

# HACKER

(Forthcoming, The Johns Hopkins Encyclopedia of Digital Textuality)

E. Gabriella Coleman

## *Introduction*

Generally, a hacker is a technologist with a penchant for computing and a hack is a clever technical solution arrived at through non-obvious means (Levy 1984, Turkle 2005). It is telling that a hack, as defined by the *Hacker Jargon File*, can mean the complete opposite of an ingenious intervention: a clunky, ugly fix, that nevertheless completes the job at hand. Among hackers, the term is often worn as a badge of honor. In the popular press, however, the connotations of 'hacker' are often negative, or at minimum refer to illegal intrusion of computer systems. These differences point to the various meanings and histories associated with the terms hacker and hacking.

Hackers tend to uphold a cluster of values: freedom, privacy, and access. They adore computers and networks. They are trained in the specialized—and economically lucrative—technical arts of programming, system/network administration and security. Some gain unauthorized access to technologies (though much hacking is legal). Foremost, hacking, in its different incarnations, embodies an aesthetic where craftsmanship and craftiness converge; hackers value playfulness, pranking and cleverness, and will frequently display their wit through source code, humor, or both. But once one confronts hacking historically and sociologically, this shared plane melts into a sea of differences that have, until recently, been overlooked in the literature on hacking (Coleman and Golub 2008, Jordan 2008).

## *Rethinking the Story of the Hacker Ethic, from Single-Origin to Multiple Origins*

The term hacker was first used consistently in the 1960s among technologists at MIT whose lives maniacally revolved around making, using and improving computer software—a preoccupation that Steven Levy dubbed “a daring symbiosis between man and machine” in his engaging 1984 account *Hackers: Heroes of the Computer Revolution* (1984: 39). Levy unbundled the groups’ unstated ethical codes from their passionate, everyday collective pursuits and conceptualized them as “the hacker ethic,” shorthand for a mix of aesthetic and pragmatic imperatives that included: commitment to information freedom, mistrust of authority, heightened dedication to meritocracy and the firm belief that computers can be the basis for beauty and a better world (1984: 39-46). Levy’s book not only represented what had been, at the time, an esoteric community but also inspired others to identify with the moniker “hacker” and its ethical principles.

By the 1980s, many other technologists routinely deployed the term “hacker,” individuals enthralled with tinkering and technical spelunking but whose history and politics were distinct from those chronicled by Levy. Sometimes referred to as the “hacker underground,” the story goes that they arose in the 1980s, sullyng what had been a pristine and legal tradition. What is often overlooked is their history: their heirs are the phone phreaks who existed at the same time as the first crop of university hackers in the late 1950s and early 1960s. These phreaks, as they were eventually known, tapped into the phone system to make free phone calls, explored 'The System,' and found each other on phone conferences also known as party lines (Sterling 1992, Rosenbaum 1971, Thomas 2003).

The end of the analog phone network after the divestiture of “Ma Bell” heralded the end of the golden age of phreaking, which was largely replaced with the exploration of computer networks. The marriage between phreaking and computer hacking was represented in the popular e-zine *Phrack*, first published in 1985 on Bulletin Boards Systems, where hackers of all kinds congregated (Scott 2005, Sterling 1992, Thomas 2002). Hackers in this vein would continue to publish prolifically in diverse genres, including manifestos (most famously “The Conscience of a Hacker”), textfiles (written in sparse ASCII text but often filled with ASCII art, audaciously worded l content) and zines (such as *Hack-Tic* in the Netherlands and *2600* in the United States). By the 1990s, they were routinely meeting during annual hacker “cons” (Coleman 2010). Although many of these underground hackers engaged in technical exploration, often scouting for security vulnerabilities they also sought forbidden fruit and their actions included mockery, spectacle, and transgression—a politics and ethics distinct from the university hackers of MIT, Carnegie Mellon, and Stanford (although there was plenty of pranking and irreverence among these hackers).

The canonical narrative identifying MIT as hackings’ first homeland—a place where the hacker ethic was born—is complicated when we account for other traditions such as phreaking, which existed independently of university-based hacker communities, and shaped a subversive tradition that flourished in the 1980s and 1990s, only to change with the rise of the security industry and new laws criminalizing computer break-ins. Instead of locating a single point of origin for hacking, we should be attentive to multiple origins, distinct lineages and variable ethics.

### *The Politics of Naming*

By the late 1980s, although various instances of hacking existed, this more subversive tradition became *the* public face of hacking, cemented, and sometimes distorted by, media accounts. Some hackers, concerned by the illicit actions of other hackers and negative, sensationalist media portrayals, started to call those who hacked for illegal or malicious purposes, “crackers” (Nissenbaum 2004). The use of “cracker” was a linguistic attempt to reclaim and sanitize “hacker.” Unsurprisingly, many hackers also questioned the term. As more automation tools became available, many also started to use the derogatory terms “script kiddies” to designate those who use scripts to circumvent computer security or deface websites, rather than finding a unique compromise. It is a scornful term (no one would elect to self-designate as such) that demarcates boundaries, signals appropriate behavior, and gives voice to the value placed on ingenuity, inventiveness and self-sufficiency.

To this day, debate rages among technologists: who deserves the title of “hacker”? What constitutes its parameters? Some readily accept variability, while others starkly demarcate borders. When asked, many are ready to fire off definitions. When interviewed, two hackers distinguished between *builders*—often found in free and open source communities whose lineage goes back to the university communities explored in Levy—and *breakers* with whom these hackers identify. They define breakers as follows:

Di: I call myself a hacker, what I mean is that I apply creativity and technical knowledge to bypassing defenses.

Da : Yeah I've heard 'obtaining lower level understanding of a system to bypass systems'... which is a reasonable definition.

### *Genres of Hacking*

To hackers themselves, “to hack” can thus mean distinct activities, from improving the Linux operating system to finding vulnerabilities and “fuzzing” for exploits. Some distinctions are subtle, while others are profound enough to warrant thinking about hacking in terms of genres with distinct aesthetics and histories (Coleman and Golub 2008). Free and Open Source hackers — those that have used legal means to guarantee perpetual access to source code—tend to uphold political structures of transparency (Coleman 2012c). In contrast, the hacker underground is more opaque in its social organization (Thomas 2003). These hackers have made secrecy and spectacle into a high art form (Coleman 2012b). For decades in Europe, artistic practice has been marshaled for the sake of hackings (Bazzichelli 2008, Deseriis and Marano 2008). Hardware hacking has also been part of hacking for a long time. Historically, its most notable manifestation was among the Homebrew hackers of the Bay Area who hacked one of the first personal computer kits, the MITS Altair 8800, and helped fuel a nascent personal computer industry. Today, hardware hacking is exploding, buoyed by the spread of hack spaces—physical workshops filled with tools and computers—across North America and Europe but also in Latin America and China. Some hackers run vibrant political collectives whose names, Riseup and Mayfirst, unabashedly broadcast their technical crusade to make this world a better one (Juris 2008, Milberry 2012). Other politically-minded hackers have gravitated toward Anonymous—an umbrella term for a range of distinct and often unconnected digital operations—to engage in hacking for the sake of leaking sensitive corporate and government information (Coleman 2012a), extending a longer tradition in hacktivism (Taylor and Jordan 2004). Others—for example, many “infosec” (information security) hackers—are first and foremost committed to security, and tend to steer clear of defining their actions in such overtly political terms, even if hacking tends to creep into political territory. Among those in the infosec community there are differences as to whether one should release a security vulnerability (often called full disclosure) or announce its existence without revealing details (referred to as anti-disclosure). A smaller, more extreme movement known as anti-sec, is vehemently against any disclosure, claiming that it is their “goal that, through mayhem and the destruction of all exploitative and detrimental communities, companies, and individuals, full-disclosure will be abandoned and the security industry will be forced to reform.”<sup>1</sup>

---

<sup>1</sup> [https://upload.wikimedia.org/wikipedia/commons/b/b7/Anti-sec\\_manifesto.png](https://upload.wikimedia.org/wikipedia/commons/b/b7/Anti-sec_manifesto.png)

National and regional differences also make their mark. Southern European hackers have articulated a more leftist, anarchist commitment than their northern European counterparts. Recently, nationalistic hacking—though virtually unexplored by scholars—has spread (Karatzogianni 2006 is an important exception). Pakistani hackers are routinely at war with their Indian neighbors. Chinese hackers are quite nationalistic in their aims and aspirations (Henderson 2007), in contrast to those in North America, Latin America, and Europe, whose anti-authoritarian stance makes many—though certainly not all—wary of joining government endeavors.

It would be a mistake to treat different types of hacking as cultural cocoons. Technical architectures, the language of codes, and protocols bring together different types of hackers and activities. For instance, as it was developed over the last four decades, the Unix Operating System, has worked to bind thousands of hackers together as part of what Chris Kelty calls a “recursive public” (2008). While we can say that hacker action and ethical principles share a common core or general ethos, inquiry demonstrates that we can identify variance and even serious points of contention. Given the multi-faceted, rich, and often controversial political effects engendered by hackers, from the creation of new licensing regimes to exposing the abuses of the surveillance state (Himanen 2001, Söderberg 2008, Wark 2004) and its historical dynamism, it is imperative to keep the variations of hacking at the forefront of our inquiries.

## Works Cited

Bazzichelli, Tatiana

2008 Networking, The Net as Artwork. Digital Aesthetics Research Center: Aarhus University

Coleman, E. Gabriella

2010 The Hacker Conference: A Ritual Condensation and Celebration of a Lifeworld. *Anthropological Quarterly*. 83(1): 47-72

2012a Our Weirdness is Free: The logic of Anonymous: Online Army, Agent of Chaos, and Seeker of Justice. Triple Canopy  
[http://canopycanopycanopy.com/15/our\\_weirdness\\_is\\_free](http://canopycanopycanopy.com/15/our_weirdness_is_free)

2012b Phreaks, Hackers, and Trolls and the Politics of Transgression and Spectacle. In *The Social Media Reader*, ed. Michael Mandiberg. New York: NYU Press

2012c *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press.

Coleman, Gabriella and Golub Alex

2008 Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism.” *Anthropological Theory*, Vol. 8, No. 3, 255-277.

Deseriis, Marco. and G. Marano

2008 *Net.Art: L'arte della Connessione* (Net.Art: The Art of Connecting) Milan: Shake. (First edition 2003)

Henderson, Scott

2007 *The Dark Visitor: Inside the World of Chinese Hackers*. Lulu.com

Himanen, Pekka

2001 *The Hacker Ethic and the Spirit of the Information Age*. New York: Random House.

Jordan, Tim

2008 *Hacking: Digital Media and Technological Determinism*. Cambridge: Polity Press.

Jordan, Tim and Paul Taylor

2004 *Hactivism and Cyberwars: Rebels with a Cause?* London: Routledge.

Juris, Jeff

2008 *Networking Futures*. Durham: Duke University Press.

Kelty, Chris M.

2008 *Two Bits: The Cultural Significance of Free Software*. Durham: Duke University Press.

Karatzogianni, Athina

2006 *The Politics of Cyberconflict*. Routledge: London and New York.

Levy, Steven

1984 *Hackers Heroes of the Computer Revolution*. New York: Delta.

Milberry, Kate

2012 "Hacking for social justice: The politics of prefigurative technology." In (Re)Inventing the Internet: Critical Case Studies. Andrew Feenberg and Norm Friesen, editors. Rotterdam, The Netherlands: Sense Publishers.

Nissenbaum, Helen

2004 "Hackers and the Contested Ontology of Cyberspace." *New Media and Society* (6)2:195-217.

Rosenbaum, Ron

1971 *Secrets of the Little Blue Box*. *Esquire Magazine*.

<http://www.webcrunchers.com/crunch/stories/esq-art.html>

Scott, Jason

2005 *BBS: The Documentary*. <http://www.bbsdocumentary.com/>

Söderberg, Johan

2008 Hacking Capitalism: The Free and Open Source Software Movement. London: Routledge.

Sterling, Bruce

1992 The Hacker Crackdown: Law and Disorder on the Electronic Frontier. New York: Bantam.

Thomas, Douglas

2002 Hacker Culture. Minneapolis: University of Minnesota Press.

Turkle, Sherry

2005 The Second Self: Computers and the Human Spirit, Twentieth Anniversary Edition.  
Cambridge: MIT Press.

Wark, Ken

2004 A Hacker Manifesto. Cambridge: Harvard University Press.

