**Hacking and hacktivism**
**[Pre-final entry for the Routledge Encyclopedia of Citizen Media, http://citizenmediaseries.org/published_volumes/routledge-encyclopedia-of-citizen-media/]**

**Julia Rone, University of Cambridge, UK**

Hacking – usually defined as the process of gaining unauthorized access into a computer or network – is a practice that redetermines information technologies and infrastructures and repurposes them through playful exploration, craft and modification (Jordan 2016). In his classic work on early computer researchers at MIT, Levy (1984) defines the central tenets of hacker ethics as sharing, openness, decentralization, free access to computers and world improvement. Coleman (2012:17) suggests, however, that having taken into account all the varieties of hacking and hackers' diverse attitudes to work, money and networks, the core of common values can be reduced to only three – freedom, privacy and access – combined with an ambiguous relationship to legality. For Coleman (2012:13), "[f]iercely pragmatic and utilitarian" hackers are also "fiercely poetic and repeatedly affirm the artistic elements of their work". Hackers relate to technology with joy and passion in search of inventive solutions and clever hacks (Himanen et al. 2001:4-7). In this respect, they embody a Romantic vision of expressive individualism that produces not only software as a technical artefact but also particular social relations and institutions, such as the Free and Open Source Software (FOSS) community (Coleman 2012:14). As Torvalds notes, "[a] 'hacker' is a person who has gone past using the computer for survival ('I bring home the bread by programming') to the next two stages. He (or, in theory but all too seldom in practice, she) uses the computer for his social ties – e-mail and the Net are great ways to have a community. But to the hacker a computer is also entertainment" (Himanen et al. 2001:xvii). That said, most of the time hacking involves mundane technical work and dealing with "constantly malfunctioning technology" (Coleman 2012:11).

An important characteristic of the hacking community, as suggested in Torvalds's definition above, is its strongly-gendered nature. Hackers have been predominantly males or female-performing males (Coleman 2015:175), often maintaining male-only stereotypes (Tanczer 2015) and occasionally blurring the lines between misogyny and non-gender related trolling (Taylor 2003). Indeed, pervasive metaphors of the Web as the Wild West and as an electronic frontier appeal to notions of transgression and 'frontier masculinity' (Adam 2005). Nevertheless, media activists have increasingly challenged gendered and raced technologies with varying success and resonances with wider societal struggles (Dunbar-Hester 2010, 2017). Feminist thinking, moreover, has enriched notions of hacking by coupling them with the concept of 'making' as both a method and a framework with which to "introduce new kinds of expertise, such as craft and care, into conversations of information technology" (SSL Nagbot 2016).

The multiple tensions within the hacking community are often expressed in binary distinctions between 'hackers' and 'crackers' (the latter being those engaged in unethical criminal hacking – Perin 2009), or through the use of finer categories such as 'black hat', 'white hat', 'grey hat', 'red hat' and 'state sponsored' hackers, 'script kiddies' (also known as 'skiddies'), 'hacktivists', 'whistleblowers' and others (Aukta 2018). The proliferation of such internal distinctions and sects has led some authors to abandon hacking as a monolithic analytical concept and to focus instead on "genealogies of hacking" (Jordan 2016:2-3) or "genres of hacking" (Coleman 2012:18), reflecting the historical development of different attitudes towards secrecy, computer security, criminality and political engagement. In addition, there have been calls to address the multiple origins of hacking and to acknowledge the contributions of groups such as the 'phone phreaks', who have tapped into the phone system in the US (Coleman 2015), and the hacker communities operating outside of the US such as the Chaos Computer Club and XS4ALL, based in Germany and the Netherlands respectively (Jordan 2016). Such sensitivity towards the multiple origins of this phenomenon is even more important considering the different ways in which hacking has been conceptualized in relation to politics: for example, while in the US, hackers have tended to focus on the politics of technology and have attempted to provide an internal critique of liberalism (Coleman 2012), in countries such as Greece and Spain, hacking has been actively incorporated into the techno-imaginary of the leftist-anarchist scene (Treré et al. 2017). Regardless of its particularities within each national context however, hacking has been marked by a series of shared trends that often run parallel to each other: these can be defined as commercialization, criminalization and politicization. The following sections explore each of these trends in turn.

**Commercialization**

Since the early days of this subculture, hacking has been persistently professionalized and integrated into the process of economic production. In the mid-1980s and in reaction against the increasing commercialization of system software, Stallman wrote the GNU Manifesto (1987), proposing an alternative free operating system. Stallman's (2002) 'free software movement' protected the core hacking values of sharing and free access by defining four freedoms, namely, the freedom to run a programme, the freedom to study and change a programme, the freedom to redistribute a programme, and finally the freedom to redistribute modifications of the programme. Free software was thus defined as free in the sense of free speech, not free beer (Free Software Definition 2018); the emphasis is on an absence of use restrictions, not on its cost to the user. While this movement successfully pushed back against corporate encroachments upon cyberspace, in the late 1990s some of its members split in order to create the Open Source Initiative, avoiding the political and ideological connotations of the word *free* and accentuating instead, in a more business-friendly way, the superior characteristics of open modes of production (Raymond 1999).

While the free software movement has continued to exist and attract new supporters, the appropriation of hacker ethics by Silicon Valley businesses in order to further their own commercial goals has been widespread. This trend has culminated in ever more popular hackathons, where participants write code and build apps in intense events often promoted as recruiting opportunities but which are above all a promotion tool for particular technology brands. The promise of technological innovation and the joyfulness and creativity of hacking are intertwined at hackathons with a desire for self-promotion that often leads to self-exploitation (Zukin and Papadantonakis 2017). The creative disruption that hackathons aim to promote in fact contributes to the legitimation of a mode of labour that is short-term and highly insecure (ibid.). Additionally, in contexts such as India, for example, hackathons have been shown to rehearse a particular type of entrepreneurial citizenship that favours quick and unproblematic collaboration with socially similar actors (for instance, other members of the middle classes) instead of more long-term democratic engagement and attempts at coalition making between diverse actors (Irani 2015).

At the same time, hacking practices have become increasingly popularized and integrated in the culture of consumption. As users have developed ways of modifying non-Apple computers to make them compatible with Apple software, hacking-related cultural references and discourses have grown in terms of their visibility among new segments of the population, including not only software experts and computer geeks, but also amateurs, laypersons and non-experts (Magaudda 2012). Since the early 2010s, hacking has entered the language of a variety of fields, with experts offering life-hacks, growth-hacks and even happiness-hacks (Yagoda 2014). Thus, the original meaning of *hack* has clearly been expanded and the term is now used widely in management and lifestyle contexts in a move that represents a significant shift away from its earlier technology-related connotations.

## Criminalization

Another important trend in the history of hacking has been the turn to criminality among certain hackers who have started employing their skills for illegal and unethical purposes. The criminalization of hacking reached its first peak in the 1990s, often dubbed the “golden age of cracking” (Jordan 2016:7). The now ubiquitous use of digital technologies in everyday life, as well as in more specialized fields such as robotics, nanotechnology and artificial intelligence, provides even more opportunities for hackers and the invention of new types of ‘future crimes’ (Goodman 2015). As a result, both hackers themselves and researchers have attempted to distinguish between ethical and unethical hacking practices: this has generally been achieved by separating hackers from crackers, or by contrasting white hat hackers, who specialize in testing methodologies to ensure the security of particular information systems, with black hat hackers, who break into computer systems for personal or financial gain, blackmail or simply to wreak havoc (Moore 2010).

Examples of unethical hacking include practices such as carding – stealing credit card details (Glenny 2011) – but also Distributed Denial of Service Attacks (DDoS), ransom demands and identity theft (Alexander 2013). A key set of tools facilitating such criminal activities are data encryption and anonymity protection software packages such as Tor, originally promoted as a means of providing “privacy for the weak and transparency for the powerful” (Assange et al. 2012), but often used by black hat hackers, along with drug dealers and child pornography distributers on the Dark Net (Bartlett 2014). Thus, the methods and tools of hacking cannot be categorically defined as either liberating and progressive or criminal. There is a fundamental ambiguity in the hacker’s craft that makes the question of goals crucial in determining the morality of any instance of hacking.

Finally, the criminal dimensions of hacking should be situated in their broader societal contexts, as cybercrime is not randomly distributed around the world but emerges from particular localities and social groups (Lusthaus and Varese 2017). Rather than operating in some ethereal virtual realm, disentangled from reality, both white hat and black hat hackers operate from specific offline locations and in concrete national and class contexts that need to be taken into account in order to understand the turn to criminality. As discussed in the next section, these local contexts are also important when considering the more political dimensions of hacking.

## Politicization

When hacking is combined with grassroots political protest and activism, it is typically referred to as hacktivism (Jordan and Taylor 2004). One of the most prominent hacktivist groups to have emerged online has been Anonymous, best known for its use of a Guy Fawkes mask as its symbol. This collective had its rather unconventional origins on the pages of the image board 4Chan, where anonymous posting, trolling, humorous deviance and doing things for the ‘lulz’ (a corruption of the phrase ‘laughing out loud’) were the norm (Coleman 2015). It was only in 2008, after a couple of years of existence, that Anonymous became politicized through its organization of a mass action against the Church of Scientology. Following Project Chanology, as the mass action became known, Anonymous continued engaging in online trolling but also started embracing political causes (such as siding with protesters in Tunisia, for example), employing a variety of legal and mainly illegal techniques that included DDoS attacks, doxing (researching and broadcasting private and identifiable information) and providing technical assistance to on-the-ground activists (ibid.). The cyborg-activism of Anonymous has thus exploited and reconfigured tensions between equality and hierarchy, reason and emotion, nihilism and idealism (Asenbaum 2017).

Similar to other collective names such as Ned Lud, the legendary leader of the Luddite movement in Britain in the late eighteenth and nineteenth century, the ‘improper name’ of Anonymous has become a terrain for multiple contestations over the use of its symbolic power (Deseriis 2015). Far from being a homogeneous collective composed only of white, libertarian Anglo-Saxon youths, Anonymous has spread across the globe, attracting enthusiasts from diverse countries, backgrounds and levels of technical expertise (Coleman 2015). While one of the basic features of Anonymous has been the collective's inclusivity and the claim that 'everyone can be Anonymous', in particular national contexts the group has also been associated with nationalistic attitudes and exclusionary discourse (Rone 2014).

Hacktivism has a long history that predates the appearance of Anonymous, however. The very term *hacktivism* was invented in the 1990s by a member of the hackers and do-it-yourself media group The Cult of the Dead Cow that formed the offshoots Ninja Strike Force and Hacktivismo, the latter seeking to apply to the Internet the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (cDa Communications and Hacktivismo 2001; Shantz and Tomblin 2014). Closely related to the practices of these groups has been the notion of electronic civil disobedience invented by the Critical Art Ensemble to describe the performance of non-violent disruptive protest through technical means, including DDoS attacks and virtual sit-ins (Critical Art Ensemble 1994). Also in the 1990s, the Mexico-based Zapatista movement and alter-globalization activists started using technology creatively in order to achieve political impact, forging new and important blends of hacking and social movement mobilization (Jordan and Taylor 2004).

All in all, this was a period of unprecedented growth for independent media (Indymedia being a prominent example) and radical servers, understood as "anti-capitalist, anti-hierarchy, autonomous revolutionary collectives" that provided free or mutual aid services to radical and grassroots activists (Riseup 1999). If this first period of hacktivism can be described as cyber-autonomism, the 2011-2013 movement of the squares after the financial crisis was marked rather by cyber-populism, treating the Internet as a 'popular space', populated by ordinary citizens who feel comfortable using proprietary platforms such as Twitter and Facebook for citizen activism and protest (Gerbaudo 2017a; 2017b). Hacktivist collectives such as Anonymous engaging in DDoS attacks, defacing and digital disobedience entered in complex cooperative and occasionally conflictual relations with these mass protest movements using commercial platforms (Rone 2018). At the same time, new data actvist projects and collectives appeared that focused not so much on hacking in the sense of unauthorized access to computers but on hacking politics: they sought to create new types of collaborative free and open source platforms for activism and whistleblower websites with the aim of opening up governments' actions for public scrutiny.

Another highly visible example of hacktivism has been the Cypherpunk movement (Levy 2002), which from the 1980s onwards sought to wield cryptography as a weapon of freedom, autonomy, and privacy that would "fundamentally and inexorably reshape social, economic, and political power structures" (Narayanan 2013:76). The cryptographic quest to ensure privacy for citizens and transparency for governments culminated in the founding of WikiLeaks by cypherpunk Julian Assange (Assange et al. 2012). Since its launch in 2006, WikiLeaks has provided a secure way for whistleblowers such as Chelsea Manning to share sensitive government information and has worked in collaboration with established media such as *The Guardian*, *The New York Times* and *Der Spiegel* in order to make this information accessible to the general public (WikiLeaks 2015). The site published leaks dealing with issues such as government corruption in Peru, civilian casualties in Afghanistan, torture in Guantanamo and the internal machinations of the US Democratic Party.

Needless to say, the disruptive activities of WikiLeaks attracted the attention of law enforcement authorities. Already back in 2010, the US government launched a criminal investigation against Assange and the Swedish government issued an international arrest warrant because of allegations he had engaged in sexual assault. Assange sought asylum and spent seven years in the Ecuadorian

Embassy in London until, in 2019, his asylum status was withdrawn and his indictment unsealed by Trump's Justice Department. Assange was accused among other things of hacking because he tried to help whistleblower Chelsea Manning to cover her tracks (Greenwald and Lee 2019). However, leading journalists have noted that this example of hacking was in fact a common journalistic practice of protecting sources. Thus, the US government's indictment of Assange "poses grave threats to press freedom" (Greenwald and Lee 2019). Meanwhile, a large number of defections, insufficient funding and negative press coverage, especially after the leaks related to the Democratic Party, have meant that the future of the entire WikiLeaks project is under serious threat (Lynch 2019).

Other hacktivist projects have been less controversial and have increasingly tried to combine the use of tech expertise with street protest, legal action and even art in order to address broader economic and political issues. The Spanish data activist collective X-Net, for example, engaged in advocacy for free culture and net neutrality but also took active part in the Indignados movement and established a secure anonymous mailbox for corruption-related leaks. After receiving a leak with the emails of one of Spain's top bankers, X-Net not only started a court-case, financed by crowdfunding, but also staged the data-based theatre play 'Become a Banker', with which they toured the country (Rone 2017; X-Net 2018).

Finally, in light of revelations regarding both autocratic and democratic governments' programmes for mass surveillance (Bauman et al. 2014; Morozov 2012), many hacktivists have started developing ways to empower and protect protesters and secure their data. In a world in which state-sponsored hacking, espionage and surveillance are the practice rather than an exception (Wooley and Howard 2017; Zetter 2015), new projects such as 'Security Without Borders' (Guarnieri 2017) and 'Security in a Box' (Tactical Tech 2018) aim to offer secure technologies to citizen activists and journalists. As both governments and corporations increasingly store and analyze big data, new social practices also emerge that adopt a critical approach to data collection and exploitation. Drawing on the heritage of hacking and the Free Software Movement, data activists find technical fixes to resist the threats to civil and human rights caused by mass surveillance (reactive data activism), but also use the possibilities that big data offers for civic engagement, advocacy and campaigning (proactive data activism) (Milan and van der Velden 2016). Examples such as iOS 'jail-breaking', that is, the removal of software restrictions imposed by Apple on its operating systems, allow users to customize their devices, circumnavigate top-down modalities of information protection, improve privacy control and sometimes even gain additional insights into data flows that would otherwise remain opaque (Cooke 2018; Dimitrov and Chow 2013).

As commercialization, criminalization and politicization of hacking practices have unfolded since the 1990s, hacking has moved from the fringes to the mainstream of public attention. The control and use of data will be crucial in forthcoming battles for freedom of expression, recognition and empowerment. Thus, hacking and hacktivism, understood as part of broader social and political trends, are here to stay. Rather than remaining simply a subculture, hacking has become a vital skill for securing free citizen participation in politics, culture and society.

## Recommended reading

**Coleman, G. (2012) *Coding Freedom: The ethics and aesthetics of hacking*, Princeton: Princeton University Press.**

Provides a detailed discussion of the history, ethics, aesthetics and politics of hacking, with a special focus on the free and open source software community and the particular strains of liberalism that have informed its practice.

**Jordan, T. (2016) 'A Genealogy of Hacking', in *Convergence: The International Journal of Research into New Technologies*, 23(5): 528-544.**

Outlines four key historical phases in the development of hacking, beginning with the activities of 'phone phreaks' and other do-it-yourself enthusiasts, and culminating in the rise of state-sponsored hacking, maker labs, hackathons and the wider cultural diffuson of hacking as a practice.

**Lusthaus, J. and F. Varese (2017) 'Offline and Local: The hidden face of cybercrime', *Policing: A Journal of Policy and Practice*, pax042: 1-11.**

Shows that cybercrime is not only an anonymous activity that exists in cyberspace but there are significant offline, human and contextual elements to take into account.

**Stallman, R. (2002) *Free Software, Free Society: Selected essays of Richard Stallman*, Boston: Free Software Society.**

A collection of essays that define free software and trace the origins and philosophy of the Free Software Foundation. Stallman offers a timely critique of patents and copyright regulation, and defends the importance of four essential freedoms: the ability to run a programme as one wishes, to study how it works, to modify it and to redistribute it.

**Zukin, S. and M. Papadantonakis (2017) 'Hackathons as Co-optation Ritual: Socializing workers and institutionalizing innovation in the "new" economy', in A. L. Kalleberg and S. P. Vallas (eds) *Precarious Work (Research in the Sociology of Work) Volume 31*, Bingley: Emerald Publishing Limited, 157-181.**

Explores hackatons as a powerful strategy used to legitimize precarious labour. The authors argue that while participants benefit from the chance to network and learn new skills, corporate sponsors frequently organize such events as a means of enhancing their own reputation, outsourcing work and crowdsourcing innovaton.