Hackers and Hacking

Luis Felipe Rosado Murillo[1] and Christopher Kelty[2]

[1]*Berkman Center for Internet and Society, Harvard University*

[2]*Institute for Society and Genetics, Department of Anthropology, and Department of Information Studies, UCLA*

Abstract

In this article we ask the question of what can social scientists and humanities researchers learn from hacking and hackers with respect to contemporary processes of technical, social, political, and economic change. We explore some of the ways hackers and hacking have been studied by academics, as well as the forms of self-narration that different hacker groups have themselves forged. We argue that the subjectivities involved in cultivating "hacking skills" are not necessarily implicated in the range of things that can be called "hacks," leading to a highly distributed phenomena in which not all "hacks" are perpetrated by "hackers" in the contemporary. We then ask what the relationship is between a particular elaboration on what it means to be a "hacker" and "hacking" as a particular sociotechnical and political practice. We end by suggesting one possible way to decompose hacking into a "stack" of practices that can be used to diagnose technical and political thresholds indicative of a mutation in the "topology" of power in the world today.

Introduction

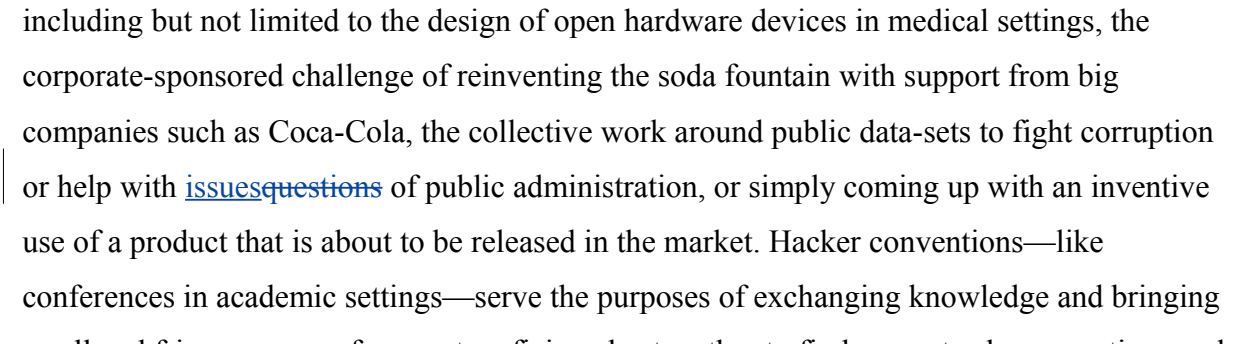
Hackers seem to be everywhere today.

Fifty to t~~T~~wenty~~-five~~ years ago, "hacking" was an underground practice, associated with a particular politics and defining a set of individuals usually characterised as adolescent, white males obsessed with computers. Today, literally anyone could call themselves a hacker, or any action a "hack". In recent decades, we have experienced the extension of the term to encompass many ordinary technical practices in various domains, such as education, health care, humanitarian response, farming, parenting, bodily modification, among many others. In Silicon Valley, companies like Facebook describe a "hacker way" to reference ordinary practices of coding, engineering, or entrepreneurship. In public relation campaigns, hackers are described simply as "doers" since "hacking just means building something quickly or testing the boundaries of what can be done" (see Fig. 1, Funders and Founders Notes 2016). According to this very generous definition, we can all be called "hackers", since we have been making artifacts for, at least, 2 millions years with the creation of mode-1 stone tools (Clark 1961).

We have also witnessed a proliferation and globalisation of hackfests, hackathons, hackerspaces, and gatherings around the symbol of hacking for a myriad of purposes,

[Figure 1 about here]

~~Figure 1: "Hackers are Doers" Funders and Founders Website (Funders and Founders Notes 2016)~~



including but not limited to the design of open hardware devices in medical settings, the corporate-sponsored challenge of reinventing the soda fountain with support from big companies such as Coca-Cola, the collective work around public data-sets to fight corruption or help with issues~~questions~~ of public administration, or simply coming up with an inventive use of a product that is about to be released in the market. Hacker conventions—like conferences in academic settings—serve the purposes of exchanging knowledge and bringing small and fringe groups of computer aficionados together to find peers, to share questions and findings that emerge when playing and working with information and communication systems (Coleman 2010b). In the contemporary, many "hacker marathons" have been organised by companies to identify programmers for hire, offering comparatively small sums as prizes for new software or hardware solutions which would necessarily cost considerably much more in research and development. A new business has been created around the work of head-hunting for software engineering talent under the rubric of the "hackathon", despite its original connotation of a community-led sprint for developing technologies.

These facts suggest that the figure of hacking and hackers has~~s~~ become fundamental to a contemporary technopolitical imaginary. Whatever hacking is, it is a very appealing figure and explanation for something. Hacking has become both a rubric for something very general, while at the same time designating a very specific set of practices from specific genealogies. In this article we explore some of the ways hackers and hacking have been studied by academics, as well as the forms of self-narration that different hacker groups have themselves forged. We argue that the subjectivities involved in cultivating "hacking skills" are not implicated in the range of things that can be called "hacks"—or put differently: these days not all hacks are perpetrated by hackers. We then ask what the relationship is between *hackers* as a particular elaboration on what it means to be a "technical person," and *hacking* as a particular practice. We end by suggesting one possible way to decompose hacking into a

"stack" of practices that can be used to diagnose technical and political thresholds indicative of a mutation in the "topology" of power in the world today. Or to put it differently, there is a reason why hacking seems to be spreading everywhere: because the forms and affordances of technical and political power are themselves changing, and hackers are at one forefront of experimenting with such mutations.

Stories of Hackers and Hacking

From the early 1950's experimentation with communication and computing systems to the present-day hacker activist initiatives in the Global North and South, the narratives of hacking have been given different genealogies, supporting different positionings with respect to who and what counts as a legitimate expression of hacking. Most of these influential narratives have been provided by journalists and self-designated hackers, but canonical scholarly works generally focus on the "culture" of computing—and not specifically ~~about~~on hacking: Sherry Turkle (1995, 1984), Diana Forsythe (2001); David Hakken and Barbara Andrews (1993); Lucy Suchman (1987); Star and Ruhleder (1996); Stephen Helmreich (1998); Joseph Dumit (2004), and Gary Downey (1998). At the most basic level, this literature has helped to address the so-called "myth of autonomous technology" which presupposes a modernist ontology which separates it from human culture and society (Latour 2008, Winner 1978). Pfaffenberger (1992) pioneered the anthropological study of sociotechnical systems in this tradition ~~by refusing a separation between technology and culture~~. In his studies of digital technology (such as the Usenet and the Personal Computer), he argued for the processual analysis of technological design as invariably embedded in cultural systems. With the exception of Pfaffenberger and Turkle, little of this scholarly work is directly focused on hackers or hacking as such, but nonetheless constitutes some of the most significant ethnographic studies of computing in English-language.

The journalist Steven Levy is one of the most authoritative sources on the early history. His mid-1980's book *Hackers: Heroes of the Computer Revolution* (Levy 1984) is exemplary in offering early heroic narratives of the exploration of computer systems. It is based on life-histories, tracing the origins of the hackerdom to the "Tech Model Railroad Club" (TMRC) of the Massachusetts Institute of Technology (MIT) of the 1950's. *Hackers* has been translated into several languages and accepted among distinct hacker communities worldwide. Its

narrative had the performative force of instituting a return to the figure of the "virtuous hacker" through descriptions of the experience of early hackers at MIT and Stanford, in Northern California collectives such as "People's Computer Company" and "Homebrew Computer Club", and companies such as Apple Computer and Sierra Games. Levy has also popularised a positive definition of hacking as grounded in the "hands-on imperative" and the "hacker ethic". This ethic includes the commitment to information freedom to facilitate technical exchange and to promote further hacking; a rebellious attitude with respect to authority, centralisation, and control of computing infrastructures; and the idea that technical work could be used to bring forth beauty and effect positive social change. Similar stories are told in the widely read books *Where Wizards Stay up Late* (Hafner & Lyon 1998) and later in *The Hacker Ethic and the Spirit of Information Age* by the Finnish philosopher Pekka Himanen (2001). While the former offered a heroic tale of the early days of the Internet engineering research, the latter was calling attention to the subjective dimensions of a cultivation that is distinctive of the computer hacker ascesis.

A more recent account of the early origins of hacking was given by the technologist Phil Lapsley (2013) in his book *Exploding the Phone: The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell* which reconstructed the early history of "phone-phreaking", the precursor of computer hacking which consisted in the exploration and information sharing about phone systems. Lapsley describes a genealogy which connects the direct action of Yippies of the 1960's with exploration of information and communication systems in the context of corporate control and centralisation of computing in the 1960's and 1970's. His account calls attention to a fundamental aspect of phone phreaking: a shared experience in which the telephone became the very embodiment of curiosity, and the phone network, a space for exploration, discovery, and socialisation.

A distinctive feature of hacker collectives resides in their effort of self-organisation around publications and gatherings. Akin to other independent groups, many phone- phreaking and hacker groups engaged in the practice of self-documentation, with the publication of "electronic zines", manifestos, and, in a few cases, with the enthusiastic adoption of an anthropological and historiographic mode of inquiry. Jason Scott (see further references) has emerged as a self-appointed archivist of much of this material, maintaining extensive archives of natively produced electronic documents, series of life-histories on hacking, Bulletin Board Systems (BBS), text-based adventure games and much else. Eric Raymond, a well-known

hacker and writer is also regarded by many as a native anthropologist of hackerdom, having written on the culture and language of hackers, and the moral norms associated with Oopen Ssource and Ffree Ssoftware (Raymond 1999, Raymond 2004). Raymond did much to preserve and popularise the collaboratively produced document known as the "Jargon File" which documented the rich language of early Internet, usenet and hacking terminology, and was republished as *The New Hackers Dictionary* (Raymond 1993) (see further references). Two major sociological and historiographic contributions in the literature depicting the rise and fall of the "hacker underground" of the 1980's and 1990's were "Hacker Culture" by the communications scholar Douglas Thomas (2003) and "Hackers" by the sociologist Paul Taylor (1999). These two books are complementary in the sense that they describe the underground hacker scene of the United States and the United Kingdom in the period of popularisation of hacker techniques and criminalisation of its practice. Taylor's work is focused on the relationship between the nascent computer security industry of the 1990's and the computer underground, giving a fruitful description of the duality which is characteristic of the underground lifeworld in which hackers are ambiguously the chaser and the chase, both on the side of law enforcement and on the side of the curious hacker collectives. Douglas' work is particularly useful in describing the discursive strategies in which the figure of the hacker as a unpredictable and uncontrollable "criminal" was instituted – having created a mythology created around the alleged superpowers of curious adolescents with access to a personal computer, a modem, a phone line, and certain access to information about flaws and holes in computer and communication security.

The work of the science-fiction writer Bruce Sterling alongside others in creating the "cyberpunk" literary genre led him to cross paths with hacker groups in the United States in a key moment of its history: the late 80's and early 90's in which the wave of "crackdowns" on hacker collectives has become widespread, especially in the wake of the US Computer Fraud and Abuse Act (CFAA) of 1986 and the UK Computer Misuse Act of 1990. His book "Hacker Crackdown" narrates the story of police chasing e after teenage hackers (Sterling 1993). Key in to his depiction is the argument of how misguided the police attempts were in framing computer hacking as a serious criminal offense without understanding of the practice and its consequences. This period also saw the rise of several media darlings and misfits, the most famous being Kevin Mitnick, who became the mainstream media martyr after an incredible story of playing cat-and-mouse with the federal police in the United States. Following his arrest in 1995After being arrested, a mobilisation of hackers around the slogan "Free Kevin"

took over the computer underground to clarify the misguidance and overreach of prosecutors in Mitnick's case. Many other hackers' stories rose to prominence in this period, ~~including~~ such as the hacker collective Legion of Doom (LOD) and their New York-based rival offshoot Masters of Deception (MOD).

In the 2000s, scholarly attention to hackers and related communities of computer users picked up significantly, especially around Free and Open Source Software on the one hand and online gaming on the other (the latter being too large a field to touch on here, but see Coleman (2010a). Hackers in F~~f~~ree S~~s~~oftware projects formed the subject of work by Kelty, Coleman, Auray, Broca, ~~Karanovic, Hakken,~~ and others (Kelty 2008, Coleman 2012, Auray 2003, Broca 2013). This literature connected work on hackers directly to issues of intellectual property and activism around it on the one hand, and also to questions about the liberal underpinnings of Free Software and the question of the putative liberalism and/or libertarianism of hackers themselves in the Euro-American context. Coleman and Golub (2008) argued most explicitly for refining our understanding of the differences *within* hackerdom by proposing several "genres" of hacking to get at distinctions with respect to the moral and technical orders different hacker groups inhabit.

More recent publication and public debates around Free Software and hacker communities has shifted the focus to questions of gender discrimination and imbalance. Alongside the work of feminist and women hackers around computer collectives such as Systers, LinuxChix, Ada Initiative and Geek Feminism, new publications have addressed the question of extreme disparity in Free and Open Source projects where it is estimated that less than 2% of the contributors are women and other gender minorities (Ghosh 2005). Nafus (2012) has discussed the question of gender with respect to the ways in which the organising symbol of "openness" represents more than an alternative to the intellectual property regime and a mode of managing the collaborative efforts in software development. According to the author, the question of openness is accompanied with the insistence that gender plays no role in software development, serving in fact to disguise the mechanisms of exclusion of women and gender minorities from Free and Open Source projects.

The most recent publication on the topic of "hacking" includes work by Michel Lallement on the topic of "hackerspaces" and the rise of the discourse and practice of "making" (Lallement 2015). Lallement has offered an ethnography of the "maker movement" in the San Francisco

Bay Area with a focus on the question of the transformations labour and its reorganisation with the creation of independent spaces for collaborative work with digital technologies. The book describes the community space "Noisebridge" in San Francisco, which has been one of the most influential autonomous spaces for the recreation of hacking as a political symbol for self-organisation and wider access to expert computing knowledge around the globe.

Hackers...

One of the key insights of recent anthropology of hackers in the Euro-American context is how they represent a distinctive elaboration of liberalism—especially in the domains of free speech and ~~the~~ a cultivation of ~~a~~ self that is ~~-~~directed towards freedom, autonomy, privacy, and other liberal values (Coleman 2012, Kelty 2008, Coleman 2014). Hackers are not uniformly libertarian or simply privacy advocates, but articulate a relationship to technology with a different range of values depending on their "genre" (Coleman & Golub 2008). Little work has been done on the way this relation to technology articulates with different political and philosophical traditions outside the Euro-American world, though a handful of people have advanced such questioning (Xiang 2007, Takhteyev 2012, Chan 2013, Murillo ~~Rosado~~ 2015).

Complicating this question of the productive relation to technology, however, is the question of whether "hacking" is a specific practice, skill, or domain of knowledge. How are hacks valued and assessed, and how they are shared, learned, improvised, recorded and displayed, or circulated? Hackers are said to have a culture of perpetrating a particular kind of act ~~which~~ that can supposedly be distinguished from the actions of other kinds of people in other professional domains (especially, those in bureaucracies, corporations, or other hidebound organisations of the past). The "hack" however can be mobile and re-usable, and it often, but not always, takes the form of a tool or set of tools; it can be a one-off, round-about way of getting something done, but it is often something that is re-usable, which serves as yet another element for generalisation. Many ordinary practices of repurposing, in different contexts, have different expressions, such as the "gambiarra", the Brazilian term for an improvisation of and deviation technical knowledge, the "juugad", which expresses a similar improvisation of technical nature in India, and the "shanzhai", which is a more specific form of repurposing mobile devices in mainland China.

In these cases, the “hacker” persona is troubled by the recognition that “hacks” are frequently borrowed, re-used, reconfigured, and redeployed by people who only subsequently come to self-identify as hackers—or maybe do not do so at all. Conversely, depending on the context of occurrence and the participants of the exchange, you could be called a hacker regardless of your expertise, but solely on the basis of the technical feat you have performed. Hacks are contextually visible to hackers, and depend on such assessment and attribution to legitimately be called hacks.

The tension in hacker personhood arises when someone claims to be a hacker, but of an unfamiliar sort. Most classic hackers hew to a definition of hacker that is open to inclusion in a particular way: through the convivial but competitive demonstration of skill in hacking. The definition of what can be included as a hack is always extensible, but only by demonstration to some set of witnesses capable of judging it. So when the word “hack” is used to refer to something that does not seem to manifest particular skill or convivial competitiveness, then a tension emerges. For example, when participants in a hackerspace assert that they “hack politics” or “hack food”—but do not provide a suitably “hackish” example of having done so —they might fail to be recognised as hackers.

Such a complicated identification of who counts as a hacker poses a dual problem for anthropological research. On the one hand, it creates a challenge for making sense of personhood ~~itself~~ in a domain where conventional idioms of what it means to be a hacker are highly contested and subjected to critique and extension. In particular, hackers are often fond of rejecting the traditional credentials of schools, employers, states, or other entities that confer expertise; they prefer the recognition of the hack itself. On the other hand, our anthropological attention can be directed to the act itself— “hacking”—and to the question of what it is and how it might be studied anthropologically, or for instance, with the tools of science studies. When are the actions of pirates, activists, criminals, spies, and other such figures considered “hacks”? When do people call mid-level engineers, librarians, scholars, and designers “hackers” and when do they not? Do all of these people, with a wide range of computing expertise, share a particular set of cultivated dispositions, or do they share a milieu of technical devices and communication infrastructures at their disposal? How can we disentangle the sudden dispersal of hacking and hackers, in the sense of a wide circulation of devices, persons, and discourses, around the world?

As we briefly explored in the previous section, there have long been competing definitions of hackers. Consider two distinctive definitions: one from the Internet engineering community and the other from the "hacker underground". For the former, a hacker is defined as a person "who delights in having an intimate understanding of a technological system" (see Request for Comments 1392 in further references), whereas his or her opposite, a "cracker", is an individual who attempts to access computer systems without authorisation. These hackers pride themselves on building complex systems out of available parts, or on getting around an engineering problem in a simple and elegant way–and they deride "crackers" as adolescents with only enough knowledge to cause trouble. As Coleman (2012) details, they are highly individualistic (in the Euro-American context), but strongly oriented towards a community of other hackers—as in the global case of Free Software hackers.

By contrast, for underground hacker collectives, hacking may signify exclusively "systems' penetration" and exploitation of vulnerabilities as a display of technical ability and mastery or, increasingly, for monetary gain. For them, hackers are people who gain unauthorised access to computer systems, a practice which is evaluated in terms of technical aptitude and virtue, measured up against the value of contributions in software code, information, and documentation. "Exploits" become objects of value that circulate—at one time only for a kind of cultural capital amongst hackers, but increasingly today as part of a robust market for "zero-day" exploits. Increasingly, these forms of hacking are also well established in the military and defence world, both defensively and offensively in geopolitical arenas.

Members of the early Internet engineering expert communities claiming ~~the~~ hacker status would strongly disagree with the definition given by or of the hacker underground. Many of these communities were described in the origin stories of Free and Open Source development as a "natural attitude" of pioneer computer technologists. They are strongly associated with research universities and with a Mertonian understanding of scientific practice; they point back to avatars such as the Digital Equipment Computer Users' Society (DECUS) in the sixties, or SHARE, the IBM mainframe computer users' group (Akera 2001), the MIT community around the Tech Model Railroad Club, the Artificial Intelligence Laboratory operating system development staff, and the early community around the Berkeley Software Distribution (BSD) version of Unix, among many others. The period which extends from the 1950's to the 1970's is identified in the literature with the work of early, pioneer hackers in pushing the boundaries of computing on many fronts: from hardware hacking to personal

computers, from new operating systems to video games and graphical user interfaces as we discussed above.

By contrast the "hacker underground" has its own mythical histories, associated with the history of phone phreaking, bulletin board systems (BBS), zines like "2600" and "Phrack", and movies like *War Games* and *Hackers*. These stories are more likely to reference the criminalisation of hacking under the US Computer Fraud and Abuse Act, and the fabled exploits of people like Phiber Optik, Kevin Mitnick, Markus Hess, Dark Dante, Erik Bloodaxe, and many others. While many Internet Engineers will point to Stephen Levy's *Hackers* as canonical, the hacker underground may point to Bruce Sterling's *Hacker Crackdown*. Over the years, these two versions of hacking have competed and collaborated: they cross paths at conferences like DEF CON, Chaos Communication Congress, and Hackers on Planet Earth (HOPE), as well as at major Free Software and Open Source events worldwide. The *cause célèbre* of intellectual property activism amongst hackers– Dmitri Sklyarov—was arrested at DEF CON 9, but became a symbol for hacking as political form —"code as speech" (Coleman 2009).

Both of these communities reject with derision the widespread use of the term today in mainstream culture. Facebook employees who "hack", "brogrammers" in Silicon Valley, and the generalised use of the term "hack" to mean "do something" are seen as corruptions of various competing versions of a tradition. The Vitra "Hack" desk (see Fig. 2), for instance, performs an attentuated and distorted version of hacking that emphasises Silicon Valley neoliberal start-up culture, an "individually adaptable private sphere" (see Fig. 2), and a vision of flexibility in which the desks convert into sofas as part of a longed for collapse of work, leisure, and political authenticity, primarily amongst white, upper middle class technology employees in Europe and North America.

[Figure 2 About here]

~~Figure 2: The Hack Desk, designed by Konstantin Greic, manufactured by Vitra.~~

But the mainstreaming of hackerdom is just as likely to expose the sexism and/or racism of past communities of hackers. An "elite hacker" in an interview to an influential hacker zine declared the demise of the hacker underground with the xenophobic and misogynistic observation that "today it is claimed that the Chinese and even WOMEN are hackers. Man,

am I ever glad I got a chance to experience 'the scene' before it degenerated completely" (.:: *Phrack Magazine* ::. 2016). Symbolically violent in its own terms, this observation indexes not only the ethnocentric and gendered lifeworld of most hacker collectives, but the fact that hacking is no longer limited to the virtual play-fight among Anglo-American suburban adolescents, pointing also to questions of personhood, ethnicity, and gender with the evaluation of who gets to be considered a hacker.

What is important to emphasise in these examples is not the adoption of one definition or another, but the evidence of a series of disparate, conflicting, and generative differences for the contextualisation of ~~the~~ hacking. This is the evidence of an oscillation in respect to the value of "hacking" over time: fluctuating from positive to negative moral valences, that is, from elite, exclusive groups of technologists to online and offline communities marked by the rhetoric of openness and transparency, or, from what the communications' scholar Douglas Thomas (2003) called the "culture of secrecy" of the hacker underground in the height of the Cold War to a culture of collaboration, openness, and transparency as a shared utopian horizon in neoliberal times.

...or hacking?

What is a hack? And how is it different from leaks, breaches, exploits, or other actions of information disclosure and circulation, both constructive and destructive?

Leaking, for instance, has become associated with hacking more strongly in the last decade. The furor around WikiLeaks brought the fun-loving underground anti-collective Anonymous to world-wide attention via its coordinated attacks on corporations and governments. Similarly, piracy: The May 15 movement in Spain was spearheaded alongside protests of La Ley Sinde—an anti-piracy law widely opposed by musicians and consumers alike. These protests ultimately merged with anti-austerity protests of the "Indignados" who shared key activists in the North African revolutions, who were also involved in the movements organised by Anonymous, who were often connected to actors in both May15 and Occupy, as well as hacker activists of many groups including the group "Telecomix". Taken together, such actions have often been labelled "hacktivism".

Hacktivist movements, sometimes autonomous and sometimes part of larger movements like Occupy, borrow tactics, technologies, slogans, and ideas that both explicitly and implicitly reference the "hacking" of Free Software, of the Pirate Party, of anti-surveillance, pro-privacy hackers (like Tor) and copyright reform movements like Creative Commons or activists fighting for Net Neutrality. All of this has occurred at the same time that US and Israeli spies were infecting Iranian nuclear power plants with the StuxNet virus (Zetter 2014), and the NSA and GHCQ were cataloguing all of this, and perpetrating some of the greatest "hacks" the Internet has ever seen—and this we know mostly because of the even greater intelligence leak—or "hack"— of Edward Snowden.

Hacking, as a practice, is not confined to hackers, but increasingly a practice essential to the social fabric in surprising ways. One might turn to "practice theory" in its various forms to explore this—are hackers part of a "community of practice" constituted by hacks-as-practice? Is hacking a political expression of an emergent sociocultural field, in Bourdieusian terms? Are hackers heterodox actors in the context of a mainstream computing field, wildcards in various professional domains, akin to the figure of Luther Blissett or Guy Fawkes who can come in and out of a mysterious identity? Is hacking now mainstream itself?

To speak of hackers as a community of practice, or of hacking as a field, combines questions of technical and political cultivation with the identification of a distinctive practice in order to suggest that the identity of a hacker is based in the practice of hacking. Indeed, such definitions are common (we ourselves have proposed them—in the case of a "recursive public" for instance in Kelty (2008)). But this approach cannot accommodate the fact that hacking and hacks have become more obstreperous and unruly in their circulation: hackers fight hackers (vigilante-style or as collaborators of law enforcement), trolls troll trolls, and pirates steal from pirates today. To conflate the question of hacker identity with the question of the practice, political, technical, or otherwise, would miss the mark.

Instead, there are multiple and intersecting moral and technical orders inhabited by people who self-identify or are identified by peers as hackers. From the underground hacker collectives to "grey hat" security researchers to spam-slinging criminal actors, to the hard-core free speech and privacy cryptography defenders; from the die-hard Free Software activist to the business-oriented Open Source evangelist; from the über-cool Northern European design artists to the goofy-but-terrifying Anonymous hackers, and so on. As Coleman and

Golub (2008) point out, there is no single liberal ideology that hackers adopt, but rather a range of "genres" in which any given individual or group might operate, implying both the freedom and the constraints that word signals.

The notion of genre is useful for integrating hackers and hacks in a complex whole— a kind of story that integrates elements of personhood with material forms, technical practices, and political rationalities. But it is also the case that "hacks" can be independent, modified, shared, and re-appropriated across genres. Hacks imply a range of technological affordances that make practices of hacking less dependent on embodied skill than many other kinds of practice (e.g. glass blowing or cabinet making) and as a result more mobile and modifiable. The expanded field of hacks, leaks, exploits, breaches, ops, online campaigns, and so on form the very substance of political and working life today in its complex entanglements with things, protocols, perspectives, and sensibilities of digital technologists and technologies.

In the next section, therefore, we turn to the question of how one might distinguish hacks as different forms and expressions of power. Because hacks are a regular feature of work, play, and politics, it is important to look at the kinds of hacks that cross these divisions, and represent mutations in the configuration of power, knowledge, and everyday practice in a Foucauldian sense. Hacking, leaking, breaching, hacktivism, and so on each imply different sets of tools, tactics and practices, and engage overlapping genres of hackers. Foucault's approach to power has generally been used to make a claim for certain general or epochal changes as a result of such mutations in the field of tactical power: sovereignty, biopower/disciplinary power, and the governmentality of neoliberalism. But recent work on Foucault ~~suggests that~~ reflects his own interest in the mutual configuration of these different political rationalities (Macmillan 2011). Instead, we suggest that there are reconfigurable elements in the domains of in which "hacking" is relevant—a "topology" in which some forms of "hacking" respond to and constrain others. Hacks are often a recombination of the elements of power, a stretching of this topology in which action and response create tensions and thresholds of power related to particular modes of hacking. Approached this way, one can better narrate the "recombination of elements" that Foucault (at least later in his work) recognised as a way to stretch, transform or warp the patterns of correlation that make up a given mode or configuration of power (Collier 2009).

Viewed this way, we can better account for the fact that many "hacker practices" do not originate with hackers, nor do they confine themselves to use by hackers. Tactics or practices are picked up by computer security scientists and researchers, security firms, police forces, political campaigns, anti-piracy outfits, analysts of all sorts, as well as spreading globally through networks of activists, hacker and maker spaces, legal firms, musicians and artists, or consumers and pirates. Hackers go to work for Google or Facebook, anti-piracy companies appropriate the tools of hackers and pirates. Pirates hack Ff~~f~~ree Ss~~s~~oftware tools, and large corporations engage in technical and legal cat-and- mouse games with pirates. Power, in this sense, is about the recognition, appropriation, recomposition, and redistribution of tactics and practices: not ideologies or genres as much as recomposable instances of power. The technique of DDOS attack, for instance, or the use of a copyright infringement cease-and-desist letter, the creation of commons-producing copyleft licenses, or the use of the BitTorrent protocol can all be called hacks, but they look different when employed in response to other hacks, leaks or breaches.

The first three practices listed here (invention, inversion, and figuration) are quasi- direct forms of action; they are accessible to anyone and do not require large investments of money or stable organisations to mobilise. The last two (regulatory action and enforcement), however, are often more second-order or "representative" in that they often require physical, financial, or organisational resources and a certain scale and depth of involvement to perform. But we suggest that even these two forms have a "hackish" character in the contemporary.

Invention

Invention is the broadest possible meaning of hacking. It includes building and making things, and not only material things, but especially so-called "immaterial" products such as software, legal licenses, or organisations. Invention might include those practices that arise out of a lack, and at least in the conventional language of research and development, it comes with extensive planning, study and investment of time and money. But considered as a form of "hacking", invention often implies a possibility based in the existence of multiple existing tools and components. Creating software, hacking together hardware components or starting up an organisation are all practices of invention in so far as they are carried out to solve a problem or respond to a lack that makes certain possibilities clear.

Invention in the era of hacking has become much simpler and cheaper, as toolkits, frameworks, patterns, and languages and other easily reusable and either cheap or free to use tools create a material culture of ready-made, accessible, often lego-like parts. Easy access to tools is by now an ethic (as in the case of the Whole Earth Catalog, "Access to Tools" described by Turner (2006)) of mutual aid and instruction, and an appreciation for both the DIY possibilities of our world, and sometimes a respect for (and desire to contribute to) the coordinated engineering necessary to bring them into being.

Furthermore, the practice of invention implies an affinity based in shared understandings of how things work. Whether that is a classic engineering culture (based in University and/or corporate practice), a DIY geek culture, a UNIX culture, a glass- blowing culture (O'Connor 2005), invention demands not only skill but the capacity to recognise others with more or less the same skills, habits of practice, and commitments to certain kinds of technological or material choices (Sennett 2008). It is this version of hacking that is most clearly identified with, for instance, the Internet Engineering communities described above, but also because of its generally positive valence, the aspect which is emphasised by Silicon Valley start-ups.

Inversion

Inversion is a term meant to signal a practice that—at least under the label of "hacking"—is often insufficiently distinguished from invention. Inversion is the kind of hacking that involves finding a way to use existing tools or technologies to achieve something they were not meant to do. Under this aspect, exploits of vulnerabilities, using systems against themselves, inverting the intended purpose of a system, or remixing something for purposes of critique, parody, ridicule, or something more practical (Galloway & Thacker 2007). In terms of hardware, it includes the practices of modding and customisation; in terms of software, it includes the practice of finding and exploiting weaknesses in software (for good or evil intent) or recombining software elements in a surprising and clever way in order to achieve a new goal.

A famous example of inversion is neither hardware nor software but a so-called "legal hack": the General Public License (GPL), which uses existing statutory copyright law to accomplish something it was not intended to do.

Inversion generally assumes institutional structures or infrastructures with a certain transparency (one must be able to see how something works in order to exploit it). Some tactics exist for inverting the non-transparent. Leaking—such as the actions of ~~WikiLeaks~~Manning or Snowden—might be considered an inversion, as might some forms of reverse engineering of secret techniques or closed technologies. For technologists of the "hacker underground" ilk, a whole range of tools exist for attempting to break technologies, either to gain access, or to control them (the creation of Botnets, zombie servers, etc.) Inversion also implies faith in engineering and in the rule of law: for something to be inverted is not the same as for it to be destroyed or disabled. GPL licenses work because copyright law is legitimate and enforced outside hacker circles. Remix or recombination of software is done because the challenge is often to make something work better or meet higher standards of practice or security. By extension, the faith is that things can always be and become better; only imperfect things can be hacked— inverted—in this sense.

Similarly inversion implies patterns of regularity that can be exploited—the very thing upon which the practice of invention often depends as well. Inversion works upon certain technological or organisational preferences shared amongst a large group of people—for instance the use of SCADA control systems amongst process engineers who design large industrial plants allows for hackers to imagine exploits with powerful effects on the material world. Similarly, entrenched social practices~~behaviours~~ are often exploited in "social engineering" hacks that rely on the regularities of organisational design and human behaviour.

Figuration

It is also clear that not all hacking is restricted to technological manipulation. We suggest **figuration** to capture the more traditional and recognisable forms of political action: rhetorical persuasion, ideological argument, political advocacy, etc. Classic descriptions of the functions of the public sphere tend to characterise it as an issue of sovereignty—the ability of "the people" to speak to and force changes amongst established domains of power like the state, the church, the military, etc. (Anderson 2006). All of the tactics involved here are about visibility and the legitimacy of a political process.

To speak of figuration as a mode or component of "hacking" today, however, is to recognise that such classical forms of discursive and persuasive power are also used as forms of, and in response to, hacking: operations by A~~a~~nonymous, for instance, can be restricted to the

widespread circulation of messages, videos and manifestos. The protests against SOPA and PIPA in 2012 in the United States were largely traditional responses by hackers (and others) to an attempted regulatory action.

Materially speaking, figuration depends on shared communication structures. Very often today, hacking can take the form of *inventing* or *inverting* communication practices as part of or in response to practices of figuration. In many ways, open government data advocates of the last few years are demanding that longstanding institutional structures (such as public hearings or requests for comments) be hacked in order to make interacting with the government and its agencies simpler or to make agencies more responsive. To do this they rely on a figuration of government as slow, non-responsive, elitist, or rigidly bureaucratic.

Substantively (at least in the domains of intellectual property and information technology) practices of figuration have been heavily focused on issues such as privacy, transparency, free speech, freedom to operate (or innovate), and network neutrality. These issues subtend a long and rich discourse that includes both scholarly debates and conventional understandings of these concepts and their value to our lives. Examples of "hackish" figuration include the Electronic Frontier Foundation. EFF was created in the context of "hacker crackdowns" of the early 1990's to articulate a discourse on the importance of defending civil liberties online, and as a fund to legally defend hackers from prosecutorial overreach. Similarly, the death of Aaron Swartz provides a figure of openness and Oopen Aaccess as vital global struggles to which hackers can and should contribute.

Regulatory action

Regulatory action is not historically a form of hacking, and in many ways it is its most important opposite. Nonetheless, a hackish attitude towards regulatory action has emerged as a possibility—the strategic attempt to regulate (either formally as part of government action or through software, or informally through other means) represents another tool in the hacker kit. The language of regulation-as-control was most clearly articulated in terms of hacking by Lessig's famous work *Code, and other laws of cyberspace*, which argued that many different kinds of things regulate behaviour (law, morals, architecture) and are amenable to change to different degrees (Lessig 2000).

At the most general level, regulatory action includes any form of policy change intended to introduce, maintain, or extend control. State-based forms of regulatory action are the most obvious and familiar but large corporations also engage in regulatory action of particular kinds routinely—especially those industries who control networks or technologies in widespread use.

Regulatory action almost necessarily implies large bureaucratic organisations of a classic Weberian type—rule-based, hierarchically ordered, and subject to regimes of oversight and transparency. As a result, regulatory action is relatively rare, and comparatively complicated to carry through. The tactics of invention, inversion, and figuration are often oriented towards influencing, responding to or disrupting regulatory action of various kinds—the 2012 case of protests against SOPA/PIPA being a clear case; another case would be Operation Payback conducted by participants of Anonymous against the global credit card companies MasterCard and Visa, who had engaged in the regulatory action of systematically blocking PayPal donations to the WikiLeaks organisation.

Inversion often borders on regulatory action when it is used strategically to achieve something in the interests of a particular entity, but so too does figuration, which is the tactic most often employed to support or protest a proposed legal change (both were used in the case of SOPA/PIPA). Cases of significant interest include those where regulatory action look more like cases of inversion—i.e. where a legal action, for instance, is used to threaten, intimidate, or censor a particular group. The injunctions filed against Megaupload and its owner, Kim Dotcom, for instance, are represented as mere enforcement of the law, but in reality represent the effective mobilisation of state power by industry organisations like the MPAA and the RIAA.

Enforcement(s)

Finally, there are practices of enforcement. Often only implicitly or metaphorically included in a Foucauldian analysis (discipline is held to be more insidious and more profound kind of force, a ’government of the soul’ for instance). While classic displays of sovereign power are relatively rare (helicopter raids by anti-terrorist forces on New Zealand mansions of flamboyant wannabe hackers notwithstanding, such as the case of Kim Dotcom), they remain a central tactic in the repertoire of power, and they are by no means restricted to a state and its repressive apparatuses.

Many forms of enforcement are widely available today. A range of tactics and practices, of which the DDOS is only the most common, are not confined to any particular segment of society, but available to anyone who might, for instance, download and install a copy of the Low Orbit Ion Cannon (or its predecessor, FloodNet, written by the Electronic Disturbance Theater group in 1994 to flood the Mexican government website with requests in order to send a message of support for the Zapatistas). Legal tools like cease-and-desist letters are also routinely used as a tactic of force; even patent litigation can be understood this way when conducted by so-called patent trolls. Networked-based forms of disruption are very often simultaneously tactics of invention or inversion—coming into existence in response to the actions of states or corporations. Piracy and cracking generally might be said to move from being a tactic of inversion when a vulnerability in a copy-protection scheme is merely demonstrated (e.g. Sklyarov demonstrating holes in the eBook Reader) to a tactic of force when that vulnerability is routinely exploited for gain, protest, or sabotage.

[Figure 3 about here]

~~Figure 3: Stack of Power: an analytic decomposition of hacking practices and how they might relate~~

These five practices fit together as one possible description of how "hacking" is part of a topology of power today. The software programmer's metaphor of a "stack" is useful here—in common parlance it refers to a frequently deployed but heterogeneous collection of tools, libraries, and interfaces. Such tools interface with each other, and can in some cases come to depend on one another (nothing would happen without an operating system in place, but there are many variants available).

The image of the stack we employ here, however, is meant to provide a basic map of push and pull, of action and reaction, or of provocation and response. We intend it to be used to help diagnose certain technical or political thresholds in the recent past of hacking; ~~(~~and we take it as axiomatic, as anthropologists, that hackers are historically situated subjects who experience these thresholds in their own lives and practices under different conditions, despite sharing many technical devices, protocols, and infrastructures~~)~~.

Conclusion

Are we experiencing the distancing between the "hacker" as a particular manifestation of personhood and the "hack" as a set of tactics of power? Or, conversely, are we witnessing a global expansion of the conditions for cultivation of hacker expertise, leading to a proliferation of differences in the context of what it means to be a hacker and to hack? How is the global difference in technical and moral cultivation of computer technologists related to the global accessibility of hacks? What are examples of the reverse process in which the actions of global hackers (say, book pirates in Russia, hacktivists in Tunisia, or Anonymous' attacks on ISIS) have an impact on mainstream practices?

To return to these open questions, we conclude with the following observations. First, we suggest that the study of hacking as a practice of ethical and technical enskillment can be advanced to describe and interpret manifestations of hacking outside the Euro-American centres of technical and discursive production on digital technology. Such work is necessary if we seek to displace the imperial imperative of digital technology, which often transforms sociotechnical *difference* into resemblance (or poorly made copy of Euro-American "sources") in other parts of the world.

Anthropological studies of the global circulation of digital technologies and expert technologists have demonstrated the naturalisation of Euro-American assumptions in digital design: from user interfaces to data models; assumptions of usefulness of particular technologies based on the prestige of their place of creation; and the imposition of particular projects from centres of production to disconnected peripheries of the global South (Chan 2013, Takhteyev 2012, Xiang 2007, Murillo ~~Rosado~~ 2015). We suggest that such assumptions might well be built into the global stack of power we describe above, and to look to different traditions would be to ask how hacks themselves might be hacked.

The recent past of hacking clearly overlaps with other practices–those of piracy, activism (whether labelled cyber-activism or hacktivism), trolling, leaking, and breaching. Such practices should be understood not as simple forms of hacking, but as part of a topology of power ~~which~~ that is locally stable, but historically changing. If history has tended towards the stabilisation of forms of power, the manifest speed and ease with which the contemporary topology can be stretched and deformed suggests a perpetual oscillation or turbulence, limited only by the energy and enthusiasm that can be committed to the various practices of invention, inversion, enforcement, figuration, or regulation. Secondly, we suggest that the

widespread embrace of hacking reflects changes in threetwo traditional domains of study: work, education, and political action. The language of hacking and the question of hacker personhood provides a window on the changing meaning of work, career, and expertise. Rather than a life-long career, grounded in training and acquisition of expertise, maintained through repeated trials of problem-solving within the basic framework of the division of labour, the embrace of "hacking" (as in the case of the Hack Desk) is clear evidence of anxieties about work that is temporary, flexible, transient, and often includes highly individualised ways of demonstrating one's creativity. They remain focused on problem-solving, but disdain a division of labour and a hierarchy of expertise, which often mirrors actual changes in work environments in the last several decades (Boltanski & Chiapello 2005). In this respect, hacker personhood may represent a vanguard of sorts for changes affecting large parts of a global labour force.

By contrast, when hacker personhood is considered in light of political action, it highlights a different set of changes, and possibly a political threshold which might be described as a new form of sabotage. It is this aspect—especially under the label of hacktivism—which raises the central question of the link between hackers and hacking, precisely because of the proliferation of hacks that can simultaneously be used for diametrically opposed political purposes. Sabotage does not always imply a form of class resistance and consciousness—it is also often a competitive tactic within capitalism and a form of warfare engaged in by state actors. But whether this form of hacking-as-sabotage is related to the production of a particular form of hacker personhood remains an open question.

Finally, there are important methodological lessons to be learned by anthropologists and other social scientists through the study of hacking. The obsession with "the digital" in contemporary scholarship is a kind of Stockholm Syndrome: we have been kidnapped by shiny new technologies and the discourse of innovation, and as a result we have come to love our captors. But Ththe digital (as in "digital humanities") is not a panacea for the problems of collaborative research in anthropology and the human sciences at large; but even ifit can certainly help if digital technologies aremust be redesigned to further promote collaborative engagements between ourselves and with the communities with which we conduct research. Digitisation of field research carries potential benefits with respect to the ease of archivingval and data sharing, allowing for longitudinal and extensive comparative studies. But it also carries serious issues of data privacy and anonymity as most researchers (in both the sciences

and humanities) are not well informed and trained to handle problems of information security. Hacking, in this regard, is an important source of practices and workarounds—, both in the sense of invention and inversion—, to deal with questions of information security, sharing, and remote collaboration across transnational lines of exchange; —but it also represents a danger that transcends the immediate ethical relations that anthropologists have traditionally been concerned with. In the future, we may have more to learn from hacking than about it.

Further resources

- Original MIT Jargon File, kept by Paul Dourish: http://www.dourish.com/goodies/jargon.html
- Extended Jargon File at Eric Raymond's site: http://www.catb.org/jargon/html/
- Jason Scott's textfiles: http://textfiles.com/
- Hackerspaces wiki: http://hackerspaces.org
- Request for Comments 1392: http://www.rfc-base.org/txt/rfc-1392.txt

References

Akera, Atsushi (2001). "Voluntarism and the fruits of collaboration: The IBM user group SHARE". In: *Technology and Culture* 42.4, pp.710–736.

Anderson, Benedict (2006). *Imagined communities: Reflections on the origin and spread of nationalism*. Verso Books.

Auray, N (2003). "Communautés epistemiques d'innovation - La regulation de la connaissance : arbitrage sur la taille et gestion aux frontières dans la communauté Debian". In: *Revue d'économie politique.* 113, p. 161. issn: 0373-2630.

Boltanski, Luc and Eve Chiapello (2005). *The New Spirit of Capitalism*. London: Verso.

Broca, Sébastien (2013). *Utopie du logiciel libre: du bricolage informatique à la réinvention sociale*. French. Neuvy-en-Champagne: Éd. le Passager clandestin.

Chan, Anita (2013). *Networking peripheries: technological futures and the myth of digital universalism*. Text in English. Cambridge, Mass.: MIT Press.

Clark, Grahame (1961). *World prehistory: an outline*. Cambridge Eng.: University Press.

Coleman, E. Gabriella and Alex Golub (2008). "Hacker practice: Moral genres and the cultural articulation of liberalism". In: *Anthropological Theory* 8.3, pp. 255–277. doi: 10.1177/1463499608093814. url: http://ant.sagepub.com/content/8/3/255. abstract (visited on 01/31/2012).

Coleman, Gabriella (2009). “Code is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers”. In: *Cultural Anthropology* 24.3, pp. 420–454. issn: 0886-7356.

Coleman, Gabriella (2010a). “Ethnographic Approaches to Digital Media”. In: *Annual Review of Anthropology* 39.1, pp. 487–505. issn: 0084-6570. doi: 10 . 1146 / annurev.anthro.012809.104945. url: http://www.annualreviews.org/eprint/gzYRzazRZpBjEGWfcWr5/full/10.1146/annurev.anthro.012809.104945.

Coleman, Gabriella (2010b). “The Hacker Conference: A Ritual Condensation and Celebration of a Life- world”. In: *Anthropological Quarterly* 83.1, pp. 47–72. issn: 1534-1518. doi: 10 . 1353/anq.0.0112. url: http://muse.jhu.edu/content/crossref/journals/anthropological%5C_quarterly/v083/83.1.coleman.html.

–(2012). *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton University Press.

–(2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso Books.

Collier, Stephen J (2009). “Topologies of Power Foucault’s Analysis of Political Government beyond ‘Governmentality’”. In: *Theory, Culture & Society* 26.6, pp. 78–108. issn: 0263-2764.

Downey, Gary Lee (1998). *The machine in me: an anthropologist sits among computer engineers*. English. New York: Routledge.

Dumit, Joseph (2004). *Picturing personhood: brain scans and biomedical identity*. English. Princeton, N.J.: Princeton University Press.

Forsythe, Diana (2001). *Studying Those who Study Us: An Anthropologist in the World of Artificial Intelligence*. Stanford University Press.

Funders and Founders Notes (2016). *Who Are Hackers? Hackers Are Doers.* url: http://notes.fundersandfounders.com/post/50417296471/who-are-hackers- hackers-are-doers (visited on 01/28/2016).

Galloway, Alexander R and Eugene Thacker (2007). *The exploit: A theory of networks*. Vol. 21. University of Minnesota Press.

Ghosh, R A (2005). “Understanding Free Software Developers: Findings from the FLOSS Study”. In: *Perspectives on Free and Open Source Software*. Ed. by J Feller et al. Cambridge, MA: MIT Press, pp. 23–46.

Hafner, Katie and Matthew Lyon (1998). *Where wizards stay up late: The origins of the Internet*. Simon and Schuster.

Hakken, David and Barbara Andrews (1993). *Computing myths, class realities: an ethnography of technology and working people in Sheffield, England*. English. Boulder: Westview Press.

Helmreich, Stefan (1998). *Silicon second nature: culturing artificial life in a digital world*. English. Berkeley: University of California Press.

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

Kelty, Christopher (2008). *Two bits: the cultural significance of free software*. Durham: Duke University Press.

Lallement, Michel (2015). *L'âge du faire: hacking, travail, anarchie*. Paris: Seuil. Lapsley, Phil (2013). *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell*. English. New York: Grove Press.

Latour, Bruno (2008). *We Have Never Been Modern*. Harvard University Press, p. 168.

Lessig, Lawrence (2000). *Code: and other laws of cyberspace*. New York, N.Y: Basic Books.

Levy, Steven (1984). *Hackers: heroes of the computer revolution*. English. Garden City, N.Y.: Anchor Press/Doubleday.

Macmillan, A. (2011). "Empire, Biopolitics, and Communication". In: *Journal of Communication Inquiry* 35.4, pp. 356–361. issn: 0196-8599. doi: 10.1177/0196859911415678. url: http://jci.sagepub.com/cgi/content/abstract/35/4/356.

Murillo ~~Rosado~~, Luis Felipe R. (2015). "Transnationality, Morality, and Politics of Computing Expertise". PhD thesis. Los Angeles: University of California, Los Angeles.

Nafus, Dawn (2012). "'Patches don't have gender': What is not open in open source software". en. In: *New Media & Society* 14.4, pp. 669–683. issn: 1461-4448, 1461-7315. doi: 10.1177/1461444811422887. url: http://nms.sagepub.com/content/ 14/4/669 (visited on 04/01/2014).

O'Connor, Erin (2005). "Embodied knowledge The experience of meaning and the struggle towards proficiency in glassblowing". In: *Ethnography* 6.2, pp.183–204.

Pfaffenberger, Bryan (1992). "Social anthropology of technology". English. In: *Annual review of anthropology* 21, pp.491–516.

.:: Phrack Magazine ::. (2016). url: http : / / phrack . org / issues / 65 / 2 . html # article (visited on 01/28/2016).

Raymond, Eric S. (1993). *The new hacker's dictionary*. 2nd ed. Cambridge (Mass.) [etc.]: MIT Press.

Raymond, Eric S. (1999). *The cathedral & the bazaar musings on Linux and open source by an accidental revolutionary*. English. Beijing: O'Reilly. (Visited on 01/09/2013).

Raymond, Eric S. (2004). *The art of Unix programming*. English. Boston: Addison-Wesley.

Sennett, Richard (2008). *The Craftsman*. New Haven: Yale University Press.

Star, Susan Leigh and Karen Ruhleder (1996). "Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces". In: *INFORMATION SYSTEMS RESEARCH* 7.1, pp. 111–134. doi: 10 . 1287 / isre . 7 . 1 . 111. url: http://isr.journal.informs.org/cgi/content/abstract/7/1/111%20http://infosys.highwire.org/cgi/content/abstract/7/1/111.

Sterling, Bruce (1993). *The hacker crackdown: law and disorder on the electronic frontier*. New York: Bantam.

Suchman, Lucy Alice (1987). *Plans and situated actions: the problem of human- machine communication*. English. Cambridge [Cambridgeshire]; New York: Cambridge University Press.

Takhteyev, Yuri (2012). *Coding places: software practice in a South American city*. English. Cambridge, Mass.: MIT Press.

Taylor, Paul A (1999). *Hackers: crime in the digital sublime*. London: Psychology Press.

Thomas, Douglas (2003). *Hacker culture*. Minneapolis: University of Minnesota Press.

Turkle, Sherry (1984). *The second self: Computers and the human spirit*. New York: Simon and Schuster.

– (1995). *Life on the screen: identity in the age of the Internet*. New York: Simon & Schuster.

Turner, Fred (2006). *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. Chicago: University of Chicago Press.

Winner, Langdon (1978). *Autonomous technology: technics-out-of-control as a theme in political thought*. MIT Press, p.396.

Xiang, Biao (2007). *Global "body shopping": An Indian labor system in the information technology industry*. English. Princeton, N.J.: Princeton University Press.

Zetter, Kim (2014). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. English. New York: Crown Books.

Comments and issues overview:

References

- **The Request for Comments 1392 source was added in both the text (Page 8) and the further references section as agreed upon in the German version of the article.**
- **Fig. 2 with Vitra press release and photos: Reference missing in text and literature list. Please provide this information to include in the article.**

Image requirements (Figures 1, 2, and 3)

Unfortunately, the images you submitted for both the English and German articles do not meet the publisher's requirements. In light of this, it would be important for you to modify the images to meet these requirements.

English article: Routledge requires that all images are provided individually in TIFF or JPEG formats at a minimum resolution of 300 dpi. There are also specific requirements for artwork such as the line art you provided for Fig. 3. For all details on these requirements, see attachment in email: Author instructions: Section 8. How to supply artwork (pp. 35-40).

German article: UVK requires that all images are provided within the article at a minimum resolution of 600 dpi.