# Anthropological Theory

**Hacker practice: Moral genres and the cultural articulation of liberalism**

E. Gabriella Coleman and Alex Golub

The online version of this article can be found at:

Published by:
$\circledS$SAGE

**Additional services and information for *Anthropological Theory* can be found at:**

**Email Alerts:** http://ant.sagepub.com/cgi/alerts

**Subscriptions:** http://ant.sagepub.com/subscriptions

**Reprints:** http://www.sagepub.com/journalsReprints.nav
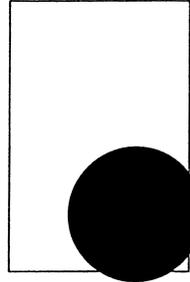
**Permissions:** http://www.sagepub.co.uk/journalsPermissions.nav

# Hacker practice

## Moral genres and the cultural articulation of liberalism

E. Gabriella Coleman
*New York University, USA*

Alex Golub
*University of Hawaii, USA*

### Abstract

Past literature tends towards dichotomous representations of computer hackers as either unhealthy young men engaged in bold tournaments of sinister hacking or visionaries whose utopian technological lifestyle has the potential to disrupt the pathologies of capitalism and modernity more generally. In contrast, this article examines the heterogeneous nature of hacker sociality in order to more adequately portray the complex topography of hacker morality and liberalism. We distinguish between and compare three different, though overlapping, moral expressions of hacking in order to theorize liberalism not as it is traditionally framed – as a coherent body of philosophical, economic, and legal thought or a set of normative precepts and doctrines – but as a cultural sensibility that, in practice, is under constant negotiation and reformulation and replete with points of contention. In doing so, we seek to contribute not only to the ethnographic literature on hacking, but to wider theoretical issues regarding the relationship of culture, morality, liberalism and technology in the contemporary world.

### Key Words

computers • ethics • hackers • law • liberalism • moral genres • technology

> There is no one hacker ethic. Everyone has his own. To say that we all think that same way is preposterous. (Acid Phreak, 1990)

In 1984 Steven Levy published what is now considered to be the classic account of the golden age of hacking, *Hackers: Heroes of the Computer Revolution*. Among a few generations of MIT hackers, Levy found a truly unique and 'daring symbiosis between man and machine' (Levy, 1984: 32) in which hackers elevated the desire to tinker, learn and create technical beauty above all other goals. While Levy defined the hacker ethic in

255

terms of the hacker commitment to information freedom and meritocracy as well as their mistrust of authority, and their firm belief that computers can be the basis for beauty and a better world (1984: 39–46), more recent portrayals of hackers reverse this moral valuation. In the USA today, for instance, hackers are portrayed as young men whose pathological addiction to the internet leads to elaborate deceptions, obsessive quests for knowledge, and bold tournaments of sinister computer break-ins (see Borsook, 2001; Sandberg, 1994; Schwartau, 2000; Shimomura and Markoff, 1996; Slatalla and Quittner, 1995). More recent studies have also reacted against negative stereotypes of hackers by emphasizing instead the original positive connotation of hacking as inquisitive tinkering (Levy, 1984; Turkle, 1984), highlighting the hacker ethic's ability to emancipate its practitioners from the iron cage of late modernity and capitalism (Himanen, 2001; Nissen, 1998; Wark, 2004) and otherwise recuperating hacking's tarnished reputation (Best, 2003; Hannemyr, 1999; Nissenbaum, 2004; Thomas, 2002).

The literature on hackers, thus, tends to collapse hacking into a moral binary in which hackers are either lauded or denounced. This tendency threatens to obscure more than it reveals about the cultural significance of computer hacking. In this article we attempt to move beyond this dichotomous view and argue that in order to understand the ethical diversity as well as the cultural significance of hacking, we must examine how hacker morality in fact exists as multiple, overlapping genres that converge with broader prevailing political and cultural processes, such as those of liberalism.

Although often overlooked, it does not take much to understand the centrality of liberal ideas to hackers. Even a quick gloss of the language that hackers frequently invoke to describe themselves or formulate ethical claims – freedom, free speech, privacy, the individual, meritocracy – discloses liberal imprints and concerns. 'We believe in freedom of speech, the right to explore and learn by doing', explains one hacker editorial 'and the tremendous power of the individual' (*2600*, 1998–1999: 4). Indeed, because of the ways hackers *so visibly yet also so variably* negotiate, transform and critique a wide ambit of liberal precepts in the context of their everyday cultural world, the practices and ethics of computer hacking afford an exceptional entryway for conceptualizing liberalism as a cultural sensibility with diverse and sometimes conflicting strands. In this article, we distinguish between three different, though overlapping, moral expressions of hacking in order to theorize liberalism not as it is traditionally framed – as a coherent body of philosophical, economic and legal thought or a set of normative precepts and doctrines – but as a cultural sensibility closely wedded to what Charles Taylor has called the 'expressive self' (1989) that in practice is under constant negotiation and reformulation and replete with points of contention.

This article begins by first briefly conceptualizing liberalism in explicitly anthropological terms. It then moves into a detailed comparison of three modes of hacker practice – cryptofreedom, free and open source software, and the hacker underground – to demonstrate how, in the words of Acid Phreak quoted in the epigraph, '[t]here is no one hacker ethic'. However, contrary to his stipulation that ethics are simply a matter of individual choice, we will present three moral genres of hacking and the ways hackers reformulate and critique a range of liberal values in the context of their everyday lives. The third section examines how these hacker moral idioms reveal tensions in the liberal tradition even as they all engage and express various facets of the liberal expressive self.

## ANTHROPOLOGIES OF LIBERALISM AND HACKER MORAL GENRES

Recently, a rich body of scholarship has significantly expanded the study of liberalism beyond political theory by attending to the interpenetration between liberal ideals and cultural formations. By examining how ideals of freedom influence the built environment (Joyce, 2003), senses of selfhood and ethical techniques (Rose, 1999), theories of communication, speech and publics (Fish, 1994, 1997; Habermas, 1989; Peters, 2005; Taylor, 2004; Warner, 2002), and theories of rights, tolerance and identity (Brown, 1995, 2006; Marcuse, 1965; Passavant, 2002), these scholars have taken the study of liberalism down important new analytical paths. For all their cogency, however, these works tend to overlook how liberalism is manifest in everyday practice and how these moral orders affect the subjectivities of individuals.

In contrast to most cultural and critical studies of liberalism, we seek a more anthropological focus on the role of practice and diversity both among hackers and within the liberal tradition. The anthropological strand we draw on has incisively studied liberalism in the making by attending to the complex intersection between law, society and multicultural politics. For example, in examining how the law behaves as a privileged site for defining and establishing rights-based frameworks and national constitutions (cf. Collier et al., 1995; Comaroff and Comaroff, 2003; Coombe, 1998; Povinelli, 2002) these works not only demonstrate the social locations where liberal values are defined and adopted, but also reveal the significant cultural and legal impasses that riddle the instantiation of liberal governance. However, while most of the anthropological literature on liberalism has stayed primarily within the purview of multiculturalism or the postcolonial societies (see Kelty, 2005, 2008; Pfaffenberger, 1996; Rapp, 1999 for important exceptions), here we attempt to expand this frame of analysis. To enrich an anthropological account of liberalism in our own societies and in the context of the production of digital media, we must open the lens of investigation wider to examine how liberal ideals are woven into the cultural fabric of everyday life in new, often unexpected contexts, such as those of computer hacking.

To be more specific, we take liberalism to embrace several, sometimes conflicting, historical and present day moral and political sensibilities concerned with a cluster of commitments: protecting property and civil liberties, promoting individual autonomy and tolerance, securing a free press, ruling through limited government and universal law, and preserving a commitment to equal opportunity and meritocracy. These are realized institutionally and culturally in various locations and cultural contexts such as the institutions of higher education, market policies set by transnational institutions, the press and computer hacking. Because liberal ideals always take root in a variety of cultural and institutional contexts and through the action and reactions of social groups, liberal commitments and critiques of liberalism are not only made tangibly manifest in these various contexts but are the very sites for liberalism's heterogeneous articulation and historical transformation.

Regarding hacking and liberalism, hackers discuss freedom and liberty constantly. Indeed, elaborating a sense of what freedom is and what it means to be free *constitutes* moral discourse for hackers (cf. Coleman, 2004; Kelty, 2005, 2008) and shapes what we presented earlier as the hacker ethic. However, while this definition of the hacker ethic may accurately reference a general set of moral commitments still in existence today, the actual articulation of this ethos, we argue, has taken on multiple, though coherent forms.

257

From the global production of free and open source software to the transgressive pranks of underground hacking, hackers reveal their ethical commitments through an *array* of practices and idioms. While these idioms are not reducible to liberal concerns, they are certainly in close conversation with them. Some of their moral visions and technical implementations politically proffer critique by privileging certain liberal principles, for example as is the case of free software, which values speech over intellectual property law. Others speak to the limits of liberal legal regimes, for example, when hackers break the law.

To conceptualize the substantive links between liberalism and the diversity of hacker ethical positions, we find it helpful to draw on Mikhail Bakhtin's theories of speech genres (1986) and heteroglossia (1981). Bakhtin emphasizes that the nature of speech is 'determined by the specific nature of the particular sphere of communication' (1986: 60), and that 'each sphere of activity contains an entire repertoire of speech genres, or relatively stable types or genres of talk' (1986: 60). These genres bespeak types and positions of social actors (scientist, worker, lover, administrator, youth, artist, mother, academic) and can be meaningfully evaluated only by referencing the social norms and material and institutional context in which they arose.

Local speech communities of particular social groups, professions, and generations – what Bakhtin calls heteroglossia – express 'specific points of view on the world' (1981: 291–2). Even while heteroglossia reveals the plurality of social life (1981: 292), local speech forms do not exist completely independent of each other. They cross cut each other in ways that range from the complementary to the contradictory, but always dialogically (1981: 293). Subjectivity, on this account, is not made multiple because of a postmodern condition (though certain conditions may accentuate multiplicity) but because people routinely engage in multiple, overlapping spheres of action in everyday life.

Conceptualizing hacker ethics not as a set of unitary and stable commitments but instead as a constellation of shifting genres similar to speech genres provides a powerful heuristic device. It enables us to analyze hacker ethical codes as replete with overlapping but, nonetheless, variable and sometimes contradictory content, styles, and political effects, without reifying these genres as discrete communities. In other words, hackers move between genres, changing moral registers the way a multilingual speaker switches from one language to another.

Finally, theorizing hacker ethical diversity is analytically significant not simply because it provides a richer account of computer hacking but because it can help us reconceptualize the tradition of liberalism as a heteroglossic one, under constant negotiation, reformation and critique through the very vicissitudes of everyday life. Thus hacking, so often marginalized or misunderstood in popular culture as a sub-cultural group separate from or diametrically opposed to mainstream society, is in fact one crucial location whereby the fractured and cultural character of liberalism is given *new life and visibility* in the digital age.

By simultaneously differentiating what is normally lumped together simply as the 'hacker ethic' into multiple genres and theorizing liberalism as a sensibility revealed variably in the context of computer hacking, in the next two sections we are able to demonstrate two related points. First, we demonstrate how liberalism works as one important context by which hackers make sense of their selves and their world as well as justify the tools they produce. But because of the different, sometimes conflicting,

moral positions that are evident among hackers, we can also discuss the diversity and tensions within both computer hacking *and* liberalism. In keeping with Bakhtin's notion of heteroglossia, in the following we draw on the ethnographic and historical record to present canonical moments, events, technologies and figures out of which three hacker genres have developed.

## HACKER ETHICAL PRACTICE: THREE EXAMPLES

### Crypto-freedom and the politics of technology

Since the late 1970s one kind of hacker practice, crypto-freedom, has taken liberal concerns with freedom and self-reliance and combined them with advances in cryptography to develop technically informed understandings of privacy. The origins of crypto-freedom can be traced back to 1975, when two cryptographers, Whitfield Diffie and Martin Hellman, developed public-key cryptography and created a revolution in encryption science, for public-key encryption allowed its users to send information securely over an insecure channel. It is notable that they developed this technology at a research university (MIT) rather than a government security agency. As a result, the public could potentially now use esoteric cryptographic technology previously available only to government intelligence agencies. Nevertheless, in the 1970s and 1980s the largest growth in the use of encryption technologies came in the corporate sphere, where companies used encryption to secure their ever-growing reliance on computers for financial transactions. Patents on algorithms ensured corporate monopolies and robust encryption was not being developed for personal computers (Levy, 1999; Singh, 2000).

This was the case until 1991, when Phil Zimmerman, an amateur cryptographer, 'freed' encryption by developing a method that could be used on personal computers. The result was not only a robust piece of technology but a risky act of civil dissent, Pretty Good Privacy (PGP), a project whose widespread adoption was, at the time, uncertain at best. As Zimmerman was putting the final touches on PGP, he heard about a pending bill in the Senate to ban cryptography and quickly released his program to the world, with the hope that its popularity would keep the state from outlawing cryptography. Despite the risks, Zimmerman made it his personal mission to put the possibility of privacy via encryption into the hands of anyone who cared to use it. Zimmerman created PGP and encouraged its use by distributing it to friends and colleagues, one of whom posted it on a Usenet discussion group. It was this posting that made PGP available to the world and prompted the FBI's many years of investigation of Zimmerman.

His acts of civil disobedience flew in the face of both intellectual property and national security laws. The state perceived his creation of this piece of encryption technology as a violation of disclosure and transfer of cryptographic software to foreigners opening Zimmerman up to many possible years in jail. In the end, the Federal Government decided not to prosecute Mr Zimmerman (without saying why they dropped the investigation). Within this tumultuous legal context, Zimmerman formulated an explanation of his motivations which is perhaps one of the first clear formulations of the ethic of crypto-freedom:

> If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have good
> access to good cryptographic technology. So do the big arms and drug traffickers. So

259

do defense contractors, oil companies, and other corporate giants. But ordinary people and grass roots political organizations mostly have not had access to affordable 'military grade' public-key cryptographic technology. Until now. PGP empowers people to take privacy into their own hands. There's a growing social need for it. That's why I wrote it. (Zimmerman, 1999: 184)

In this statement, Zimmerman clearly articulates liberal values of individual autonomy and freedom from government interference in the register of cryptography. Although PGP marked a dramatic watershed in the formation of this moral genre, at the time it was only the most visible sign of crypto-freedom's growth.

In 1992, the genre came to maturity with the creation of the Cypherpunks, a loose volunteer association of hackers, programmers, and civil rights advocates united through a mailing list and in-person meetings held in northern California. Cypherpunks work on new privacy technologies and oppose laws that curtail individual privacy. They see themselves as the vanguard of encryption science and their political outlook is a liberal one, but culturally specified because it is rooted in a techno-political response to threats to privacy: 'Cypherpunks write code. They know someone has to write code to defend privacy and since it's their privacy, they are going to write it . . . Cypherpunks know that software can't be destroyed. Cypherpunks know that a widely dispersed system can't be shut down' (Hughes, 1993).

Their confidence in their ability to craft technological solutions to societal problems is wedded to an ethical sensibility that affirms the sacrosanct nature of individual privacy. Like Zimmerman before them, Cypherpunks thus articulate their vision of hacking in a moral idiom that invokes conceptions of individual autonomy, self-reliance, and self-control and applies these liberal concepts to the world of digital information. In doing so they represent a manifestation of a more general American liberal sensibility that distrusts institutionalized authority. This strain of individual self-reliance was identified early in American history by De Tocqueville when he wrote about the peculiarly American character of independence and democracy:

The citizen of the United States is taught from infancy to rely upon his own exertions in order to resist the evils and the difficulties of life; he looks upon the social authority with an eye of mistrust and anxiety, and he claims its assistance only when he is unable to do without it. (De Tocqueville, 1840)

Cypherpunks have reworked, in a new technological idiom, general cultural concerns similar to those that drove De Tocqueville's gentleman farmers.

Nevertheless, Cypherpunks' pessimism regarding the intrusive nature of government and corporations is neither politically Left nor Right – its suspicion of the industrial-military complex falls as easily within the libertarian Right as it does a certain anti-military Left-pacifism. And while some of its most adept practitioners are often libertarian loyalists who hold a faith in free-market capitalism, the loose association of Cypherpunks professes no outward political affiliation. As a result, cryto-freedom practices, groups and events include people with divergent political viewpoints and Cypherpunks are quite clear about this: 'Some of us are anarcho-capitalist radicals . . . others of us are staid Republicans, and still others are Wobblies and other assorted

leftists'.[1] Nonetheless, many do not understand this concern with privacy as radically novel; it is for them an affirmation and continuation of principles deeply held in their culture and expressed in the national constitution.

## Free software and the politics of inversion

While Whitfield Diffie's tenure at MIT was instrumental to his creation of public-key cryptography, other members of the hacking community there later developed a very different take on security. In one era, Diffie was concerned with making multi-user computer systems at MIT secure (Levy, 1999), then Stallman, a short time later, was trying to open them up. Stallman thought the best password was no password. When administrators eventually made passwords mandatory at MIT, Richard Stallman responded with a message that appeared every time a user logged on with a password: 'I see you chose the password [such and such]. I suggest that you switch to the password 'carriage return'. It is much easier to type, and also it stands up to the principle that there should be no password' (Levy, 1984: 417).

Stallman was not necessarily against personal privacy, but when it came to computers and knowledge, he believed that the presence of passwords and copyrighted software at MIT was a corruption of the open access to information on which he had cut his teeth. Stallman treated various barriers designed to impede the creation and spread of knowledge as fundamentally unethical – because he saw them as mechanisms to privatize information in order to allow individuals to profit at the expense of the community. In 1984, he founded the Free Software Foundation in order to further the values of reciprocity, pedagogy and scientific openness he had learned among the MIT hackers and to halt the intrusion of copyrights and patents in software. Stallman was a hacker, and so he realized his liberal ideals in a technological idiom and he linked his political goals to one of the most popular operating systems among the technical community, UNIX. Although the UNIX operating system had become popular in university departments the world over (Lions, 1977; Kelty, 2008; Salus, 1994), it was increasingly inaccessible due to licensing fees. Thus, Stallman set out to write a free version of UNIX, which he called GNU, in order to ensure its eternal availability.

While Zimmerman engaged in an act of civil disobedience and violated the law by writing PGP, Stallman stayed within the law and used it to his own ends. In order to assure his software would remain free in future times, Stallman released it under a license he created, the GNU Public License (GPL). Under this license, Stallman retained copyright in his code but distributed it freely, providing all of its users did so as well. The result was an inversion of traditional copyright law. Through the GPL Stallman used copyright not to enforce a monopoly of his right as an author, but to ensure that software was unable to be monopolized. The result was the creation of a 'safe zone' of publicly available code that could not be privatized by corporate interests, a sort of open space in which Stallman's dream hacker community could work in freedom.

While Cypherpunks embraced a notion of negative freedom, Stallman's GPL derived from a more positive notion of liberty. Through the avenue of licensing and manifestos, Stallman sought to create the technological basis out of which a flourishing hacker community could develop. Instead of deploying a negative understanding of freedom as 'absolute' freedom from coercion, he employed, and thus instantiated, a liberal version of freedom that invoked the virtues of sharing and pedagogy.

261

Thus, although differently configured, Free Software still draws on the same underlying liberal culture as crypto-freedom. By the mid-1990s, Richard Stallman and many other enthusiasts also adopted the liberal terminology of free speech, and it is now ubiquitous to hear some variant of the following phrase among developers to describe the nature of freedom: 'Free software is a matter of liberty, not price. To understand the concept, you should think of free as in free speech, not as in free beer'.[2] This conception of free speech also questions the very purpose of copyright law. By inverting the power of copyright law to create freely available speech rather than the monopoly on expression intended by the Constitution, Stallman planted the seeds of what would become an explosive site of innovation in later years.

While Stallman's impact on software and hacking was the result of a carefully premeditated plan, Linus Torvalds' creation of the Linux operating system was a much more happenstance affair (Torvalds and Diamond, 2001). In 1991, Torvalds released the source code of his hobby project on a mailing list. What no one could have foreseen was that this move would prompt the first successful long-distance, large-scale software collaboration and his project – a free UNIX kernel – was combined with Stallman's GNU software to create what is today known as GNU/Linux. By the mid to late 1990s, advances in information technology facilitated the emergence of free software as a full-blown, technological 'movement'. Now volunteers from across the globe collaborate on thousands of software projects.

By 1998, the free software movement had spawned a variation that came to be known as 'open source software' (OSS). OSS differs from free software in its message, a semantic revaluation tactically used to attract investors. Advocates of OSS such as Eric Raymond argued that open source is a superior 'development model' for making software, in contrast to traditional approaches that used copyrights and patents. OSS, Raymond argued, was not only the right thing to do; it was also the more *efficient* thing to do (1999). OSS's ethical virtues were made manifest in the fact that the enjoyment of programming and the reputation one derived from doing it well were simply better incentives to produce good software than a salary. Raymond's arguments and evangelism have proved effective – today, corporations spend millions of dollars developing and advertising OSS.

Less strongly utopian than free software, OSS is still part of a moral genre whose primary concern is information access. But while Stallman envisioned a community maintained through shared norms and values, OSS harkens back to thinkers of the Scottish Enlightenment such as Mandeville (1995), who argue that public good comes from private vice (see Smith, 1985). On this account, a truly efficient market, like a truly efficient code, would benefit everyone, and the most likely way to get the latter was to insist that the former was in place.

While the political and economic ideology of free and open source software (F/OSS) focuses on liberal values of freedom and efficiency, the lived experience of F/OSS programmers exemplifies different aspects of the liberal tradition. F/OSS hackers often consider themselves to be artists, and see coding as a type of 'diligent craftsmanship' in which they imbue software with a unique element of their creative selves. Software developers construe their technical activity as inherently valuable avenues for highly creative forms of expression, even if they openly admit to various types of worldly and technical constraints. One otherwise shy free software developer, when asked during an

262

ethnographic interview to explain the essence of programming, replied with no hesitation by equating the experience of writing a good piece of software to the joy and awe of making and exploding homemade fireworks:

> It is artistic. It is an art really. I once saw a quote [sic] . . . It was about someone who has a hobby of creating fireworks. So [in the quote] he was explaining to someone what he did: 'It is 3 or 4 months of hard work and a lot of thinking and then one night it all goes up in one beautiful multi-colored fire ball'. But of course you can't imagine what that is like. And the other person replies: 'I do, I am a software developer'. I feel the same way. So, really, it is art.

The result is artisanship in the service of creating useful knowledge, the hallmark of Jeffersonian liberal science (Boorstin, 1948), combined with a romantic drive for self-creative expression and self-cultivation typical of Millian notions of liberty (Donner, 1991; Halliday, 1976; Starr, 2007).

At the same time, it is important to realize that F/OSS developers do not see themselves as 'romantic authors' in the sense, now well-known in the literature, of people entitled to copyright their works because of the way those works uniquely embody their artistic subjectivity (Rose, 1993; Woodmansee, 1994). The lived experience of F/OSS hacking is more populist and communal, and at the core of F/OSS practice is an awareness of connection with a community of developers who make all code possible: the source code of others is easily available for use or reuse; source code repositories, Internet Relay Chat, mailing lists, bug tracking software, and other technical applications facilitate all work; and all the while, your fellow coders are at hand, ready to help when difficulties arise and willing to serve as an attentive audience to view and admire the finished product.

## The underground and the politics of transgression

The final form of hacker practice we will examine here is that of the hacker underground, which asserts that ideals for information access and privacy are in fact simply that, ideals, which can actually never be achieved in an absolute or total sense. Their moral conventions and practices bespeak a Nietzschian notion of power and pleasure, and especially a critique of liberalism (Nietzsche, 1967). In his time, Nietzsche criticized John Stuart Mill's utilitarianism as a secular incarnation of a debased Christian morality whose emphasis on social good and equality sought to enervate the power of the individual. So too does the hacker underground eschew liberal solutions and celebrate and perform the eternal return of power. And just as Nietzsche's attempt to elevate the creative powers of the individual never fully succeeded in definitively escaping the orbit of the Enlightenment's liberal notions, so too, the practice of the hacker underground represents merely a radicalization, rather than a complete break from, the moral claims of liberalism.

Quite distinct from the politics of inversion evident in free software legal techniques, the hacker underground enacts its political critique primarily through transgression. This group envisages hacking as a constant arms race between those with the knowledge and power to erect barriers and those with the equal power, knowledge and especially desire, to disarm them. Bruce Sterling, in his masterful account of the hacker

underground, humorously conveys this dialectic of power in his sardonic 'advice' to young aspiring hackers:

> In my opinion, any teenager enthralled by computers, fascinated by the ins and outs of computer security, and attracted to the lure of specialized forms of knowledge and power would do well to forget all about hacking and set his (or her) sights on becoming a fed. Feds can trump hackers at almost every single thing hackers do, including gathering intelligence, undercover disguise, trashing, phone-tapping, building dossiers, networking, and infiltrating computer systems. (Sterling, 1993: 207)

By dismissing the supposedly more moral ends of law enforcement agencies and focusing on the means that they employ, the hacker underground attempts to defy institutions of consolidated power such as the CIA, FBI, and AT&T (American Telephone & Telegraph), even as it identifies with their desires for control and power. The underground seeks to remind those in power that there are individuals in an unknown, cavernous 'out-there' who *can* and *always will* unsettle, even if only temporarily, the purported absolute power of 'the establishment'. The morality encoded in this form of hacker practice thus values the *process* of piercing through locks, disarming security, accessing the inaccessible, eliminating barriers, and reaching the pot of gold behind the locked door – knowing full well that barriers will always come back in some form.

One of their central and stylized modes of social play, social engineering, distills the aesthetics of eating forbidden fruit into the human art of the short con. Instead of piercing through a technological barricade, humans become the target of play, duped in the search for information. This social engineering is a reinscription of technical control in the realm of human relations. Deceived into handing over some prized piece of data, humans are seen to be just as crackable and manipulable as computers.

The historical roots of the underground lie in the 1960s, and particularly in the Yippies (Youth International Party), who used outlandishly clever and transgressive antics to protest against the Vietnam War. Two hackers, 'Al Bell' and 'Tom Edison', took over the Yippie newsletter *TAP* (Technical Assistance Program) and transformed it into a manual detailing telephony – a genre of technical writing, which exists today in the form of hacker zines such as *Phrack* and *2600* (Thomas, 2002). Shortly thereafter the now-famous hackers and pranksters, such as Captain Crunch and Steven Wozniak, got their hands on a small blue box that emitted a 2600-Hz tone and used it to tap into the phone system and 'phone phreaking' flourished.

Today the hacker underground boasts groups of warez brokers, hackers, and phone phreakers who are all united by a sequestered and secret lifestyle. Personal identity is no more than a handle – the hacker nickname – and hacker gatherings are by invitation only as the following description in 'A day in the life of a warez broker' from *Phrack* Magazine makes clear:

> The ELiTE Community is very secretive, and very secure. No one is let in, and once you're in, you're not expected to leave. There is a lot of trust built in The Community. The only way to get into The ELiTE Community is to know someone who is willing to vouch for you. Without someone to speak of your credibility, you will get no

where. Once you are in and have established yourself, you can pretty much speak for
yourself, or get a sysop to refer you.[3]

Thus, this genre differs from the social organization of F/OSS projects that pride them-
selves in upholding structures of accessibility and transparency. Underground affairs take
place in secret with secured network connections. And not surprisingly, this genre of
hacker practice draws on a sense of individual autonomy and romantic self-expression
similar, though far more accentuated, to what we have seen in F/OSS.

Underground hackers divulge their identities through acts of technical bravado and
thrive on illicit activities. Thus, while underground hackers go to great lengths to protect
their personal identities, they expose their inner thoughts and feelings by publishing
them online in hundreds of entertaining files. Known only as 'textfiles', these documents
leave trails of tasty morsels to offer those on the outside a glimpse of their hacker
interiority:

> He knows he will never get caught. He knows that, in reality, the ever-increasing
> complaints of software manufacturers, and programmers whose wealth and luxury
> are threatened by his actions, are but a reflection on their inability to effectively
> protect their treasures. He knows that if one man can do it, another man can undo
> it. He knows that computers have rules that must be obeyed, and that all bootable
> disks must start the same way. That is enough of a crack for him to get through.[4]

These anonymous autobiographical tales evince the 'pleasures of being watched' and
demonstrate the ways in which hacker practice erupts 'at the interface between surveil-
lance and the evasion of surveillance' (Hebdige, 1997: 403). They are manifestations of
a romantic subjectivity expressing itself, exposing bankrupt dreams of technocracy
derived from the Enlightenment. The manifestos, textfiles, and actions bespeak the thrill
of breaking rules and gaining access to forbidden knowledge not necessarily to make the
world a better place or secure civil liberties, but for its own pleasurable sake. The hackers
who transgress receive overwhelming public and media attention, for in their ability to
play with legal boundaries, the hacker 'personifies an existence beyond the law, an
existence at once awesome, sublime, and awful' (Comaroff and Comaroff, 2004: 807).

Despite confident proclamations of untouchability, the history of this genre is littered
with notorious computer crime cases. In fact, the constant specter of apprehension and
the high-profile prosecution of famous hackers have provided the greatest impetus for
the underground to organize politically (Sterling, 1993; Thomas, 2002), most notably
the legal battles involving Knight Lightning's alleged theft of AT&T E911 documents
in the early 1990s and the government's draconian prosecution of one of the most
famous American hackers of all time, Kevin Mitnick. Many in the hacker community
followed the news of Knight Lightning's ordeal and the string of hacker crackdowns of
the early 1990s, but since they occurred before the widespread use of the internet, protest
mobilization was minimal.

This was not to be the case with Kevin Mitnick. After his fifth arrest for a computer-
related crime in 1989, for one count of computer fraud and one count of possessing
illegal long-distance access codes, he was able to get an unusual plea bargain where he
agreed to one year in prison and six months in a counseling program for his computer

265

'addiction' and was forbidden from touching a computer. After a warrant was put out for his arrest in 1992 for illegally accessing a phone company computer and breaking his parole by associating with one of the people with whom he had originally been arrested in 1981, Mitnick went missing. He was on the FBI's 'Most Wanted' list for two years before they were able to track him down and arrest him in 1995. He was held without bail for over two years before sentencing (thus earning the distinction of being the longest pre-trial detainee in American history prior to 9/11) and in solitary confinement for eight months, supposedly 'in order to prevent a massive nuclear strike from being initiated by me via a prison payphone'.[5] The paranoia and misunderstanding of technology led officials to believe that Mitnick could launch a deadly nuclear strike by whistling into the jail pay phone and thus phreaking his way into NORAD, the North American Aerospace Defense Command Center (Mitnick and Simon, 2002). Although he was unquestionably guilty of many crimes (though he never gained anything financially from his hacks), such as selling proprietary software to competing firms, hackers felt the extreme nature of his punishment was part of a government attempt to send a warning message to the wider community. 'I was the guy pinned up on the cross', Kevin Mitnick told a packed room of hackers a couple of years after his release 'to deter you from hacking'.[6] At the time of his arrest, they did not take this in stride, and responded vigorously by launching a 'Free Kevin' campaign.

Starting in the mid-1990s and continuing until Mitnick's release in January 2002, the Free Kevin movement schooled the hacker underground in new political idioms and activities. The hacker underground supplemented its politics of transgression with traditional forms of political protest that were more public and organized than any that had come before. They marched in the streets, wrote editorials, made documentaries, and began attending the enormously popular 'hacker con' HOPE (Hackers on Planet Earth) – a convention founded in 1994 for publicizing Mitnick's ordeal. In July of 2004, Mitnick, free at last and allowed to use computers again, attended HOPE in NYC for the first time. He delivered his humorous and enticing keynote address to an overflowing crowd of over 2000 hackers, who listened, enraptured, to the man who had commanded their political attention for over a decade. Despite the fact that lawyers and journalists had used Mitnick's case to give hackers a bad name, Mitnick still used the term with pride.

He offered story after story about his clever pranks of hacking from childhood on: 'I think I was born as a hacker because at ten I was fascinated with magic . . . I wanted a bite of the forbidden fruit'. Even as a kid, his victims were a diverse lot: his homeroom teacher, the phone company, and even the LA Rapid Transit District. After he bought the same punch hole device used by bus drivers for punching transfers, he adopted the persona of Robin Hood, spending hours riding the bus network, punching his own pirated transfers to give to customers. He found transfer stubs while dumpster diving, another time honored hacker practice for finding information that was especially popular before the advent of paper shredding. His exploits were always centered on the circumvention of rules and barriers, technical or human. A consuming passion for evasion, gaining access, and exploration would result in many triumphant exploits admired by peers and vilified by the FBI, whose agents, he said, showed 'no sense of humor' when he tried to crack jokes during his arrests. In speaking of his passionate desire to taste forbidden fruit, Mitnick enunciated an ethic of which he was the

paradigmatic figure, and whose organizing power was made manifest in the very occasion of speaking itself.

## HACKER MORAL GENRES, EXPRESSIVE SELFHOOD AND LIBERAL POINTS OF TENSION

There are, then, a wide variety of hacker practices that have been assembled out of a diverse collection of exemplary personalities, institutions, political techniques, critical events, and technologies. These practices are not guided by a singular hacker ethic but are instead rooted in and reveal a number of distinct but intersecting genres of ethical practice. It is evident that some hackers engage freely in illicit file trading, while others do not. Some hackers are oblivious to the legal and technical esoterica of cryptography while others see this as constitutive of their hacker identity. Many hackers are committed to the ethical philosophy of free software, while others feel they have a personal right to deploy intellectual property as they see fit. Some hackers announce with pride their illegal exploits, and others only admit to them reluctantly, a little embarrassed by their foray into the underground. Clearly the material presented here gainsays any attempt to describe hacker practice and ethics as a unitary or homogeneous phenomenon.

Despite this fact, however, it seems clear that important similarities underlie this welter of practice. The themes raised again and again by hackers – free speech, meritocracy, privacy, the power of the individual – suggest that we can read the hacker material as a cultural case in which long-standing liberal ideals are reworked in the context of interaction with technical systems to create a diverse but related set of expressions concerning selfhood, property, privacy, labor, and creativity. In this section, we argue that there is a dialectical relationship between particular technocultural forms and more general cultural structures, which leads hackers to variably implement, reformulate and critique liberal social institutions, legal formulations and ethical precepts even as hacker practice, and especially their senses of expressive selfhood, are precipitated out of them.

Studies of American ideals of freedom and liberty underline the existence of 'romantic individualism' – and its correlate 'utilitararian individualism' (Bellah et al., 1996) – even as American conceptions of freedom have shifted throughout time (Foner, 1999; Starr, 2007). Without reifying an impossibly broad category – 'American Culture' – we argue that it is possible to see the varieties of hacker genres of practice as selective and partial realizations of this model. More broadly, we might combine these approaches with that of Charles Taylor, who has argued that western society in the past 200 years has witnessed the emergence of what he calls the 'expressive self'. Taylor claims that this notion of subjectivity (which is both a folk notion and, as the cultural background for the western academy, also an academic model) rests on three main points. First, that humans are capable of exteriorizing their inner selves through creative action; second, that this action is a deeply moral act; and third, that it is not enough simply for the subject to act, but that its acts must be recognized by others for them to be truly expressive of itself (Taylor, 1989).

All three of these genres represent different ways in which liberal concerns surrounding the expressive self and its social context are distinctly and variably realized. Although all of them capture how interactions with technical systems are moments and places under which hacker subjectivity might be expressed, they also do so in different ways and thus, at the same time, reveal points of tension within liberalism. Whether it be the

self which creates the computer code that secures it from the threat of surveillance, the self whose sharing with the community overrides intellectual property regimes and enables greater recognition within it, or the self which seeks to surpass and dominate technical systems in an act of Nietzschean self-expression, all three of these genres rely heavily on the idea that coding is about the programmer, and that the action of coding is moral; and yet each example also makes tensions in liberalism starkly visible to wider publics.

One classical and recurring question in the liberal tradition, for instance, is the extent to which expansive property rights are coterminous with human freedom. Here the propriety of the self and its autonomy is tied to the idea that freedom is contiguous with and inseparable from an individual's freedom to make contracts, sell their labor, and secure their property (Epstein, 2003; Gray, 2000; Hayek, 1978). In the last two decades this idea has taken its most accentuated expression in neoliberal beliefs and institutions, such as the World Trade Organization (Harvey, 2005), where corporate firms argue that stringent new intellectual property restrictions are indispensable for healthy economic growth and thus for a 'free society' (Braithwaite and Drahos, 2002; Sell, 2003).

The foregoing ethnographic record suggests that hacker practice continues to revolve around the way the self is realized and expressed through property rights, but in a way that is altered by the technocultural core of hacker practice and the wider context of neoliberal property discourses to which it has responded and, in some cases, critiqued. Most notably, free and open source software licenses enable new regimes in which the autonomy of the self is still connected with the use and enjoyment of property, but in these regimes the property is intellectual and the use and enjoyment is enabled through sharing, rather than through a form of 'possessive individualism' (Macpherson, 1962). Free and open source software practice thus not only questions current regimes of copyright and patents but also provides an alternative template for the rearticulation of long-standing ideals of liberal freedom, such as free speech, but in a technocultural mode distinct from previous property regimes (Chopra and Dexter, 2007; Coleman, 2004; Kelty, 2005, 2008; Weber, 2005).

Equally, in the case of the hacker underground, hackers realize themselves in the context of property relations. But in this case, the self is constituted and displayed through the violation of laws which, through enclosure, prevent hackers access to code, software systems, and intellectual property that they desire. Assertions of self in this form of practice come from the violation of property rights and the usurpation of control and use of hacked material, tales of which routinely circulate among hackers. Thus, anonymous tales of hacking indicate the need for recognition, which Taylor's model suggests many hackers deploy to complete their own expressive activity. In this genre of hacker practice, we see how the violation of norms must be both surreptitious and recognized, and that their techniques of transgression also provide a critique of the sanctity of liberal creeds and law.

This issue of recognition leads to another major concern of the expressive self as described by Taylor, the uneasy fit between a world view that emphasizes the creative action of the individual and yet requires validation and recognition from a wider community. For Richard Stallman and many free software developers, for example, the self has the right not only to know but to be known, and the free circulation of

information about and by the hacker is figured not as an intrusion but part of a reciprocal recognition of identities in a larger community in which individuation is both recognized and transcended. Code functions here to simultaneously affirm and erase the boundaries between individuals. Raymond, and open source developers, on the other hand, follow another path in which the invisible hand – the mysterious emergent coordination of action – prevents there being any conflict to one's self-interest that code be shared (Raymond, 1999). Similarly, the hacker underground demands recognition for their exploits – even anonymous recognition – because transgression is the method of self-assertion.

This tension between individualism and collectivism opens a window into another long-standing liberal tension between what Isaiah Berlin has identified as the difference between positive and negative freedom (2001). Many authors have emphasized that individual freedom and self-autonomy are central concerns of liberalism (Dumont, 1986; Macpherson, 1962); nonetheless, the grounding of this freedom is often understood in quite different terms. More libertarian thinkers (Epstein, 2003; Hayek, 1978) have conceptualized liberal freedom 'negatively' as an absence of coercion. Thus Wendy Brown rightly notes that liberal freedom often operates 'as a relational and contextual practice that takes shape in opposition to whatever is locally and ideologically conceived as unfreedom' (1995: 6).

Other strains of liberalism in political theory, among hackers, and other internet enthusiasts, however, focus on positive liberty as a precondition for self-development and human flourishing. Though Berlin (2001) argues that seminal thinkers, such as John Stuart Mill, formulate a negative conception of liberty, it is clear that Mill, influenced by the Romantic tradition (Halliday, 1976), defines the free individual as one who develops, determines, and changes his own desires and interests autonomously through self-expression, debate and reasoned deliberation (Donner, 1991; Peters, 2005). Following this vein of liberal thinking, in the American context, John Dewey most famously elevates 'the ultimate responsibility' of liberalism to be 'education, in the broadest sense of that term' (1935: 58). We might associate this line of thought with a more communitarian approach or one which understands freedom as cultivation or self-development (Mulhall, 1996; Sen, 2000). Traditionally, within liberal nation-states across the world, the most prominent practical institutional articulation of this commitment is to be found in the public and higher education system – an infrastructure of ostensible equal access meant to enable a meritocratic order and support the cultivation of an educated citizenry.

Again, we can see how this tension plays out in the different genres of hacker practice mentioned earlier, revealing the continued oscillation and expression between positive and negative freedom today within the interplay between cultural practice and technological systems. An approach to negative freedom which emphasizes the autonomy of the individual is certainly evident among some hackers, which is why a number of their critics have so often accused hacking of being a virulent strain of 'technolibertarianism gone feral' (Borsook, 2001: 91; Lovink, 2008). Even within the F/OSS community, for instance, some prefer more libertarian free software licenses such as the Berkeley Software Distribution (BSD), which eliminates the 'coercion' of the more communitarian licenses such as the GPL and centralizes individual choice over community rights (Chopra and Dexter, 2007).

269

Equally, among Cypherpunks, the gaze of the other – and particularly of powerful institutions – is seen as corrosive to the autonomy of the subject. Privacy, that is to say, control of the intimate knowledge of a subject's interiority, must be protected. And finally, hackers often playfully but sternly quip that others must RTFM (Read the Fucking Manual), which pushes those asking for help to adopt and perform techniques of self-reliance. In all of these cases, elevating the sacrosanct nature of the self-reliant individual and expressing deep distrust of authority or centralized government, hackers have remade these broader maxims of negative freedom into cultural reality by inscribing them in a variety of material and semiotic artifacts.

That said, the emphasis on the 'technolibertarian' or 'Byronic' nature of hacker practice made by some authors should not be overstressed. Much of hacker practice focuses on a far more positive conception of liberty. Manuals, after all, have been written by someone who has shared them so that others might learn. And indeed, in the sphere of F/OSS we see a subtle dialectic of recognition and identity under which a more positive notion of freedom has been visibly elevated and cultivated.

For example, in the span of a decade, F/OSS hackers have implemented a set of liberal principles that posit a direct relationship between self-cultivation, education, meritocracy and a healthy public sphere. Unlike the meritocracy of capitalism, which sanctions the privatization of self-made value, the hacker implementation of meritocracy – however imperfect and entwined with other modes of governance – seeks to constantly equalize the conditions for self-cultivation. Within the domain F/OSS, personally-crafted value, such as source code and documentation, is fed back and circulated among peers, contributing to an endowed and growing pool of resources through which other hackers can constantly engage in their asymptotic process of technical self-cultivation. As part of this, they have remade a Millian-inspired liberal language of free speech their own. 'The right to create software is seen in a similar light as the right to state an opinion', explains Chris Kelty. 'If your opinion (software implementation) is heard, critiqued, refined and reasserted – just as Mill proposed – then the best (the truest) opinion will win out' (2005: 187). These types of liberal conceptualizations ground their production of technology as a form of imaginative expression that ensures technical progress and should never be subject to limitations and barriers.

## CONCLUSION

New information technologies, notably the internet, have become a privileged site for projecting the aspirations of liberal society. Nowhere today are the battles over control, freedom, access and privacy more clearly thematized than on the internet (Fischer, 1999; Gillespie, 2007; Holmes, 2008). A virtual space of innovative collaborative production, communitarian sociality and play, and high-tech networked activism (Castells, 1996, 2001; Danet, 2001; Escobar, 2000; Kirshenblatt-Gimblett, 1996; Rheingold, 1993), the internet's commercial turn in the mid-1990s also opened it to the vast workings of finance capital, the service industry and consumer capitalism (Robins and Webster, 1999; Schiller, 2000; Terranova, 2000).

Many Americans are entangled in and, at least partially, aware of this contemporary situation. But hackers experience these same problems and contradictions of the information age more directly because they live and express this tension through the peculiar lifeblood of their cultural world, computing and communications technologies.

Consequently, studying hackers is an ideal way to bring 'into sharp juxtaposition the contradictory elements of cyberspace's political economy, cultural elaborations, liberating and subjugating potentials, new informational-based sciences, [and] alternative engineering designs' (Fischer, 1999: 247).

Hacker practice is at the center of these debates, experientially and theoretically, because technology is not a means to an end for hackers, it is central to their sense of self – making and using technology is how hackers individually create and how they socially make and reproduce themselves. Through regular and shared routine practices of their ordinary, technical life, which are not fully or always available to conscious reflection, hackers come to collectively embody evaluative moral and aesthetic dispositions in which knowledge is sacred territory; access to and personal control over the means of information creation and circulation is valued as essential; and technical activity is often experienced as the vehicle for self-fashioning and creative self-expression. These unwritten codes of morality, while emerging from cultural action, draw from and tie into broader value systems so that for 'the hacker, the computer begins to reveal itself as the means to realize our highest cultural values: independence, freedom, and education' (Thomas, 2002: 76).

Even as hackers reveal and rework dominant cultural values, the ethnographic and historical record, however, demonstrates that they do so by producing a mosaic of ethical positions which hackers move through and between. And it is this fluidity that expresses one of the more palpable ironies of hacker morality. While much of hacker ethical discourse draws from and reformulates liberal commitments, hackers embody a form of subjectivity and formulate an implicit politics often denied by liberal theory; they align more closely to the flexible subjectivities and poetic politics identified by theorists as notable characteristics of the postcolonial experience (Bhabha, 1994; Gilroy, 1993; Ortiz, 1995).

Conceptualizing hacker ethics as a constellation of genres, as we have done here, provides a powerful heuristic device. Rather than focus our attention on a putatively homogeneous set of norms, values, and practices among hackers or within the liberal tradition, such an approach enables us to simultaneously analyze the interconnected heterogeneity of hacker ethical codes as well as those of liberalism. We have defined hacker morality as a related but diverse repertoire of moral genres that variably realize and critique the concerns and contradictions of the wider liberal culture in which hacking is situated and yet reveal consistent concerns with the liberal expressive self.

This article has stayed within the scope of the American and Anglo-European liberal tradition and has examined only hacking in the USA. A wider-ranging study would require an analysis of the ways computer hacking runs against the grain of liberal logics as well as a comparative study of hacker culture globally.[7] In the last few years, for example, the explosion of leftist and anarchist politics critical of economic globalization has attracted hacker sympathies (Coleman, 2005a; Riemens, 2004). Examining how the semiotic logics of technology cross-cut with political ideologies such as liberalism and anarchism to inform hacker ethics provides an opportunity to expand the study of hacker ethics as well as explore the places in which the lines between liberal and anarchist tenets come together and diverge in the political and technical sphere.

As we have shown, hacker practice makes visible socially relevant questions to those interested in the legal politics of information access. Its answers take shape in an array

of implicit and explicit political actions and artifacts: bold manifestos, taunting games, routine technical publications, and novel legal agreements. Increasingly today lawyers, academics and policy makers have begun to scrutinize the living practice of the people who most acutely feel the force of these questions when formulating their own approaches to law, economics, and policy (Benkler, 2006; Bollier, 2002; Lessig, 1999, 2001; Vaidhyanathan, 2001, 2004). Because their lifestyles push the envelope of what is both technically possible and legally allowable, hacker moral visions not only reveal broader contradictions but at times offer a critical perspective and tangible alternatives to current ethical dilemmas in the digital landscape (Galloway, 2004; Nissenbaum, 2004; Wark, 2004). Ranging from new, legal software licenses to illegal acts of digital transgression, hackers are already thinking through and envisioning alternatives that will be central to debates about possible digital futures.

## Acknowledgements

## Notes
1 See http://swissnet.ai.mit.edu/6805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ (accessed September 2007).
2 http://www.gnu.org/philosophy/free-sw.html (accessed May 2008).
3 http://www.phrack.org/issues.html?issue=47&id=20#article (accessed 15 April 2006).
4 'Anatomy of a Pirate', at http://www.textfiles.com/piracy/anatomy.txt (accessed 25 July 2004).
5 http://encyclozine.com/Kevin_Mitnick (accessed September 2007).
6 Keynote speech delivered at Hackers on Planet Earth (HOPE) in New York City on 9 July 2004.
7 To be clear, computer hacking in the USA or abroad cannot be simply reduced to a liberal framework. Elsewhere I have discussed the pleasures of hacking in terms of jouissance to demonstrate how hacking deviates from, and at times even undermines, liberal grammars (Coleman, 2005b). However, the focus of this article has been narrower: to start making connections between hacking and liberalism as a way to conceptualize the culturally coherent though heterogeneous nature of both.

## References
2600 (1998–1999) 'The Victor Spoiled' (Editorial), 2600: The Hacker Quarterly (winter): 3–4.
Acid Phreak (1990) Quoted in Jack Hitt and Paul Tough, 'Is Computer Hacking a Crime?', Harpers Magazine (March): 48.
Bakhtin, Mikhail (1981) The Dialogic Imagination. Austin: University of Texas Press.
Bakhtin, Mikhail (1986) Speech Genres and Other Late Essays. Austin: University of Texas Press.
Bellah, Robert, Richard Madsen, William Sullivan and Ann Swidler (1996) Habits of the Heart: Individualism and Commitment in American Life. Berkeley: University of California Press.

Benkler, Yochai (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press.

Berlin, Isaiah (2001) *Roots of Romanticism*. Princeton, NJ: Princeton University Press.

Best, Kirsty (2003) 'The Hacker's Challenge: Active Access to Information, Visceral Democracy, and Discursive Practice', *Social Semiotics* (13)3: 263–82.

Bhabha, Homi (1994) *The Location of Culture*. New York and London: Routledge.

Bollier, David (2002) *Silent Theft: The Private Plunder of Our Common Wealth*. New York: Routledge.

Boorstin, Daniel (1948) *The Lost World of Thomas Jefferson*. New York: H. Holt.

Borsook, Paulina (2001) *Cyberselfish: A Critical Romp through the Terribly Libertarian Culture of High Tech*. New York: Public Affairs.

Braithwaite, John and Peter Drahos (2002) *Information Feudalism: Who Owns the Knowledge Economy*. New York: New Press.

Brown, Wendy (1995) *States of Injury: Power and Freedom*. Princeton, NJ: Princeton University Press.

Brown, Wendy (2006) *Regulating Aversion: Tolerance in the Age of Identity and Empire*. Princeton, NJ: Princeton University Press.

Castells, Manuel (1996) *The Rise of the Network Society*. Oxford: Blackwell.

Castells, Manuel (2001) *The Internet Galaxy: Reflections on Internet, Business, and Society*. Oxford: Oxford University Press.

Chopra, Samir and Scott Dexter (2007) *Decoding Liberation: The Promise of Free and Open Source Software*. New York and London: Routledge.

Coleman, E. Gabriella (2004) 'The Political Agnosticism of Free and Open Source Software and the Inadvertent Politics of Contrast', *Anthropological Quarterly* 77(3): 507–19.

Coleman, E. Gabriella (2005a) 'Les temps d'Indymedia', *Multitudes* 21: 41–8.

Coleman, E. Gabriella (2005b) 'The Social Construction of Freedom in Free and Open Source Software: Hackers, Ethics, and the Liberal Tradition', PhD Dissertation, Department of Anthropology, University of Chicago.

Collier, Jane, Bill Maurer and Liliana Suarez-Navaz (1995) 'Sanctioned Identities: Legal Constructions of Modern Personhood', *Identities* 2 (1–2): 1–27.

Comaroff, Jean and John Comaroff (2003) 'Reflections on Liberalism, Policulturalism, and ID-ology: Citizenship and Difference in South Africa', *Social Identities* 9(3): 445–74.

Comaroff, Jean and John Comaroff (2004) 'Criminal Obsessions, after Foucault: Postcoloniality, Policing, and the Metaphysics of Disorder', *Critical Inquiry* 30(4): 800–24.

Coombe, Rosemary (1998) *The Cultural Life of Intellectual Properties: Authorship, Appropriation and the Law*. Durham, NC: Duke University Press.

Danet, Brenda (2001) *Cyberplay: Communicating Online*. Oxford: Berg.

Dewey, John (1935) *Liberalism and Social Action*. New York: G.P. Putnam's Sons.

De Tocqueville, Alexander (1840) 'Political Associations in the United States', in Alexander de Tocqueville *Democracy in the United States*, URL (accessed 3 August 2004) http://xroads.virginia.edu/~HYPER/DETOC/1_ch12.htm

Donner, Wendy (1991) *The Liberal Self: John Stuart Mill's Moral and Political Philosophy*. Ithaca, NY: Cornell University Press.

Dumont, Louis (1986) *Essays on Individualism: Modern Ideology in Anthropological Perspective*. Chicago, IL: University of Chicago Press.

Epstein, Richard (2003) *Skepticism and Freedom: A Modern Case for Classical Liberalism*. Chicago, IL: University of Chicago Press.

Escobar, Arturo (2000) 'Welcome to Cyberia: Notes on the Anthropology of Cyberculture', in Daniel Bell and Barbara Kennedy (eds) *The Cybercultures Reader*, pp. 56–76. New York: Routledge.

Fischer, Michael J. (1999) 'Worlding Cyberspace: Towards a Crucial Ethnography in Time, Space, Theory', in George Marcus (ed.) *Critical Anthropology Now: Unexpected Context, Shifting Constituencies, Changing Agendas*, pp. 245–304. Santa Fe, NM: SAR Press.

Fish, Stanley (1994) *There's No Such Thing As Free Speech: And It's a Good Thing, Too.* Oxford: Oxford University Press.

Fish, Stanley (1997) 'Boutique Multiculturalism, or Why Liberals are Incapable of Thinking About Hate Speech', *Critical Inquiry* 23(2): 387–95.

Foner, Eric (1999) *The Story of American Freedom.* New York: W.W. Norton.

Galloway, Alexander (2004) *Protocol: How Control Exists after Decentralization.* Cambridge, MA: MIT Press.

Gillespie, Tarleton (2007) *Wired Shut: Copyright and the Digital Shape of Culture.* Cambridge, MA: MIT Press.

Gilroy, Paul (1993) *The Black Atlantic: Modernity and Double Consciousness.* Cambridge, MA: Harvard University Press.

Gray, John (2000) *The Two Faces of Liberalism.* New York: The New Press.

Habermas, Jürgen (1989) *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society.* Cambridge, MA: MIT Press.

Halliday, R.J. (1976) *John Stuart Mill*. New York: Routledge.

Hannemyr, Gisle (1999) 'Technology and Pleasure: Considering Hacking Constructive', *First Monday* (4)2, URL (accessed May 2008): http://www.firstmonday.dk/issues/issue4_2/gisle/index.html

Harvey, David (2005) *A Brief History of Neoliberalism.* Oxford: Oxford University Press.

Hayek, F.A. (1978) *The Constitution of Liberty*. Chicago, IL: University of Chicago Press.

Hebdige, Dick (1997) 'Posing . . . Threats, Striking . . . Poses', in Ken Gelder and Sarah Thorton (eds) *The Subcultures Reader*, pp. 393–405. New York and London: Routledge.

Himanen, Pekka (2001) *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House.

Holmes, Brian (2008) *Unleashing the Collective Phantoms: Essays in Reverse Imagineering*. New York: Autonomedia.

http://encyclozine (n.d.) URL (accessed September 2007); http://encyclozine.com/Kevin_Mitnick

http://swissnet (n.d.) URL (accessed September 2007); http://swissnet.ai.mit.edu/6805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ

http://www.gnu (n.d.) URL (accessed May 2008); http://www.gnu.org/philosophy/free-sw.html

http://www.phrack (n.d.) URL (accessed 15 April 2006); http://www.phrack.org/ issues.html?issue=47&id=20#article

http://www.textfiles (n.d.) 'Anatomy of a Pirate', URL (accessed 25 July 2004); http://www.textfiles.com/piracy/anatomy.txt

Hughes, Eric (1993) 'A Cypherpunk's Manifesto', URL (accessed 3 August 2004): http://www.activism.net/cypherpunk/manifesto.html

Joyce, Patrick (2003) *The Rule of Freedom: Liberalism and the Modern City*. New York and London: Verso.

Kelty, Chris (2005) 'Geeks, Social Imaginaries, and Recursive Publics', *Cultural Anthropology* (20)2: 185–214.

Kelty, Chris (2008) *Two Bits: The Cultural Significance of Free Software*. Durham, NC: Duke University Press.

Kirshenblatt-Gimblett, Barbara (1996) 'The Electronic Vernacular', in George Marcus (ed.) *Connected: Engagements with Media*, pp. 21–65. Chicago, IL: University of Chicago Press.

Lessig, Lawrence (1999) *Code and Other Laws of Cyberspace*. New York: Perseus Books.

Lessig, Lawrence (2001) *The Future of Ideas: The Fate of the Commons in a Connected World*. New York: Random House.

Levy, Steven (1984) *Hackers: Heroes of the Computer Revolution*. New York: Delta.

Levy, Steven (1999) *Crypto: How the Code Rebels Beat the Government: Saving Privacy in the Digital Age*. New York: Viking.

Lions, John (1977) *Lions' Commentary on UNIX 6th Edition*. San Jose, CA: Peer-to-Peer Communications.

Lovink, Geert (2008) *Zero Comments: Blogging and Critical Internet Culture*. New York and London: Routledge.

Macpherson, C.B. (1962) *The Political Theory of Possessive Individualism: Hobbes to Locke*. Oxford: Clarendon Press.

Mandeville, Bernard (1995) 'Fable of the Bees', in Bernard Mandeville, *Fable of the Bees: or Private Vices, Publick Benefits* (edited by F.B. Kaye). Indianapolis, IN: Liberty Fund.

Marcuse, Herbert (1965) 'Repressive Tolerance', in Herbert Marcuse *A Critique of Pure Tolerance*, pp. 95–137. Boston, MA: Beacon Press.

Mitnick, Kevin and William Simon (2002) *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN: Wiley.

Mulhall, Stephen (1996) *Liberals and Communitarians: A Revised Edition*. New York: Blackwell.

Nietzsche, Friedrich (1967) *On the Genealogy of Morals*. New York: Vintage Books.

Nissen, Jorgen (1998) 'Hackers: Masters of Modernity and Modern Technology', in Julian Stefton-Green (ed.) *Digital Diversions: Youth Culture in the Age of Multimedia*, pp. 149–71. London: University College London.

Nissenbaum, Helen (2004) 'Hackers and the Contested Ontology of Cyberspace', *New Media and Society* (6)2: 195–217.

Ortiz, Fernando (1995) *Cuban Counterpoint: Tobacco and Sugar*. Durham, NC: Duke University Press.

Passavant, Paul (2002) *No Escape: Freedom of Speech and the Paradox of Rights*. New York and London: New York University Press.

Peters, John Durham (2005) *Courting the Abyss: Free Speech and the Liberal Tradition*. Chicago, IL: University of Chicago Press.

Pfaffenberger, Bryan (1996) 'If I Want It, It's OK: Usenet and the (Outer) Limits of Free Speech', *The Information Society* 12(4): 365–86.

Povinelli, Elizabeth (2002) *The Cunning of Recognition: Indigenous Alterities and the Making of Australian Multiculturalism*. Durham, NC: Duke University Press.

Rapp, Rayna (1999) *Testing Women, Testing the Fetus: The Social Impact of Amniocentesis in America*. New York and London: Routledge.

Raymond, Eric S. (1999) *The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Sebastopol, CA: O'Reilly.

Rheingold, Howard (1993) *The Virtual Community: Homesteading on the Electronic Frontier*. New York: Harper Perennial.

Riemens, Patrice (2004) *Transhack Meeting*, available at URL (accessed May 2008): http://greenpeppermagazine.org/process/tiki-index.php?page=transhackmeeting

Robins, Kevin and Frank Webster (1999) *Times of the Technoculture: From the Information Society to the Virtual Life*. London and New York: Routledge.

Rose, Michael (1993) *Authors and Owners: The Invention of Copyright*. Cambridge, MA: Harvard University Press.

Rose, Nikolas (1999) *Powers of Freedom: Reframing Political Thought*. Cambridge: Cambridge University Press.

Salus, Peter (1994) *A Quarter Century of Unix*. New York: Addison-Wesley.

Sandberg, Jared (1994) 'Hackers Take Revenge on the Author of New Book on Cyberspace Wars', *Wall Street Journal* 5 December: B5.

Schiller, Dan (2000) *Digital Capitalism: Networking the Global Market System*. Cambridge, MA: MIT Press.

Schwartau, Winn (2000) *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists, and Weapons of Mass Disruption*. New York: Thunder's Mouth Press.

Sell, Susan (2003) *Private Power, Public Law: The Globalization of Intellectual Property Rights*. Cambridge: Cambridge University Press.

Sen, Amartya (2000) *Development as Freedom*. New York: Anchor Press.

Shimomura, Tsutomu and John Markoff (1996) *Takedown: The Pursuit and Capture of America's Most Wanted Computer Outlaw*. New York: Hyperion.

Singh, Simon (2000) *The Code Book: The Secret History of Codes and Code-Breaking*. London: Fourth Estate Limited.

Slatalla, Michelle and Joshua Quittner (1995) *Masters of Deception: The Gang that Ruled Cyberspace*. New York: Harper Collins.

Smith, Adam (1985) *An Inquiry into the Nature and Causes of the Wealth of Nations*. New York: Modern Library.

Starr, Paul (2007) *Freedom's Power: The True Force of Liberalism*. New York: Perseus Books Group.

Sterling, Bruce (1993) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam.

Taylor, Charles (1989) *Sources of the Self: The Making of Modern Identity*. Cambridge, MA: Harvard University Press.

Taylor, Charles (2004) *Modern Social Imaginaries*. Durham, NC: Duke University Press.

Terranova, Tiziana (2000) 'Free Labor: Producing Culture for the Global Economy', *Social Text* 18(2): 33–57.

Thomas, Douglas (2002) *Hacker Culture*. Minneapolis: University of Minnesota Press.

Torvalds, Linus and David Diamond (2001) *Just for Fun: The Story of an Accidental Revolution*. New York: Harper Business Press.

Turkle, Sherry (1984) *The Second Self: Computers and the Human Spirit*. New York: Simon and Schuster.

Vaidhyanathan, Siva (2001) *Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity*. New York: New York University Press.

Vaidhyanathan, Siva (2004) *The Anarchist in the Library*. New York: Basic Books.

Wark, Mackenzie (2004) *A Hacker Manifesto*. Cambridge, MA: Harvard University Press.

Warner, Michael (2002) *Publics and Counterpublics*. New York: Zone Books.

Weber, Steven (2005) *The Success of Open Source*. Cambridge, MA: Harvard University Press.

Woodmansee, Martha (1994) *The Author, Art, and the Market: Rereading the History of Aesthetics*. New York: Columbia University Press.

Zimmerman, Phil (1999) 'How PGP Works/Why Do You Need PGP?', in Peter Ludlow (ed.) *High Noon on the Electronic Frontier*, pp. 179–84. Cambridge, MA: MIT Press.

E. GABRIELLA COLEMAN is an assistant professor in the Department of Media, Culture, and Communication at New York University. Her work examines the role of the law and new media technologies in extending and critiquing liberal values and sustaining new forms of political activism. She has conducted most of her anthropological research on the ethics and politics of free and open source software production and has also started a new project on patient activism on the internet. *Address*: 239 Greene Street, 7th floor, New York University, Deptartment of Media, Culture, and Communication, NY, NY 10003, USA. [email: biella@nyu.edu]

ALEX GOLUB is an assistant professor of anthropology at the University of Hawaii at Manoa. His dissertation research focused on mining and indigenous people in Papua New Guinea. His more recent research focuses on digital genres such as video games, blogs, and the Wikipedia. *Address*: Social Science Department, University of Hawaii, 2550 Campus Road, Honolulu, HI 96822, USA.