it "would be of most use to dissidents, rebels and others who faced serious risks as a consequence of their beliefs" (Lucas 2006, 3).

CryptoSMS, developed by a tech activist in Germany, responds to activists' need for secure digital communication by encrypting text messages. *TextSecure* is a drop-in replacement for the Android text messaging application that encrypts messages stored on mobile phones and provides end-to-end message encryption when texting with someone else who is also using the app. It was developed by an anarchist FOSS coder, who also created *RedPhone*, another Android app that enables encrypted voice communication between RedPhone users. Encrypted mobile communication is increasingly critical with the proliferation of cell phones and the continued criminalization of dissent experienced by social movement organizers. The Anarchist Tech Support (ATS) collective advises activists to be diligent about encrypting their digital communications because these "are likely to be subject to more scrutiny" (ATS 2010). Indeed, while Deibert et al. (2008, 2010) document how totalitarian regimes around the world monitor the digital communications of human rights activists and political dissidents, Western democracies are not exempt from government spying schemes. Most notorious of these domestic surveillance programs is the "warrantless wiretapping" conducted in the United States by the National Security Agency and aided by major telecommunications carriers, including AT&T (Bamford 2008). Canada recently deployed the largest known domestic spying scheme in its history against activists opposed to the Toronto G20 Summit in 2010.

TXTMob is a text messaging system designed by tech activists to allow rapid, anonymous communication during protests. TXTMob was released as free software by the Institute for Applied Autonomy, an art and engineering collective that creates technologies for political dissent, as part of its "inverse surveillance" efforts. Activists using TXTMob on their cell phones communicate real-time information with each other about police movements, direct actions and calls for medical and legal support, helping them to remain organized during chaotic street actions. Although TXTMob has been superseded by the meteoric rise of Twitter, it is worth noting that the popular microblogging service was modeled on TXTMob (Henshaw-Plath 2008).

Psiphon is a web browser proxy created by tech activists at the University of Toronto's Citizen Lab to enable censorship circumvention. By allowing users to securely bypass content-filtering systems, Psiphon enables human rights activists, political dissidents, and pro-democracy advocates in totalitarian regimes to access the web through allies in countries without Internet censorship. Psiphon is free software, and it uses the encrypted HTTPS protocol to transfer data, enabling users to securely send requests for information to a trusted computer located in another country and receive encrypted information in return. It also allows news organizations, such as the British Broadcasting Corporation, to deliver their content in censored countries.

TrackMeNot uses obfuscation rather than encryption, anonymity, or circumvention to defend against government surveillance and corporate data mining. Developed by tech activists at New York University, TrackMeNot (2001) is a web browser extension that hides web searches in a "stream of decoy queries" (Howe and Nissenbaum 2009). Like other technologies of resistance, TrackMeNot self-consciously integrates values into its design. Such values include "transparency in interface, function, code, and strategy; personal autonomy, where users need not rely on third parties; social protection of privacy with distributed/community-oriented action; minimal resource consumption . . . and usability" (Howe and Nissenbaum 2009, 421). TrackMeNot thus builds on the critical constructivist tradition that regards technology as a site of political contestation. A good example of critical making, TrackMeNot belongs to a "class of technical tools" that helps amplify "social resistance or political voice" (421).

Crabgrass is a technology of resistance that takes a more global view: it is a platform rather than a single-issue software that enables a range of secure online communications. A project of the anarchist tech collective Riseup, Crabgrass facilitates group and network organizing "tailored to the needs of the global justice movement" (About Crabgrass n.d.). Its goal is to provide the activist community with the technical tools needed to create "active, confederal, and directly democratic social change networks" (ibid.). Crabgrass represents a different user experience than commercial social networking, one geared toward community rather than the individual. "We're trying to build tools that reflect more closely our real world experience with how people democratically organize, instead of relying on social networks or on online collaboration tools that . . . actually encode logics that are contrary to the democratic impulse we're trying to foster," explains lead developer Sparrow in a 2008 interview.

Crabgrass's emphasis on secure and democratic communication is inherent in the technical encoding of both the needs and values of activists in the newest social movements. More broadly, Crabgrass seeks to "promote social ownership and democratic control over information, ideas, technology, and the means of communication; empower organizations and individuals to use technology in struggles for liberation [and] to offer support in overcoming the systemic oppression embedded in the use and development of technology" (About Crabgrass n.d.). In this way it invokes the "caring for" practice of reconnecting society and technology inherent in critical making.

Hacking the Social Factory

The need for technologies of resistance seems out of place against the tendency to conceive of the Internet as inherently democratic. This brand of cyber-optimism belies the Internet's origins in the military-industrial complex. It further ignores the Internet's central role in informational capitalism as a locus of social control, as a means of extending capitalist social relations from the material to the immaterial realm. The associated idea that immaterial labor, with its affective, cooperative, and intellectual characteristics, is a potential site of freedom from capitalism rather than its conduit, is attractive. Certainly, this seems to be true of the emancipated labor that typifies FOSS development. Yet the concept of immaterial labor draws from a rich body of theory in the autonomous Marxist tradition, which develops "a subversive counter-interpretation of the information revolution" (Dyer-Witheford 1999, 64). On this view, the Internet, as the central terrain of immaterial labor, is not necessarily or exclusively the "material and ideological heart of informated capital" (Terranova 2000, 39). Both the Internet and immaterial labor are ambivalent; both are spheres of contestation rather than merely accessories to the global project of capital.

Immaterial labor of the sort facilitated by networked computing and the growing importance of information to capitalism gives rise to the social factory. Control of the capitalist labor process as codified in Taylorism, the scientific management of work, is generalized to all of human relations in the form of the social factory. In the bricks-and-mortar factory of Marx's day, labor ceased to be a self-determined activity of species-being and was instead "subsumed under the total process of the machinery itself, as itself only a link of the system, whose unity exists not in the living workers, but rather in the living (active) machinery" (Marx 1973, 693). In the social factory thesis, the dehumanizing machinic relations of the factory not only impose upon society but absorb it fully. Tronti calls this the "process of internal colonization" wherein "the whole of society exists as a function of the factory and the factory extends its exclusive domination over the whole of society" (Tronti, cited in Wright 2002, 37).

It is hackers, according to Wark (2004), who contest the social relations that underwrite capitalism as it has evolved in the age of information. Wark's definition of hacker is expansive, not limited to the world of computing: "Whatever code we hack, be it programming language, poetic language, math or music, curves or colourings, we create the possibility of new things entering the world" (n.p.). It is hackers who are capable of transgressing the alienation of capitalist labor and opposing, through their joyful, creative, collective and subversive labor, the social factory. FOSS as a mode of production inaugurates a new labor process—one based on voluntaristic cooperation, self-determination, and the fulfillment of species-being. It opens up new terrain for a critical remaking of the Internet following a community rather than corporate model (Feenberg and Bakardjieva 2004). At the very least, the FOSS labor process suggests a politics of technological transformation that could reinvent the Internet; at most, it offers an alternative mode of social organization founded on an altogether new set of social relations.

Conclusion: Running Servers for Revolution

Technologies of resistance embody the values inherent in the global justice and Free Software movements and actualize these values in their uptake and use. They belong to the broader tech activist project that is building the digital infrastructure of the global justice movement(s) and, in the process, critically remaking the Internet. This digital infrastructure comprises web applications and platforms that are autonomous and secure, that defend against corporate and state surveillance, and that are designed with the intention of promoting the new social relations of another, better world. In this way, tech activism goes beyond simply using Internet technology toward particular ends to include the appropriation, modification, and transformation of technology itself. "As radical techies, anar(cho)geeks, hacklab members, keyboard squatters, tech-aware activists, autonomous administrators," writes one tech activist, "we've often directly participated in that evolution, advocating subversive uses of new technologies, hacking free software and sharing knowledge with passion, running servers for revolution."[1] Activist-designed and built technologies are therefore disruptive tools that destabilize trends toward a closed, privatized, economically striated, and commercially oriented Internet. By designing software that meets their practical needs and social justice goals, tech activists contribute to the democratization of the Internet. As a "practical means of resistance," this kind of critical making can be deployed in the blind spots inherent in systems of surveillance and social control, where there is always "space to manoeuvre" (Marx 2003, 372). Produced by the free and open source method, their value lies in the reconnection of the social and the technical, offering a challenge and alternative to the alienated social relations of the social factory.

Note

[1] This is taken from the invitation to participate in the People's Global Action Digital Struggles meeting to discuss issues facing radical activists using and developing Internet technology. It is archived at https://lists.aktivix.org/pipermail/aktivix-discuss/2006-June/000941.html.

References

About Crabgrass. n.d. https://we.riseup.net/crabgrass/about.

Anarchist Tech Support (ATS). 2010. *A Short Guide to Setting Up Encrypted Online Communications*. Pamphlet.

Bamford, James. 2008. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. New York: Doubleday.

Castells, Manuel. 2001. The Internet Galaxy: Reflections on the Internet, Business, and Society. New York: Oxford University Press.

Day, R. J. 2005. *Gramsci Is Dead: Anarchist Currents in the Newest Social Movements*. Toronto, ON: Between the Lines.

Deibert, Ron, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. 2008. *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, Ron, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. 2010. *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace*. Cambridge, MA: MIT Press.

Dyer-Witheford, Nick. 1999. *Cyber-Marx: Cycles and Circuits of Struggle in High Technology Capitalism*. Urbana: University of Illinois Press.

Einstein, Albert. 1954/1982. *Ideas and Opinions*. New York: Crown Publishing.

Feenberg, Andrew. 1991. *Critical Theory of Technology*. New York: Oxford University Press.

Feenberg, Andrew. 2002. *Transforming Technology*. Oxford; New York: Oxford University Press.

Feenberg, Andrew, and Maria Bakardjieva. 2004. Consumers or Citizens? The Online Community Debate. In *Community in the Digital Age: Philosophy and Practice*, ed. Andrew Feenberg and Darrin Barney, 1–28. Lanham, MD: Rowman & Littlefield.

Fromm, Erik. 1961. *Marx's Concept of Man*. New York: Continuum.

Henshaw-Plath, Evan. 2008. *TXTMob Gets Subpoenaed: Data Retention in the Surveillance Era*. http://anarchogeek.com/?s=TXtmob.

Himanen, Pekka. 2001. *The Hacker Ethic*. New York: Random House.

Horkheimer, Max. 1982. *Critical Theory: Selected Essays*. New York: Continuum.

Howe, Daniel C., and Helen Nissenbaum. 2009. Resisting Surveillance in Web Search. In *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, ed. Ian Kerr, Valerie Steeves, and Carole Lucock, 417–436. New York: Oxford University Press.

Leistert, O. 2012. Resistance against Cyber-Surveillance Within Social Movements and How Surveillance Adapts. *Surveillance & Society* 9 (4): 441–456.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. New York: Penguin Books.

Lucas, Michael W. 2006. *PGP and GPG: Email for the Practical Paranoid*. San Francisco: No Starch Press.

Marx, Gary T. 2003. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues* 59 (2): 369–390.

Marx, Karl. 1964. *Economic and Philosophic Manuscripts of 1844*. Ed. Dirk J. Struik. Trans Martin Milligan. New York: International Publishers.

Marx, Karl. 1973. *Grundrisse*. Trans. Martin Nicolaus. New York; London: Penguin Books.

Marx, Karl, and Fredrick Engels. 1970. *The German Ideology*. London: Lawrence & Wishart.

Milberry, K., and A. Clement. Forthcoming. Policing as Spectacle and the Politics of Surveillance at the Toronto G20. In *The State on Trial: Policing Protest*, ed. Margaret E. Beare and Nathalie Des Rosiers. Vancouver, BC: UBC Press.

Nelson, T. H. 1987. *Computer Lib: Dream Machines*. Redmond, WA: Tempus Books.

Ratto, Matt. 2009. Critical Making: Conceptual and Material Studies in Technology and Social Life. *Information Society* 27 (4): 252–260.

Raymond, Eric S. 2001. *How to Become a Hacker*. http://www.catb.org/~esr/faqs/hacker-howto.html (accessed November 4, 2009).

Soderberg, J. 2008. *Hacking Capitalism*. New York; London: Routledge.

Sparrow (lead developer, Crabgrass). 2008. Discussion with the author.

Stallman, Richard. 2002. *Free Software, Free Society: Selected Essays of Richard M. Stallman*. Boston, MA: Free Software Foundation.

Terranova, Tiziana. 2000. Free Labor: Producing Culture for the Digital Economy. *Social Text* 18 (2): 33–58.

Torvalds, Linus. 2001. What Makes a Hacker Tick? a.k.a. Linus's Law. In Pekka Himanen, *The Hacker Ethic*, n.p. New York: Random House.

TrackMeNot. 2001. http://cs.nyu.edu/trackmenot/ (accessed December 4, 2012).

Wark, McKenzie. 2004. *A Hacker Manifesto*. Cambridge, MA: Harvard University Press.

Wright, Steve. 2002. *Storming Heaving: Class Composition and Struggle in Italian Autonomist Marxism*. London: Pluto Press.