FREE SOFTWARE TO OPEN HARDWARE

CRITICAL THEORY ON THE FRONTIERS OF HACKING

Johan Söderberg

UNIVERSITY OF GOTHENBURG
DEPT OF SOCIOLOGY

STS Research Reports 17
Johan Söderberg
Section for Science and Technology Studies
Department of Sociology
University of Gothenburg
Box 720
SE 405 30 Gothenburg
Sweden
johan.soderberg@sts.gu.se

Free Software to Open Hardware: Critical Theory on the Frontiers of Hacking
Författare Johan Söderberg
ISSN: 1650-4437
ISBN: 978-91-975442-7-6

Omslag: Andreas Skyman
Print:Geson Hylte Tryckt, Göteborg 2011

For those curious to find out the content of the picture on the cover, this is for your information: Each pixel stores a byte value from a sound file. Data (490x490 bytes) should be read row by row, the last 256 pixels are the key, 16 bit PCM, little Endian, 8000 Hz.

contentious politics. Entitled 'Free space optics in the Czech wireless community: Shedding some light on the role of normativity for user-initiated innovations', my third article has been accepted for publication in *Science, Technology & Human Values*. The final article expresses the same concerns but this time addressing constructivist STS theory instead. Under the title 'Reconstructivism versus critical theory of technology: Alternative perspectives on activism and institutional entrepreneurship in the Czech wireless community' this paper has been published in *Social Epistemology*.

With this introduction, I hope to give the reader some orientation concerning the four articles which constitute my thesis. The ambition is to render explicit ideas which have shaped the character of the papers, but which have not always been fully developed. In the following section, I will define the term 'hacker' in more detail. In the process I shall critically review some of the earlier literature about hackers. Thereafter, I shall present my main theoretical points of departure. At the centre of discussion will stand the commonalities and divergences between constructivist STS and the critical theory of technology. These relations have preoccupied me during recent years. Thereafter, I discuss the methods I have used when studying hackers. I take my methodological cue from Theodor Adorno's reflections about balancing immanent and transcendent critique when investigating a topic. The final part of this introduction outlines in more detail how the individual articles relate to each other and sets an agenda for further research.

Who is the "Hacker"

At the outset I need to say a few words about the key figure at the centre of my work: the 'hacker'. There are several, conflicting notions to be found in the academic literature about how to address this figure. Bearing this in mind what better place to start looking for a definition than the *Jargon file*, a widely recognised lexicon of hacker slang? The first entry for 'hacker' reads:

> A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary (*Jargon file*).

Three more entries follow stressing the hacker's aptitude for programming. In addition, some general characteristics expected of an individual claiming to be a hacker are described, such as enthusiasm, curiosity, and the like. While this might offer a point of departure, scholars studying hackers must not stop there. The definitions given by the hackers, here represented by the quote from the

Jargon file, are too closely intertwined with their internal turf wars, their concern with excluding 'wannabes', with morale boosting, and so on. To start with, I will note a minor problem with the definition of the hacker laid down in the *Jargon file*. It relies heavily on one specific technical practice, i.e. programming computers. With such a definition, it would be stretching it to call the people I am looking at in this thesis for hackers. My informants are primarily involved in building wireless networks and open hardware. This underlines Christopher Kelty's speculation as to why the task of defining hackers might be particularly challenging. The practice of hackers is all about introducing new entities into the world. That is to say, hackers create things which overturn existing concepts and established modes of representation (Kelty, 2008, p. 94).

A definition of the 'hacker' must therefore be conceived in such a way that it stays open-ended towards future developments. Open hardware is a case in point. This notion draws heavily from the methodologies and principles which were first worked out by free software developers. Many of the people now tinkering with hardware have a background as software engineers. Writing code and running it on home-brewed machinery are two sides of the same coin. Hence, the development of open hardware and free software overlap due to technical requirements and personal affiliations. A visit to any of the larger hacker conferences in Europe, such as FOSDEM in Brussels or Chaos Computer Club in Berlin, will provide an idea of the rapid expansion of open hardware projects in recent years. Furthermore, just around the corner is a new field of 'open source biology' (Hope, 2008). Arguably, these phenomena should be taken account of in a discussion about what hacking is.

A definition of the hacker which is not tied down to a single technical practice or technology can be found in the tradition of cultural studies. Hackers are interpreted here as one youth subculture among others. This approach has been put forward by Douglas Thomas (Thomas, 2002). The argument makes sense given the overlap existing between hackers and geek and fan subcultures. Cultural studies perspectives have a lot to contribute to the discussion of how to delimit the category 'hackers'. After all, subcultures are all about defining who belongs to the group and who does not. The comparisons offered by Thomas are valuable also because he stresses how the hacker milieu differs from most other subcultures. The identity of hackers is bound up with a practice rather than with a style. Thomas finds this to be of importance since it endows hackers with a greater amount of self-determination vis-à-vis external influences. In contrast, style-based subcultures are more easily swayed by commercial forces and are therefore less capable of resisting authority.

A common feature of many subcultures, and here Thomas makes no exception for hackers, is that their resistance tends to be understood in terms of a 'generational conflict'. Hackers are said to be rebelling against the authority of adulthood. I would not disagree that there are generational aspects to hacking. The stereotypical image of a hacker is a boy or a man in his early twenties. Nevertheless, the description of hackers as a youth phenomenon seems less and less valid the further we move away from the 1980s and the so-called 'golden age' of hacking. This is not only due to the aging of individual participants. Equally important is the progressive integration of free software development into professional life. A large majority of the contributors to free software projects are now working in the IT sector or are students on the verge of becoming computer professionals (Lakhani and Wolf, 2005). That Douglas Thomas fails to take this into consideration might be symptomatic of what has been traditionally a blind spot of the cultural studies approach, i.e. its neglect of the political economy. If the stress is placed on the generational aspect of hackers' resistance, then one will not take full measure of the stakes involved in the political struggles of hackers.

The reasoning above points to an alternative interpretation of hackers as a social movement. Two spokespersons of this perspective are Paul Taylor and Tim Jordan. I agree with them that there is much to be learned from social movement theory. An advantage of this approach is that it asks how hackers constitute themselves as a political subject and begin to act collectively. Inquiries of this sort become increasingly urgent the more hackers become entangled in struggles against new intellectual property laws, state surveillance and so on. I borrow extensively from social movement theory in two of my articles, 'Determining social change' and ''Free space optics in the Czech wireless community'. Nevertheless, I hesitate to put hackers on an equal footing with any other social movement, and I am unconvinced by the attempts of Taylor and Jordan to do so. In their writings they tend to focus on hackers with an overt political agenda, such as the Cult of the Dead Cow and the Electro-hippies. These groups belong to a faction within the larger constellation of hackers who sometimes go under the name 'hacktivists'. Some issues championed by hacktivists include gender equality, immigration rights and alter-globalization critique. In other words, much the same agenda as can be found in a politically schooled, leftist environment. There are places, for instance in Spain and Italy, where hackers and the anarchist movement are closely intertwined. Still, this is more of an exception than the rule. A case can be made for arguing that hacktivist politics is something deriving from an 'outside'. It does not capture the full spec-

trum of ideas which have grown from within the practices of hackers. An indication of this is the frictions which often arise between hacktivists and so-called 'techies', i.e. hackers who claim to be interested in technology for its own sake. This does not rule out that the latter can become politicised too. This can happen, for instance, in response to new intellectual property laws. However, this kind of political engagement has its own distinguishing features (Coleman, 2003). One risks losing sight of the specificity of hacker politics if pride of place is given to hacktivists, as opposed to politicised techies. The subcultural lens adopted by Douglas Thomas might therefore be more promising in registering the heterogeneity and contradictions of hacker politics.

Even more problematic is the proposition that hackers constitute a new class. McKenzie Wark claims that the hacker class stands in opposition to the vectorial class, in much the same way as the working class confronted the capitalist class in the past (Wark, 2004). I do not dispute the continued relevance of class analysis in a society where an ever larger section of the global population depends on a wage for its survival (Fuchs, 2010). A discussion about hackers can be fruitfully connected to the old question about the rise of a white-collar working class. For instance, Graeme Kirkpatrick has observed that the moral panic over hackers in the mass media started in the 1980s. It was at this time that the class composition of the computer profession begun to change. If computer programming had previously been a resort for the upper middle class, the spread of home computers meant that a growing section of the working class could now become involved (Kirkpatrick, 2004).

My problem with Wark's perspective is not that he uses class analysis, but that he does so exclusively from an abstract, theoretical point of view. He says very little about the people calling themselves 'hackers' and the subjective side of class formation. What needs to be explained, in my opinion, is the discrepancy between, on the one hand, subjective experiences of belonging to a class, and, on the other hand, objective class determinations. This is particularly pertinent in the case of hackers, since their self-image largely stems from college life, fan subculture, amateurism, and, sometimes, entrepreneurial aspirations. In other words, settings not firstly associated with wage earning and corporate organisation (Liu, 2004). This outsider identity seems to become increasingly out-of-sync the more free software development becomes integrated into professional structures. Andrew Ross was one of the first to argue that hacking should be seen in the light of labour conflicts. I have explored this idea in some of my previous writings (Ross, 1991; Söderberg and Dafermoes, 2009; Söderberg,

2009). I doubt, however, that much insight can be gained from interpreting hackers as a new class in their own right.

My main objection to Wark is that the everyday life of hackers hardly ever enters into his theoretical reasoning. The opposite problem is common in descriptive works about hackers. A number of well-researched books have been published in the wake of the success of the free software movement (Benkler, 2006; Moody, 2001; Weber, 2004). These tend to be written by academics who sympathise with ideas about information freedom. My reservation with regard this genre is that the self-representations of hackers are reported by the scholars down to the point that the exclusions, omissions and so on made by the former are faithfully reproduced by the latter. A case in point is the definition given in the *Jargon file*. Hacking is here presented as if it was all about writing software, resulting in an exclusion of practices classified as 'cracking'. While free software development is closely associated with positive values such as information sharing and transparency, the hacker subculture is just as much about secrecy and stealth. My basic claim is that the definitions provided by the people calling themselves 'hackers' cannot be accepted at face value. The definitions put forward by them, just as much as the terms circulating in the mass media, are the outcome of conflicts and negotiations. The benevolent, lawful free software developer is highlighted in order to improve the tarnished, public image of the hacker. These negotiations feed into the larger political struggles which hackers are involved in, concerning intellectual property laws, net neutrality and so on. It is not hard to see, then, why many academics want to contribute to the improvement of the public image of hackers.

The thrust of my argument so far has been that 'hackers' should be defined in a loose and open-ended fashion. The definition cannot be reduced to a single technology and related technical practices, such as writing free software code. I have hinted at the need for a definition which takes account of a shared culture. Reversely, however, the specificity of the hacker vis-à-vis other groups would be lost, if all references to technical practices were abandoned. Indeed, the words 'hacking' and 'open' have often been used indiscriminately. An example of this is when artists and activists involved in 'culture jamming' claim to be doing a kind of hacking. Against these claims, I believe that some connection to technical practices must be maintained. This is crucial if one is to make sense of the strong, meritocratic values of hackers. Being skilled is the central axis by which hackers distinguish themselves from lammers, n00bes and AOLers, to mention a few of the dismaying epithets for ordinary computer users. Furthermore, hacking does not concern just any technology. Otherwise, hackers could not be

separated from tinkerers and inventors at large. There must be a connection, however remote, to practices relating to infrastructures for information processing. A concrete example hereof is the hackers developing so-called 'open cars', such as OSCar and C'mm'n projects. On the face of it, their practices might not be all that different from what goes on in a motor club. Crucially, though, these development projects are linked to adjacent hacking activities. They are inspired by the methodologies used in free software development, and they subscribe to the same moral codes, such as the centrality of information sharing.

The definition I am myself drawn towards comes close to what has been proposed by Christopher Kelty. On the one hand, his ethnographic work suggests that there is a particular hacker or geek identity shared by people in many places around the world. He recognises that scholars need a concept for addressing this commonality. On the other hand, he is aware of the pitfalls of categorising such a heterogeneous collective which, to make matters worse, is always in the process of becoming something else. He evokes the notion of a 'public' to wed together these conflicting points of consideration. The concept of a public is sufficiently vague to include an unspecified number of diverging phenomena, while, concurrently, being coherent enough to allow for collective action. It is in its role as a counter-balance to power that Kelty finds parallels between the eighteenth century public and the present one. While the old public was tied to the spread of coffee houses and the news media, among other things, the public which is now emerging builds on free software, open network standards, and the like. He speaks of the latter as a 'recursive public'. Through this, Kelty wants to stress that this public is geared towards defending/expanding the conditions of its own existence. Crucially, this takes place simultaneously on a discursive level and on the level of infrastructure. The notion of 'recursion' captures well the apolitical 'techie' who has become politicised in response to new intellectual property laws. Defending the legal and technical infrastructure required for writing software is a way of sustaining the hacker community, and, in the last instance, ones own existence as a hacker.

There are also some areas where I have problems with Christopher Kelty's account. I do not agree with his decision to abandon the word 'hacker'. He argues that the term has become too loaded with connotations about subversiveness and/or criminality. Thus he prefers to use the word 'geek' instead (Kelty, 2008, p.35). I disagree with this choice for the following reason: the people in question still refer to themselves as 'hackers'. To them, at least, the meanings invested in this word remain pertinent. A second reason for sticking to the term hacker is that it foregrounds technical practices more than the term

'geek' does. Finally, I do not think that the notion of a recursive public exhausts the problems encountered when trying to define the figure of the hacker. It cannot do justice to, for instance, the element of labour conflict which becomes more pronounced as free software development is integrated into corporate structures and professional life. Aside from these differences, Kelty's reasoning about the 'geek' is close to my understanding of the 'hacker'. With this term I am referring to a loose constellation of people who share similar ideas and values, ultimately anchored in certain kinds of technical practices. These technical practices must in one way or another relate to infrastructures of information processing. Despite being heterogeneous and perpetually changing, the shared identity of hackers is verified in that they from time to time can act as a concerted, political force. In other words, they constitute a 'recursive public'. This public is recursive in the sense that it tends to act in response to threats to the infrastructure upon which it depends.

Between Constructivist STS and Critical Theory

In this thesis, the relationship between technology and politics is investigated through studies of the practices of hackers. I approach the relationship by drawing upon a range of theoretical traditions. For the sake of orientation, I will indicate some of the sources of inspiration which have, directly or indirectly, contributed to my reasoning. A turning point for me was to encounter the theoretical-political writings of authors like Slavoj Žižek, Jacques Rancière and Chantal Mouffe. In their own distinct ways, these authors have protested against a post-political social order. They have affirmed the continued relevance of the concept of antagonism for philosophical reflection. In addition, various strands of Marxism have enriched my writing at different stages. A non-exclusive list would include labour process theory, Autonomist Marxism and Open Marxism. Social movement theory, especially where it touches upon questions of epistemology, has been another source of inspiration in my work. However, the two theoretical traditions which my thesis leans most heavily on are critical theory and constructivist STS. In order to provide a concise and balanced summary of my intellectual journey, I will restrict the following discussion to a comparison between the latter two schools. Ideas from other theoretical traditions mentioned above will be brought in as a supplementary resource.

The relation between critical theory, on the one hand, and constructivist STS theory, on the other, has been a major theme throughout my research. I will elaborate upon this relationship by looking more closely at three authors who have engaged with the STS literature from a critical theory perspective. Most