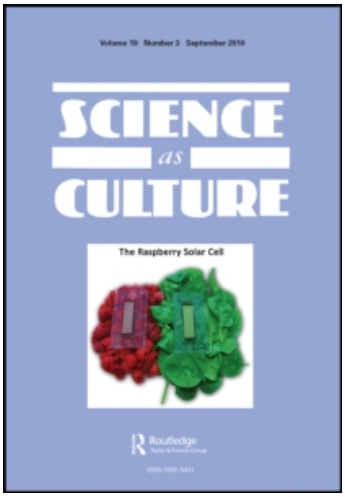

Science as Culture
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t713444970

Misuser Inventions and the Invention of the Misuser: Hackers, Crackers and Filesharers

Johan Söderberg[a]
[a] STS/Sociology, Göteborg, Sweden

Online publication date: 11 June 2010

To cite this Article Söderberg, Johan(2010) 'Misuser Inventions and the Invention of the Misuser: Hackers, Crackers and Filesharers', Science as Culture, 19: 2, 151 — 179
To link to this Article: DOI: 10.1080/09505430903168177
URL: http://dx.doi.org/10.1080/09505430903168177

Science as Culture
Vol. 19, No. 2, 151–179, June 2010

Misuser Inventions and the Invention of the Misuser: Hackers, Crackers and Filesharers

JOHAN SÖDERBERG

STS/Sociology, Göteborg, Sweden

ABSTRACT *The conflicts which have erupted over hacking, cracking and filesharing offer a stepping-stone for rethinking the involvement of users in innovation processes. As technical design processes invariably proceed in the shadow of established relations of social power, we can expect them to encompass conflicts over what constitutes the creative use of technology versus its misuse. The figure of the misuser calls attention to the importance of antagonistic relations in the mutual shaping of technology and society. Constructivist STS research has been criticised for neglecting the importance of antagonistic relations in favour of an emphasis on the limitless mutability of human/machine hybrids. The transformative effects of innovation processes on interests and subjectivities cannot be denied. But the induction of such transformations might be interpreted as a method through which struggles are conducted. This dynamic is particularly forthcoming in the case of filesharing, where users innovate precisely in order to overthrow the material practices upon which intellectual property law is founded. It is the intervention of law enforcement agencies in the process of drawing the line between users and misusers that makes the presence of an antagonistic relation manifest.*

KEY WORDS: Filesharing, hacking, cracking, innovation, misuse, antagonistic relations

Introduction

The sharing of music files became an instant hit with Napster in 1999. At its peak, the service had more than 26 million users. It came to an abrupt end with a court ruling in 2001 against the company behind Napster; but other filesharing systems

Correspondence Address: Johan Söderberg, STS/Sociology, Brahegatan 12C, Göteborg, 41501 Sweden. Email: johan.soderberg@sts.gu.se

0950-5431 Print/1470-1189 Online/10/020151-29
DOI: 10.1080/09505430903168177

immediately replaced Napster and the practice has proliferated (Menn, 2003). The methods for sharing files are becoming technically more advanced as they engage ever more people, and expand to include new kinds of information. The music-, film- and software-industries estimate that they lose billions of dollars annually due to unauthorised copying on the Internet, though the validity of these claims is a matter of dispute among economists studying the topic (Oberholzer-Gee & Strumpf, 2007). Still, the rhetoric about 'pirate copying' is intuitively compelling and has been instrumental in the lobbying for strengthened intellectual property laws. The efforts to uphold intellectual property on the Internet have turned into a slippery slope where more prohibitions are needed and more powers are granted to enforcement agencies.

For instance, copyright law has been extended from forbidding unauthorised copying into banning the development and distribution of software code which enables copying. This so-called 'anti-circumvention clause' was introduced in the US in the *Digital Rights Management Act* in 1998 and in the *EU Copyright Directive* in 2001 (2001/29/EC). Critics have protested that the clause does not just ban a single 'circumvention device' but has implications for the very knowledge of writing software code (Gillespie, 2004; EFF, 2006; Kirkegaard, 2006). An illustration hereof is the need which has arisen to exempt professional cryptologists so that they can go about their research in mathematics without risking prosecution under copyright law (Shah, 2004). A line must be drawn between recognised experts and lay experts in cryptology. It is therefore unsatisfactory to discuss copyright law as merely a showdown between content providers and their would-be customers. Mass violation of copyright law on the Internet presupposes creative and highly skilled practices from at least some of its many perpetrators. Subsequently, governing the technical know-how of advanced computer users has become paramount in the defence of intellectual property law on the Internet.

Given this background, the experiences of hackers, crackers and filesharers have a lot to contribute to current debates about 'lay expertise'.[1] Much research has been conducted in Science and Technology Studies (STS) and in Innovation Studies concerning users becoming involved in the development of science and technology (Callon, 1999). Some popular concepts are 'research in the wild' (Rabeharisoa & Callon, 2003), and 'user-centred innovation models' (von Hippel, 2005). Though these terms stem from different theoretical traditions and are applied to somewhat different situations, they roughly encircle the same phenomenon where innovation processes are taking place outside of firms, institutions and professions. Two often cited examples hereof are patient groups engaged in medical innovation and users inventing new sports equipment (Rabeharisoa & Callon, 2004; Luthje *et al.*, 2005). In recent years, the idea about engaging users in innovation processes has been adopted in policy documents about the 'knowledge society'. What invariably goes unmentioned in the official endorsements of user-initiated innovation is the acknowledgement that much of that creativity has been outlawed by intellectual

property legislations (Ashton, 2008). This article contributes to ongoing debates about lay expertise and user innovation by focusing on those cases which are opposed by law authorities. The purpose hereof is to bring attention to the discursive separation between legal and illicit uses of technology which I claim cuts straight through the literature about lay expertise.

My first key question is how this rhetorical separation is upheld through the construction of the 'misuser of technology'. In doing so, the article relates to an earlier body of literature on unruly users, including those who use products for purposes unintended by the manufacturers, or those who use technology for 'extremist' causes, or those who simply refrain from using certain technologies (Oudshoorn & Pinch, 2003; Eglash *et al.*, 2004). This study diverges from previous work in that it is strictly concerned with those novel uses of technology which come to be defined as illegal. Everything said here about misuse hinges on the intervention of law enforcement. Having said this, however, the legal grey-zone of misuse is understood to extend beyond those practices which have been explicitly criminalised. It also includes neighbouring activities whose legal status remains undecided for the time being. An example of the first is unauthorised downloading of copyrighted files from a filesharing network. An example of the latter is the writing of code enabling filesharing. Both of these activities are associated with criminality. Furthermore, in spite of the stress placed on the role of the law in defining the misuser, it should be clear that legislators are not alone in this endeavour. They are joined by computer security experts, news reporters, academics, as well as those accused of misusing the technology, in a continuous struggle to redraw the boundary between use and misuse.

It is true that very few hackers, crackers and filesharers have actually been sentenced to jail. Thus the reader might be led to think that misuse is of marginal relevance. Such an objection fails to take into consideration that millions of filesharers all over the world have been made susceptible to the punitive measures of the law. But my rationale for highlighting the criminalisation of some of these practices is a different one. I believe that the example of imprisoned hackers, however small their number, fills a void in our current understanding of lay expertise. As the legal theorist Carl Schmitt knew well, it is in the punitive system that the self-image of Western, liberal democracy has to face its own contradictions. He problematised the ideal of parliamentarianism as it was conceived by liberal-democratic formalists. Carl Schmitt called attention to the fact that peaceful deliberation always presupposes the violent suppression of hostile elements (Schmitt, 2007). In recent years, his writings have inspired a number of left-leaning critics who insist on the continued relevance of antagonistic relations against consensus-oriented, pluralistic liberalism (Zizek, 1999; Mouffe, 2005). In similar vein, this inquiry into misuse aims at laying bare the inescapability of antagonistic relations in studies of science and technology.

Antagonistic relations are implicit in the notion of misuse, since the label has been made up by someone opposing the activity in question. With the word

'antagonism' I mean something more than the Hobbsian 'war of all against all'. It implies that conflicts are linked to asymmetrical power relations and that those relations of power do not come about haphazardly but are systematic. Antagonistic relations understood in this way have disappeared from view in constructivist writings about technology. The relevance of (power) structures is downplayed in favour of an emphasis on multiplicity and contingency. Critics have protested that together with perpetually changing human–machine constellations, relations of domination and conflict are also constantly renewed (Hård, 1993). I believe that that reply is basically correct; but the response does not resolve the dilemma which constructivist STS writers have put their finger on, namely: how the formation of a political subject is possible when a closure on identities seems to be unachievable, due to a perpetually changing techno-scientific landscape? This is the second key question of the article.

The problematic sketched out above is much too big to be satisfyingly answered here. I will settle with making a few proposals for further inquiry. Firstly, I suggest that the concept 'cycles of struggle' in the post-Operaismo tradition offers a promising starting point. 'Cycles of struggle' describes how struggle is enacted through the continued reshaping of technologies and subjectivities (Holloway, 1992). Hence, the theoretical concept can be used to think about technology in the context of antagonistic relations between contending forces that nevertheless are fluid and under-determined. Secondly, I wish to point at hackers, crackers and filesharers as a good testing ground for trying out the concept of cycles of struggle. What makes these groups interesting is that they are positioned on the cutting edge of technological change. The subcultures of hackers, crackers and filesharers are extremely heterogeneous and fluid formations, yet, in spite of all flux, they have mobilised effectively against the agenda of enforcing intellectual property claims on the Internet. A factor which might have contributed to their formation as a political subject is the confrontations with law authorities and the construction of hackers as misusers.

The article is divided into three sections. The first asserts the continued relevance of antagonistic relations for STS research. My argument is advanced through a close reading of an article by Marc Berg, in which he criticises the school of Computer-Supported Cooperative Work (CSCW). My purpose is not merely to question Berg's position. His emphasis on the contingency of human/machine hybrids is taken as a stepping-stone towards an up-dated notion of antagonism. This leads the discussion to the concept of 'cycles of struggle' as mentioned above. The second section applies this concept to the context of hackers, crackers and filesharers. It will be argued that the idea of taking part in an epic struggle is constitutive of the hacker identity, but the outlines of this struggle are sketchy and there is no consensus about who the antagonists and the protagonists are. These many uncertainties notwithstanding, the laws against 'computer crime' testify to the presence of a relevant conflict line. By proposing the concept of the misuser in the third section of the article, I want to call attention

to the line which partitions hackers, crackers and filesharers and separates them from legitimate experts and users of computer technology. In my final remarks, I draw some conclusions concerning the concepts of 'cycles of struggle' and the 'misuser' in relation to ongoing debates on normativity in STS research.

The Debate on Interests and Antagonism in Relation to Computer Technology

Early campaigners of lay involvement in science and technology often relied upon a notion of antagonism. In the writings of Ivan Illich, for instance, amateurs were elevated in opposition to professionals and state-backed institutions (Illich, 1973, 1977). Similarly polarised concepts figured in the thinking of the appropriate technology movement (Slack, 1984), as well as among writers in the *Radical Science Journal* (Werskey, 2007), and in the Scandinavian school on workplace democracy (Ehn, 1992). The latter tradition was influenced by labour process theory, itself heavily indebted to Marxism (Braverman, 1974). According to labour process theory, antagonism as opposed to consensus is the characteristic feature of industrial relations. The most precise expression of antagonism is to be found in the conflict of interests between wage earners and whoever is paying their wages, but the issue cannot be adequately summarised in differing viewpoints on how to distribute economic returns. Embedded in this conflict is a contest over the design of the labour process itself. Building on this theoretical backbone, labour process theory interpreted technology in the light of a tug-of-war between managers and workers over who had control over the machinery (Wilkinson, 1983; Jeremier *et al.*, 1994).

From the outset, however, doubts were raised if priority should be assigned to antagonism. It was noted in the so-called Braverman-debate that firms rely less on coercion and more on giving workers leeway and building consensus (Friedman, 1977). Other critics of Braverman objected that the introduction of computers not only deskilled and replaced jobs but also created new employment opportunities elsewhere in the economy (Wood, 1982). The plausibility of these arguments grew in the face of the apparent feasibility of job enrichment programmes and experiments with participatory design at the workplace (Dickson, 1981; Knights *et al.*, 1985; Kensing & Blomberg, 1998; Heeles, 2002). Concurrently with this development, the validity of the concept of antagonism was questioned from a very different angle. A new generation of STS researchers that came of age in the 1980s based their reflections on science and technology in laboratory studies rather than in experiences from the shop-floor. They complained that labour process theory treated the interests of managers and workers as if set in stone. This argument was first advanced in a polemic that did not directly address the debate about industrial relations, but targeted the more general notion of 'interest' in science studies (Sismondo, 2004, p. 45).

The concept of interest had previously been elaborated by writers associated with the Edinburgh school. The truth claims of natural science were relativised by examining the interests and social structure behind scientific research. A source of influence was Marxist theories about 'class interest' (Barnes, 1977; Ylikoski, 2001, p. 118). The approach of the Edinburgh school was challenged by some STS researchers. Steve Woolgar protested that the interests of actors were treated as given in a way similar to how scientific truths had been taken for granted at a previous date. The notion of interests had replaced scientific facts as an autonomous, explanatory force. The problem was, according to Woolgar, that the cause–effect dichotomy remained intact. He demanded that interests must to be explicated too (1981). Woolgar engaged more directly with the subject of industrial relations in a book co-authored with Keith Grint. The same complaints against 'residual essentialism' and an alleged failure to dissolve dichotomies were here thrown against a cross-section of researchers that had written on work and organisation.[2] The argument was extended a few years later by John Law who underlined that the inclination among sociologists to use a relatively stable backcloth of social class interests to explain particular sets of beliefs belonged to an out-dated phase of the sociology of knowledge with its roots in Marx, Weber and Durkheim (Law, 1986, p. 11). The wariness against treating interests as given runs deep among contemporary STS researchers. For instance, it is an important criteria when Sheila Jasanoff delimits the idiom of co-production. She says that activist writers like David Noble, Langdon Winner and Richard Sclove:

> [. . .] deviate from the co-productionist thrust in S&TS by taking for granted certain social 'facts', such as the necessity of the alliance between economic and political power and the ordering of society according to well defined interests. Hence, in their writing, social formations such as capital or class are held off limits for analysis and not available for reconfiguration in new attempts to solve 'problems of knowledge' (Jasanoff, 2004, p. 31).

Langdon Winner's well known response to the general argument in constructivist STS is that its pledge to open every black box often ends up being politically empty (1993). Though I sympathise with his standpoint, my proposal here is not to reject constructivist reasoning *tout court*. The ambition with this article is instead to bring the critique against interest to fruition by enrolling it in a search for an updated notion of antagonistic relations. I will advance my position by examining in greater detail a text by Marc Berg called 'The politics of technology: on bringing social theory into technological design' (Berg, 1998). The reason for singling out Berg is that his case against labour process theory is pursued with reference to computer technology and user empowerment, themes that coincide well with the topic of this paper. The direct target of his polemic is the school of Computer-Supported Cooperative Work (CSCW). This school promotes the introduction

of participatory computer designs at workplaces and it shares some common ground with the Scandinavian school on workplace democracy (Greenbaum & Kyng, 1991; Johnson, 1998).

Marc Berg's line of argument closely follows the general critique of interests as outlined above. Berg objects to what he considers to be a rigid conceptualisation of the user on the one hand, and technology on the other. In the bulk of CSCW literature, Berg contends, it is assumed that relations between the predetermined categories of 'technology' and 'human work' proceed along a similarly predetermined axis, resulting in either more or less democracy at the workplace. This argument is posed against another research tradition where technology is portrayed as an independent, neutral force that determines social relations. The alternative offered by CSCW, according to Berg, does not go far enough in breaking with the determinism of its adversary. Stating that technology can either be utopian or dystopian depending on the actions of users is still too mechanistic and unilinear. Such an outlook fails to recognise that technology moves along multiple axes. He attributes this failure of vision to an inclination in CSCW to essentialise the distinction between humans and machines. Berg believes that the dilemma is to be resolved by constructivist STS theory where the technology–society dichotomy has been abandoned in favour of affirmations of continuously changing, human–machine hybrids.

My main objection against Berg's position is that he does not consider how antagonistic relations evolve together with ever-changing, human–machine hybrids. Berg's reluctance to reflect over antagonism shines through in his survey of the CSCW literature. His argument strikes out against two very different branches within CSCW, one with roots in Marxism and the other with roots in phenomenology. Though he is mainly preoccupied with criticising writers in the latter tradition, occasional remarks of approval suggest that he also sympathises more with the phenomenological approach (Berg, 1998, p. 469). In this branch of CSCW, the argument is built up around a tension between the functionality of technology and the situatedness of human work. The enemy that these writers take aim against is an over-belief in the universal usefulness of computers. It is thus they argue for an open-ended design process that enables the user to adapt the computer tool to shifting circumstances. Marc Berg is probably correct in suspecting that these writers elevate the user so that a fundamentally dominating and instrumentalist logic of technology can be kept in check. I agree with him on the fallacy of explaining technology with recourse to its ontology, but I remain unconvinced by the conclusion he draws from it: 'If we leave behind the illusion that technology's "fixed" ontology yields "fixed consequences", why can we not acknowledge that technologies can be fruitfully employed without the user's full insight in their modes of operation?' (1998, p. 481). This provocative question is thrown out as a challenge to the whole of the CSCW field, but the statement is only pertinent if we believe that the consequences of a technology are given by its ontology. His charge misses the mark if we instead base our assessment of a

particular technological design on the assumption that it will be enrolled by the stronger part in an asymmetrical power relation. That is the obvious point of departure for an analysis of computers at the workplace grounded in critical theory and/or labour process theory.

Berg makes a summary rejection of Marxist-oriented work within CSCW. Categories such as 'class' and 'capital' belong to a macro-sociological universe that many constructivist STS researchers consider to be illegitimate (Radder, 1992, p. 154; Golinski, 1998). Subscribing to this viewpoint, Berg declares that when such categories are postulated to explain things about technology and science, as they are in labour process theory, technological determinism is simply replaced with an equally reductionist, social determinism (Berg, 1998, p. 465). If we reject social determinism, Berg asserts, we cannot take the interests at the workplace for granted anymore.[3] The introduction of new technology will transform that setting into a different human–machine constellation. Since new technologies give rise to new subjectivities, it follows that the terms of conflict are unpredictable and continuously changing. The machine neither strengthens nor weakens the hierarchic organisation at a workplace, but alters the meaning of hierarchy as such. It is thus that Berg rejects the partisan standpoint for 'alternative' or 'democratic' technology, as advocated by scholars loosely associated with labour process theory.

Even so, Marc Berg acknowledges that it is valid to be concerned about the mechanisation of work tasks and hierarchies of domination, but he is scant on information as to how to counter these dangers. His only advice is to appreciate technology as an active agent. Thereby, the politics of technology will unfold in a: '[. . .] full-fledged realization of technology as a crucial, never fully predictable and potentially creative force' (Berg, 1998, p. 478). These rather vague assertions leave the reader with the impression that hierarchy and domination will be rendered obsolete due to the mingling of diverse actants and, as he puts it, the creation of 'new worlds'. It begs the question what these new worlds might consist of. At one point, however, Berg concretises his idea by proposing that the Internet could be such an example which promises to transform democracy as we know it (p. 479). This pointer gives away to what extent Berg's optimism is a child of the 1990s. It was then commonly believed that the Internet would level hierarchic organisation into egalitarian networks of participation. The iconic text announcing such a new dawn for republican virtue on the Internet was John Perry Barlow's *A Declaration of the Independence of Cyberspace* (Barlow, 1996).

Today it is clear that the 'governments of the industrial world', as Barlow named his adversary, did not perish due to the rise of new (cyber) worlds. Rather, the architecture of the computer network is being transformed in order to consolidate state power and ownership control over the Internet (Shiller, 1999; Mueller, 2002). This observation casts doubt on the strong emphasis which Berg puts on the fluidity of identities and institutions in the face of ever-changing human–machine hybrids. How to explain stability over time is a weak spot in the whole theoretical tradition Berg draws upon. One of the

objections often raised against 'Actor Network Theory' and related currents within constructivist STS is that its pledge to transcend the agency/structure dichotomy merely results in a strong bias towards agency (Bromley, 2004; McLean & Hassard, 2004).

Though I agree with this criticism, for now I will stay open to the possibility that Berg's theoretical approach can be justified in at least one specific area, that is, as far as youth subcultures on the Internet are concerned. A case in point which will be discussed later is the demand of filesharers to access information for free. The mobilisation behind this cause has evolved in tandem with the invention of peer-to-peer filesharing protocols, but even here there are some durables. Intellectual property law springs to mind. Antagonistic relations do not disappear in the computer network but change together with mutating human–machine hybrids. As for the workplace, we do not need to call upon macro-sociological theories about capitalism to recognise that some components in these hybrid networks, such as the legal arrangements of the firm and the employment contract, have proven to be rather stable over time. Pointing them out goes a long way to explain how old structures and animosities are reproduced from one wave of newness to the next. In making this assertion I basically follow Barry Barnes argumentation against Steve Woolgar in the interest debate: 'If one has the sense that social activity cannot be whimsically and arbitrarily modified, one may become curious about what it is which generates whatever resistance there is to modification' (Barnes, 1981, p. 494).

The epistemological priority which Berg assigns to contingency over structure goes hand-in-hand with a recommendation of studying technology on a case-by-case basis. Endorsements of case studies are stock in trade in the STS literature but merit a closer look in light of Berg's overall argumentation. The validity of the micro-sociological approach hinges on the criteria for selecting and delimiting the cases being studied (Pitt, 2001). That reservation is actualised by Berg's critique of CSCW. His argumentation is grounded in observations drawn from computer-guided methods used in the medical treatment of cancer, and in research on ancient Greek literature. These examples are hardly on parity with the cases being discussed in the literature he criticises. To make a stronger argument he would have to show the ever-changing, contingent identities and interests at a workplace, preferably one in the lower tier of the labour market. The reluctance to engage in such a discussion is symptomatic of the whole critique levelled against labour process theory by constructivist STS researchers. The absence of production in contemporary studies of users of technology was recently commented on by Nelly Oudshoorn and Trevor Pinch:

> This reminds us not only of the long and largely hidden inventive endeavours of 'common' people, but also of an important class of users that most STS studies have not yet focused sufficient attention on. These are factory workers and people who are users of machines and processes in the realm

> of production [. . .] The time is ripe to repair this imbalance (Oudshoorn & Pinch, 2008, p. 556).

This imbalance has probably had consequences for the theories derived from the empirical materials. Should we look at a call centre in Ireland, for instance, we are likely to find that the antagonism between wage earners and capital owners has lost none of its pungency due to the introduction of new communications technology (Mulholland, 2004). My claim can be defended without recourse to either technological or social determinism. It simply recognises that wage labour is a persistent construction that has been successfully re-invented across numerous ruptures, changes and multiplicities.

The continued relevance of antagonistic relations is the main insight to be recovered from older, production-oriented studies of technology. Factory machinery brings home the point that technology is seldom the result of deliberation alone. Due credit should be given to the manipulation, exclusion and suppression that often accompanies the settlement of a technological standard (Hård, 1993; Elzinga, 1998). If this basic point is forgotten, political conflicts are reduced to problem-solving. For instance, Ivan Illich's pledge for involving users in the development of science and technology was grounded in the idea of a struggle where the weaker part required assistance. In recent writings, in contrast, the argumentation rests on the benefits to society in general from engaging users in innovation processes. With such reasoning, it goes just as well to propose the opposite, as indeed Marc Berg does, and say that efficiency can also be enhanced by excluding users (Berg, 1998, p. 481). A discussion about user involvement framed in such a way turns consensus into the stable backcloth of the analysis. It reinforces the post-political condition that, according to Chantal Mouffe, dominates the social sciences nowadays. She has convincingly argued that without an awareness of antagonism, we abdicate from thinking 'politically', not to say 'democratically'. The pluralism of liberal ideology endangers the democratic idea because it refuses to give recognition to real conflicts in society. Instead, we are left with a discourse of rational governance and solving problems of knowledge (Mouffe, 2005).

This brings the discussion back to one of the key problematics in my article. Namely, how to square the point of Chantal Mouffe and others, i.e. the continuity of antagonistic relations, with Marc Berg's key insight that identities and environments are perpetually transformed by innovation? Part of the answer might be that the indeterminacy of technology has been overstated by an epistemological outlook which does not take into account antagonistic relations in the first place. In the words of Sungook Hong: 'If we ignore the differences between workers and managers and combine them into one category, that is, into humans, and thereafter focus on the relationship between humans and machines, then unpredictability pops out like a mysterious property of the machine' (Hong, 1998, p. 265). Though Hong is right in making the remark above,

I believe that there is more to the claims about the contingency of interests and identities.

Some ideas of how to take account of contingency while prioritising antagonistic struggle over technological change can be found in post-Operaismo thinking. The most well known representative of this school is Antonio Negri, though the writers gathering under the label are very diverse (Wright, 2002). In the context of the problem raised above, however, it suffices to stress one thing that all of these thinkers have in common. They believe that technological development is not something that conditions struggle from the outside, but is rather the outcome of struggle (Negri, 1996, p. 158). New technology is developed to overthrow the foundations from which resistance was first organised. The antagonists too are transformed in the process since they have to reinvent themselves in order to mount a new, effective challenge against their opponents. This dynamic, where modes of resistance are continuously dissolved and reconfigured, is known as 'cycles of struggle' (Holloway, 1992). The concept of cycles of struggle is consistent with the empirically well-grounded observation in labour process theory that factory machinery has often been introduced after a labour conflict in order to make workers redundant and weaken the strength of trade unions (Fink, 1998). Thereby I do not propose that antagonistic relations are the sole cause of innovation, though that is indeed the claim of many authors associated with post-Operaismo (Holloway, 2002). Here it suffices to assert that antagonistic relations are an important factor driving technological change and deserving of more attention.

To sum up this section of the article, the argument takes the malleability of interests and identities in the face of ever changing human–machine constellations as its starting point, but when we are asked for the reasons behind this frantic speed of 'creative destruction', part of the answer must be that the struggles between warring factions in society to entrench or overthrow relations of domination are a strong impetus to technological change. Technological invention, the flight from old identities to new ones, and the perpetual overturning of the terms of the conflict, are themselves instruments in a continuous 'cycle of struggle' between mutating antagonists. After having made this rather abstract statement from a theoretical horizon, the article will now move on to argue that such a dynamic can be witnessed in the production of interests, identities and technology in the computer underground.

Misuser Invention in the Computer Underground

It was suggested in the Introduction that hackers, crackers and filesharers provide an interesting case since the struggles they are immersed in are located at the cutting edge of technological change. In this respect, the computer underground seems to be well suited for the theoretical approach offered by Marc Berg. The enrolment of individual hackers, their identities and the causes they rally behind, have all metamorphosed together with each new

generation of computer technology. An example hereof is the eclipse of phone phreaks by hackers in the late 1980s, responding to the transition from analogue dialling systems to computer networks. New skills were required to master digital dialling systems. With the replacement of technical know-how came the inflow of a younger generation of hackers. Goals and struggles were framed differently by these people. While the overriding concern of phone phreaks was to find out ways of making free long-distance calls at the phone company's expense, a major struggle which present-day hackers are involved in is the possibility to access information (Scott, 2004).

Though the subjectivity of phreaks and hackers is highly malleable, the opposition that they have run into is less so. The ambition among states and firms to enclose software and other kinds of information behind copyright licenses and patents has been a relatively consistent, countervailing force. This agenda has been pushed at least since the 1980s when software was first recognised in law as an entity that could be owned.[4] Private ownership over software, and, by extension, over all other kinds of information, is jeopardised when hackers start to tinker with software code. Hackers then encroach on the same turf as corporations and professionals with regards to the construction of computer technology. This might be taken as an example of what Marc Berg has in mind when he endorses an alternative way of 'doing politics' by embracing the creative potential of technology (1998, p. 438). Rather than engaging in representative procedures to change laws on intellectual property, hackers 'materially refigure' these practices by intervening in the production of software code.[5] Their expertise in computer technology allows them to circumvent encryption schemes and access information for free. And, thanks to the user-friendly filesharing applications created by hackers, methods for sharing information can be scaled up to include a mass of ordinary, inexperienced users too. The self-interest of filesharers to act altruistically and share their information for free, and the problems this creates in a market economy which presupposes egoistic behaviour on the part of individuals, has been elucidated by Richard Barbrook (2002).

This challenge to the material practices which private property rests upon has not been allowed to pass. New laws against 'computer crime' have been introduced in the US and the EU. Copyright law has been extended from banning violations of copyright to include practices which enable such violations. A case in point is the anti-circumvention clause in copyright law which forbids hackers from writing code for the purpose of circumventing copyright protections. It goes a long way to show that an important aspect of intellectual property law is to regulate the know-how of advanced computer users (Gillespie, 2006). Even the completely legal activities of free software developers are inflected by intellectual property law. It prevents them from reading the source code of proprietary software applications, they are stopped from accessing technical details on network standards, and they are obstructed from learning about hardware specifications. This information is crucial in order for hackers to be able to optimise their

own technology and make free software compatible (and competitive) with proprietary solutions. Conversely, if free software became the standard solution it would risk undermining the enforceability of copyright law to the extent that the law is embodied in (proprietary) software code (Lessig, 2006). This is a compelling reason for speaking about hackers, crackers and filesharers in the same breath, in spite of the fact that they are distinct groups and only a few of them have been singled out as criminals. They are linked by the challenge which their different practices pose to intellectual property law. Furthermore, as will be discussed in the next paragraph, they are all susceptible to the construction of the hacker as a misuser.

Partly as a reaction to the enclosure of software behind intellectual property law, some fractions of the hacker subculture have become increasingly radicalised (Stallman, 2002). Public statements made by spokespeople of influential hacker organisations suggest that they think of themselves as underdogs in an epic struggle of some kind. For instance, in a keynote speech at the *Wizard of OS 3* Conference in Berlin in 2004, Eben Mogeln, at the time deputy director of the Free Software Foundation, declared that hackers were at the forefront of a battle against the monopolisation of information. This battle, he asserted, has been waged at least since the printing press undermined the monopoly of monasteries over text production. The fondness among hackers for making comparisons with the Protestant rebellion against the Catholic Church was noticed by Christopher Kelty in his ethnographic study of the hacker subculture (2008). Such metaphors paint the present conflict in vague contours which might not stand up to close scrutiny. Still, these statements must be taken seriously if we are to understand the meanings that hackers attribute to their endeavours, as well as to the technology produced by them. This can be illustrated by the WINE project, a Windows emulator for GNU/Linux. The project aims to make it easier for ordinary computer users familiar with Microsoft's applications to use the free operating system instead. The concept was born out of the animosity towards Microsoft held by many hackers. Providing an easier exit route for Windows users was perceived by the instigators of WINE as important in the contest between open versus proprietary computer standards.[6]

It should be stressed that these conflicts do not map onto the bi-polar confrontation between managers and workers that was axiomatic in the industrial conflicts addressed in labour process theory. This struggle cannot be exhaustively described as one waged between two stable fronts, the computer industry versus the hacker community.[7] A comment from Douglas Thomas' study of the hacker subculture is clarifying. He interprets hacking in terms of a clash between generations, where hackers signal a rebellion against the authority of adulthood. In the likelihood that the revolt of hackers will be recuperated by mainstream society and commercial forces, he writes: 'It is a subculture that resists incorporation by turning incorporation into opportunity' (Thomas, 2002, p. 152). He illustrates his counter-intuitive claim with reference to software programmes known as 'Trojans'.

These programmes appear to be useful applications but come with a secret back door which hackers can exploit to access the computer system.

The claim that Trojans correspond with the way the hacker subculture resists recuperation needs to be explicated a bit more. Perhaps the idea can be concretised by elaborating on the 'Trojan' qualities of the General Public License (GPL) in relation to copyright law. The purpose of the license is to prevent software developed collectively from being appropriated by a single rights holder. This is achieved by adding a few clauses to the copyright license agreement. An author choosing to license her work under the GPL abstains from the individual right to exclude other users. In return she enjoys the collective right not to be excluded from the work of others (Stallman, 2002). Thus, the free license bends the intellectual property system around an information commons and pulls corporations into this gravitational field. The computer industry is compelled to adopt software licensed under GPL because, answering to the market imperative of lowest costs, it cannot refuse free labour. By willingly giving themselves up for exploitation, hackers have found a way to influence the direction of the computer industry. The companies become entrenched in a computer architecture over which it holds few legal powers. This method of hardwiring an open computer solution into the economic system can rightly be described as 'Trojan'. Such an accomplishment would not have come about had hackers been too wary about not being exploited by commercial interests.

Invention is the key in this struggle, both the invention of new legal practices such as the GPL and software code like WINE. The upper hand is gained by generating new technologies and subjectivities faster than the opponent can contend with. This observation is far from novel. The same dynamic was identified when labour process theory argued that new machines were introduced by managers to put trade unions on the defensive. Visionary unions have therefore tried to extend their influence 'upstream' to include the development of technology, though usually without much success (Harley, 1986). In the computer sector, in contrast, the means to develop software technology have been diffused to the users. Thus, hackers and crackers can reinvent the material practices of the computer network and render legislation on copyright unenforceable. In this struggle, conducted over and through innovation processes, it is hard to make a final judgement concerning the meaning and political significance of any single artefact, since, combined in a novel way, it might serve a completely different purpose. I grant Marc Berg that, given the fleeting nature of this contest, a static conception of who's who framed as an ideological battle over fixed ends can become a liability. The reason is that one risks ending up like the general who is fighting the last war. Paradoxically, the lack of an intellectually coherent, political ideology among hackers might have advantages since it enables them to move faster, to be more promiscuous, and more creative.[8]

Another risk with making the confrontation between the computer underground and the computer industry into the centrepiece of the narrative is that it gives the

impression of hackers as a monolithic force of opposition. The absence of a firm or a profession at the core of the development process does not, however, leave us with a homogenous space of equals. A technological standard is never standardised for everybody, not even after the source code has been made publicly available (Star, 1991). Nominally speaking, it is true that every user has the right to read and modify free software, but it goes without saying that one has to know the programming language to be able to read the code. Hence, by removing legal and technical restrictions to access, the hacker movement foregrounds differences in skill level instead. Perhaps it is inevitable that the diversification of skills among users results in a new division of labour, both inside the computer underground and towards ordinary users (Giuri *et al.*, 2006; Howison *et al.*, 2006). In spite of a rhetoric cherishing openness and freedom of information, exclusivity is the universal benchmark which everyone is racing against. Having access to a high-security server or being the first to release 'warez' is testimony of superior technical ability, and with that comes peer recognition (Stewart, 2005). In his overview of the cracker scene, Ethan Mollick has described how, in the course of the lifecycle of the subculture, groups of knowledgeable 'elites' and less skilled 'kiddies' often find themselves on opposite sides in confrontations with law authorities. The first group is more likely in due time to adapt to a professional life, and perhaps to be recruited as security experts. They then end up defending law and order against new generations of 'kiddie' crackers (Mollick, 2005).

The heterogeneity of hackers, crackers and filesharers underlines that no sharp line can be drawn between their subculture and the computer industry. While the two have always co-existed in symbiosis, direct involvement of firms in the computer underground got a major boost in 1998 when Netscape took the decision to go 'open source'. Shortly after Netscape's move, multinationals such as IBM and Intel followed suit, which in turn helped to expand the market for small firms and freelancers working with free software (Moody, 2001). These firms make money from selling customised software, offering technical support and marketing services annexed to free software, or they use free software to lower overhead costs (Watson *et al.*, 2008). An indication of the extent to which the hacker subculture has been incorporated in the computer industry is given by the estimate that 41% of all free and open software projects are initiated and managed by firms (Camara, 2004). Likewise, statistics from 2008 on the Linux kernel reveal that more than 70% of the changes in the code were made by employees of computer firms (Kroah-Hartman *et al.*, 2008). It remains to be seen if this incorporation will turn out as an opportunity to resist. There is little doubt, in any case, that the perceived usefulness of free software applications to the industry and society has changed the oppositional image of the hacker. As will be discussed below, this fact has been called upon when the line between the user and misuser is renegotiated.

In this section of the article, it has been argued that the sensation of partaking in an epic struggle between two antagonists is constitutive of the hacker identity.

This idea is persuasive even though the subculture exists in close symbiosis with the computer industry and the outlines of their imagined struggle are sketchy. Arguably, hackers' agnosticism about who's who in the conflict resonates with the fact that their identities and interests are perpetually under-determined. It is not possible to know from one day to the next what the significance is of a licensing scheme or a software application, since these may serve a different purpose when combined with new business models or run on a different architecture.[9] This statement begs the question: with so much flux and uncertainty, is it at all possible to identify the contending sides in the struggle, and, subsequently, the existence of an antagonistic struggle? As was seen before, many constructivist STS scholars have answered negatively. The concept of the misuser is here proposed to give a different answer to the dilemma.

Inventing the Misuser of Technology

It is not without reason that this article seeks to gather all the associates of the computer underground under a single heading. Free software developers have been studied intensively in the aftermath of the commercial success of free software applications. Researchers have laid bare their motives, their mode of organisation, and the economic impact of their endeavours. Coupled with this interest is the expectation that free software development will foster democratic values or create a truly free market, or both at the same time (DiBona *et al.*, 1999; Kogut & Metiu, 2001; Weber, 2004; Feller, 2005; DiBona *et al.*, 2006). Crackers, and, as of late, filesharers, tend to be talked about in a different tone of voice. In the popular press, official reports and in some academic disciplines, discussions about cracking and filesharing are connected with 'computer crime' or 'piracy' and their technologies are given suspicious-sounding epithets such as 'viruses' and 'darknets'. The discussion is framed by a taken-for-granted need for restoring law-and-order on the Internet (Lilley, 2002; Hinduja, 2006; Wall, 2007). Borrowing a term from Ulrich Beck, this amounts to the same thing as a 'container theory' approach to user-initiated invention (2000). Benevolent software developers are placed in one container, maverick crackers and filesharers in another. My proposal here is that this discursive separation between the 'good' and 'bad' user of the same technology is not accidental. It provides a showcase of how the misuser of technology is being constructed.

Not only law authorities and the mass media, but academics too, have contributed to this construction. Long before the concept of computer crime arose, the behaviour of hackers had been described by social scientists as bordering on the pathological. Early ethnographic studies of hackers were coloured by the strongly felt suspicion in humanist scholarship towards technophilia (Eglash, 2009). Perhaps it is the long-standing, Heideggerian tradition in philosophy of denouncing technology which has influenced scholars to put a correspondingly negative spin on hackers. A case in point is provided by Joseph Weizenbaum, himself a

pioneer in the then embryonic field of computer science. Referring to a more general critique of technology within philosophy as a carrier of domination, he interpreted the obsessive behaviour of small groups of computer enthusiasts as an outgrowth of instrumentality. The joy they experience in programming is in fact a sign of a deficiency. Over-enthusiastic programmers crave and subsequently fail to establish the same sense of control over their everyday social relations as they seek over the computer. What lies behind their love affair with the machine is a 'will to power' that elsewhere goes unfulfilled. Weizenbaum argued that the corruption of power is intrinsic to the very practice of programming:

> The computer programmer, however, is a creator of universes for which he alone is the lawgiver. So, of course, is the designer of any game. But universes of virtually unlimited complexity can be created in the form of computer programs. Moreover, and this is a crucial point, systems so formulated and elaborated *act out* their programmed scripts. They compliantly obey their laws and vividly exhibit their obedient behaviour. No playwright, no stage director, no emperor, however powerful, has ever exercised such absolute authority to arrange a stage or a field of battle and to command such unswervingly dutiful actors or troops (Weizenbaum, 1976, p. 115).

Sherry Turkle expresses similar admonishments in her classical study of the hacker subculture but adds a feminist hue to her critique. These young men are unable to have close relations with other human beings and compensate for this through their affection to the machine. Like Weizenbaum, she think that the computer medium in itself gives a strong impetus to a will for mastery among some of its male users, a tendency reinforced by the closeness between computer technology and masculinity (1984, p. 208). The same theme of male fantasies of omnipotence acted out through absolute control over computer-generated microworlds is echoed in later commentaries on hackers. The closed world of the computer has been compared with the rule-bounded universe of games, and this circumstance has been suggested as an explanation for the obsessive behaviour of both hackers and gamblers (Edwards, 1996, p. 171).

The reference to compulsive gambling had already been made by Weizenbaum in his observations from a computing centre in the early 1970s. He described its members as dishevelled, with glaring eyes and fingers ready to strike out at the keyboard. Their attention was fully consumed by the computer screen, just as the gambler's gaze is transfixed by the rolling dice. Here, the social competence of the hackers is put in question, their physical attributes are portrayed in an unfavourable light, and, most significantly, associations are made with gambling and other unhealthy compulsions. Thus, the philosophically grounded critique of computer technology, and, by extension, its most enthusiastic users, contributed to a moral investment in the discourse about the hacker. The negative image of

hackers was cemented in the public eye in the 1980s and 1990s through a number of high-profile, law enforcement campaigns in the US against 'computer crime' (Thomas, 2005).

Moral panics about hacking have become the subject of lengthy debates both among hackers and scholars. Hackers use the acronym 'Fear, Uncertainty and Doubt' (FUD) to describe what they perceive as scaremongering by some computer firms seeking to marginalise the competition from free software. The interests of the computer security industry in playing up fear over computer crime and viruses have also been stressed by researchers (Taylor, 1999). Another reason might be a deeply rooted anxiety about technology in a society which is going through rapid transformations (Kozlovic, 2003). This underlines the generational divide known from earlier outbreaks of moral panic over other youth subcultures (Cohen, 1972; Thomas, 2002). Graeme Kirkpatrick has observed that collective worry over hackers coincides with a change in their class background. In the early days the computer enthusiasts were likely to be well-off and middle class. They were expected to eventually become part of a respected profession. Since the late 1980s, however, the class composition of hackers has changed as the lower middle class and working class have acquired access to consumer electronics. In line with the new demographics, the old fear of the mob has returned in a fear of hackers (Kirkpatrick, 2004).

So far into the discussion, the labelling of hackers as misusers has been treated as a top-down, one-directional act by the establishment. Of course, the struggle over representations is much more dynamic and ambiguous. This can most clearly be witnessed in current attempts to redeem the free software developer, and the subsequent creation of new categories of misuse. When hackers defend themselves against negative media coverage, they do so by making up their own discursive separation between users and misusers. Free software developers insist that the original meaning of the word 'hacker' is someone who shows ingenuity in the face of a difficult, technical challenge. The negative connotations of hacking, i.e. breaking into servers, picking digital locks, and writing viruses, are reserved for those labelled as 'crackers'. In quasi-official documents of the hacker subculture, the cracker is often described in demeaning words. Tellingly, it is the lack of skills of crackers and 'script-kiddies' which are being attacked most energetically (*The Jargon File*). Several other terms have been invented to characterise the same divide. A related distinction is that between 'white hat hackers' and 'black hat hackers'. The first group abides to the law, while the latter do not. These attempts at redefining the boundary between user and misuser have gained in credence as the usefulness of free software tools is more widely recognised.

For sure, the wish to redeem the hacker as a lawful, benevolent computer expert is not universally shared in the computer underground. While the old-school hacker ethic used to say that a hacker should not violate the law out of economic self-interest, it never opposed violations of the law *per se* (Levy, 1984).

The romantic image of the outlaw has held sway over the computer underground since the days of phone phreaks and Bulletin Board Systems. Hence, in some quarters of the hacker community, the branding of them as misusers is positively affirmed. The multiplicity of meanings attributed to the hacker as a misuser and the playfulness by which the label can be appropriated by hackers should not, however, overshadow the fact that there are real stakes in this contest over representations. The experience of mods and rockers suggests how outbreaks of moral panic redraw the conflict lines and the moral universes long after the media debate has subsided. In some cases, as is exemplified by the rave movement, moral panics can build up pressure for institutional change and new legislation (Goode & Ben-Yehuda, 1994). With the ability to define misuse in the public eye follows the power to create legal sanctions against such behaviour.

The intervention of law enforcement authorities highlights some commonalities between the rhetoric of computer crime and drug addiction. Legislation draws a clear line between the user and the misuser of drugs by declaring some toxic substances to be legal and others to be illicit. It suffices to mention tobacco and pharmaceuticals, however, to underline the ambiguities of this categorisation. While the discourse about the drug addict makes it look like a rather self-evident classification, a closer examination will reveal that the concept is highly equivocal (Klaue, 1999; Derrida, 2003). Perhaps the definition has less to do with the toxic substance, and more to do with the state of being out-of-control. Gerda Reith argues compellingly that the general anxiety in society with people who are overtaken by unrestrained desires is inscribed in the consumer society. The addict is the Other of the sovereign consumer. With addiction, the promise of free choice in the marketplace is cancelled out by the compulsion to consume ever-more (Reith, 2004).

These reflections by Gerda Reith apply to the rhetoric about the computer enthusiast as an adolescent whose use of computers has become excessive and unhealthy. Narratives of the sort are buttressed by social research which tries to link computer crime with a lack of individual self-control. Even software piracy has been explained according to this model (Higgins, 2005). The similarity with the discourse about drug addicts is also underscored by court rulings in the United States where hackers have been banned from using computers and mandated to attend rehabilitation centres after they have served their prison sentences. A case in point is Kevin Mitnick who was declared as the world's most dangerous hacker in news articles, in books, and even a Hollywood movie. Most of the charges against him proved to have been unsubstantiated, but the fear of Mitnick's compulsion for using computers to commit crime was such that he was jailed for four and a half years before being given a trial (Littman, 1997; Jordan, 2008).

The parallel between hackers and drug addicts ought not to be dismissed out-of-hand as mere guilt-by-association. On the contrary, it should be mined for insights into the relation between hackers and legal authorities. A step in this direction has been provided by Emilie Gomart and Antoine Hennion in their study of drug users

as passionate users of a certain kind of technology. In their article they remark on the learning processes which are taking place in communities of drug users. These exchanges of information go beyond just sharing experiences of drug consumption (Gomart & Hennion, 1999). Experimentation feeds back into user-centred innovation processes and product development. One example hereof can be found in the periphery of the rave movement and its latter-day off-springs (McKay, 1994). Small bands of advanced drug users engaged in amateur chemistry in order to invent new party drugs. A few things that these DIY-laboratories have in common with hackers and crackers are the collective innovation process and a passionate affection for the technology in question. On the flipside of the coin, the identity of both groups is affected by the illegal status of their activity and the stigmatisation which follows; but the law is not simply a negative, restricting force that acts upon the environment from the 'outside'. Among groups developing party drugs, for instance, the law has become a productive force in its own right. A strong incentive for innovation derives from the need to find out new combinations of molecules that have not yet been classified by law authorities.

It is in the same way that filesharing technology has advanced in tandem with harsher copyright laws and litigation against filesharers. The architecture of the first system for sharing files over the Internet, Napster, was only partially decentralised. The storage of files was disseminated to individual computers, but in order to find the files, users had to visit a centralised search index. This architecture provided the court system with someone who could be held responsible for running the Napster servers. Before the verdict against Napster was passed, however, hackers had developed Gnutella. It was a more decentralised architecture where both storage and the search mechanism were spread throughout the network. The absence of a ring leader to press charges against has forced the music industry to sue thousands of individual filesharers instead. Hackers are responding in kind by writing ever more sophisticated protocols that are radically decentralised and heavily encrypted (Oram, 2001; Menn, 2003). The lesson from this example is that the development of filesharing technology must be seen against the background of a larger conflict over intellectual property. If this conflict is erased from view, researchers will come to think that the innovation of peer-to-peer protocols appeared out of thin air, by the grace of well-meaning users.

Thus, the discussion is led to another similarity between drug addiction and computer crime, namely: the communicating vessels which run between communities of misusers and the industry. The innovations made by people branded as misusers are often appropriated by firms at a later date. For instance, the methods of cracking are borrowed by the computer security industry as a way to find flaws in computer systems. Skilled crackers are hired by companies for this purpose (Mollick, 2005). Another example is business ventures which pay crackers to get access to thousands of computers in order to spam the network with advertising. Likewise, the distributed method for storing and indexing files in a peer-to-peer network has proved advantageous over older, centralised

forms of data retrieval. The technique has been widely adopted in the computer industry. Even filesharing itself has been incorporated into the marketing strategies of content providers. A case in point is the company MediaDefender which helps media corporations in fighting against filesharing networks. One service offered by the firm is to make filesharing more cumbersome by flooding the network with junk files. As an added benefit, these junk files sometime carry trailers announcing new film releases. Consequently, filesharing networks have been turned into a marketing channel for the same companies who are officially condemning the practice.

These examples illustrate how cracking and filesharing have given rise to new business models at the forefront of the so-called 'information economy'. Firms wanting to be at the cutting edge of innovation have little choice but to follow the path of these users. The centrality of users to innovation processes is old news to innovation studies researchers (von Hippel, 2005). What has not been given much attention, though, is the extent to which such users find themselves on the wrong side of the law. Or, with different words, innovation studies have yet to study the extent to which the legal grey zone has become an incubator for the innovation economy.

This section has described how the concept of the 'misuser of technology' applies to hackers, crackers and filesharers. Legislation plays a major role in defining who the misuser is, but law authorities are not alone in contributing to the construction. Particularly intriguing is the appropriation of the label in the computer underground. With the invention of the free software developer as a respectable hacker, new distinctions are created between well-meaning users vis-à-vis misusers. Concurrent with this attempt to redeem the hacker, however, other groups affirm the negative associations now invested in words like 'black-hat hacker' and 'cracker'. To these people, the outlaw status heightens the excitement of belonging to the subculture. Hence, the intervention by law authorities has contradictory outcomes. It might even act as a catalyst for the inventive processes that legislators want to curb. Indeed, the legal grey zones have proved to be a productive environment for discovering new uses of technology and creating new market niches. The central claim made here is that the 'container theory' approach in much scholarly literature hides from view this interdependency between lawful uses and illegal uses of technology, and the degree to which respectable businesses depend on the latter.

Conclusion

At the heart of this article lies a discussion of the politics of technology. There have been many appeals in the last few years for the STS discipline to take a normative turn. From a few 'usual suspects' in the 1990s who complained that constructivist STS had been emptied of politics (Winner, 1993), these stray voices have grown into a chorus (Woodhouse *et al.*, 2002; Frickel & Moore, 2006;

Mirowski & Nik-Khah, 2007; Kirkpatrick, 2008; Mirowski & Sent, 2008; Pestre, 2008). This might reflect a trend in the social sciences more generally where the notion of antagonistic conflicts has been taken into renewed consideration. A number of scholars are dissatisfied with the common belief that Western societies have advanced beyond antagonistic (class) conflicts. They protest that the commitment to tolerance and pluralism which liberal democracy commends itself for is only plausible for as long as the eye does not fall on the limit to democracy laid down by the law (Ranciere, 1995, 1998; Zizek, 2000; Mouffe, 2005; Brown, 2008). This contradiction between the self-congratulatory ideology of parliamentarianism and the punitive system which it presupposes was first identified by Carl Schmitt (2007).

One of the key questions in this article is how the misuser of technology is constructed. The purpose of the concept is to introduce the insights of Carl Schmitt and his contemporary interpreters to debates about user-initiated innovation and lay expertise. The article takes issue with a tendency to discuss the inventiveness of users as chiefly a matter of peaceful deliberation and co-operation. It has been argued that those innovations which are caught up in antagonistic conflicts risk being displaced from the discussion as belonging to a different discipline, most likely criminology. Thereby the mutual interdependency between lawful and illicit uses of technology is rendered invisible. The separation of free software developers from crackers and filesharers in the literature about the computer underground exemplifies how the misuser is constructed in this way. By calling attention to those instances where lay computer expertise is confronted by law authorities, the article aims to demonstrate where deliberation has run its course in liberal democracies. The punitive measures of the legal system directed against hackers, crackers and filesharers give an indication that their struggles are structured around an asymmetrical power relation. Crucially, this argument can be made without having to rely on a 'stable backcloth of social interest' or falling prey to 'social determinism'.

The last point becomes important in relation to the second key question raised in the article, namely, how the idea of a struggle between two antagonists can be maintained even though their identities and interests are perpetually overturned by a changing techno-scientific landscape? The article highlighted Marc Berg as a representative of those STS scholars who believe that the notions of interest, and, consequently, antagonistic conflict, have become untenable due to the contingency of 'human–machine hybrids'. The counter-argument advanced here began with the observation that industrial conflicts have often been 'resolved' through the introduction of new machinery. Subsequently, the creative destruction of identities and interests can be understood as a tactical manoeuvre in a struggle conducted through innovation processes. This idea is consistent with the concept of 'cycles of struggle' developed by post-Operaismo thinkers (Holloway, 1992; Negri, 1996). The claim has here been applied to the struggles in the computer underground. Though hackers, crackers and filesharers lack a coherent

theory about the forces which confront them, they have nevertheless developed a self-consciousness as underdogs in an antagonistic conflict. This recognition has partly come about in response to persecution from law authorities and the construction of them as 'misusers of technology'.

The two lines of argument are joined together in an attempt to reinstate the concept of antagonistic relations. While doing so, however, the article has warned against the risk of throwing out the baby with the bathwater and giving up some hard-won insights from constructivist STS research. The ambition has therefore been to take its critique against interest as the starting point for an updated theory about antagonism. The difficulty consists in finding moments where relatively stable, political subjectivities and conflict lines crystallise in the midst of permanent flux. Addressing this problematic will be important for normative research of science and technology. It requires that the 'in whose interest'-question is spelled out without treating who 'who' is as a self-evident and fixed category. Though the contingency of interests needs to be taken into account, this must be done without following the constructivists all the way in dissolving interest conflicts into a seamless web of ever-changing human–machine hybrids. On this matter, Theodor Adorno's reply to Karl Mannheim is a pertinent comment also on the epistemological radicalism of Marc Berg and associated thinkers: 'Like its existentialist counterparts, [sociology of knowledge] calls everything into question and criticizes nothing' (Adorno, 1998, p. 453).

Acknowledgements

The author would like to express his gratitude to the anonymous reviewers, Les Levidow, Kean Birch and Mark Elam for their constructive comments on earlier drafts of this paper.

Notes

[1]The hacker is someone who primarily develops software code and the cracker is the name for those who break into computer systems. This straightforward definition will later be problematised and discussed as an example of how the misuser is constructed. The filesharer tends to be less knowledgeable about computers but utilises the tools made available by hackers and crackers in order to share information, often but not necessarily in violation against copyright law.

[2]Though the title suggests otherwise, the discussion never gets close to experiences of technology at the shop-floor. The main concern in the field study presented in the book, conducted by Woolgar at a computer manufacturing firm, centres on the discursive separation between the firm and its customers. The company is treated as an organic, well-oiled machine, and there is nothing to indicate that Woolgar has looked for or reflected over the presence, or absence, of discord inside that organisation (Grint & Woolgar, 1997).

[3]Here Marc Berg makes labour process theory into something of a strawman. He does not take into account the developments within this tradition in the aftermath of the so-called Braverman debate. Scholars subscribing to labour process theory tried to describe in richer nuances the

inter-dependence between workers and management, sometimes building on the work of Michel Foucault (Knights & Vurdubakis, 1994).

[4]Most countries extended their copyright law to include software codes in the 1980s in response to pressure from computer companies (Drahos & Braithwaite, 2002, p. 171; Newman, 2002). The same firms are now demanding that software should be protected under patent law (Klemens, 2006). This is already the case in the US and Japan while attempts to introduce software patents in the EU have been stalled by strong opposition from hackers, activists and small- and medium-sized computer firms. Extension of the patent system is in line with the rapid growth of intellectual property rights more generally. The academic literature on the topic is vast and I can only hint at some of the writings here (Maskus, 2000; Matthew, 2002; Sell, 2003; McLeod, 2003, 2007).

[5]The difference between these two ways of doing politics is not absolute. Hackers have also engaged in traditional forms of lobbying and street demonstrations. Their successful campaign in 2005 against the introduction of software patents in the EU is a case in point.

[6]See http://www.winehq.org/ (accessed 14 February 2009).

[7]The notion of a 'community of hackers' is, of course, problematic too. The notion that hackers and other Internet devotees belong to virtual communities was first proposed by Howard Rheingold (2000). His book sparked off a heated exchange on whether the Internet could be said to harbour any communities or merely be a substitute for them in the real world. Though the term has since become widely accepted, inflation of its use has led scholars to once more ask what is meant by 'community' (West & Lakhani, 2008). As for this article, I follow Maria Bakardjieva's retrospective of the virtual community debate. The demarcations between 'real–virtual', and 'public–private', which this debate hinged on, do not take us very far when we want to explore how the Internet is used. The togetherness and common action enabled due to communication through (private) computer terminals spans both of these demarcations making them valid to study in their own right (Bakardjieva, 2005).

[8]This somewhat abstract claim can be substantiated with an observation by Yuwei Lin. She remarks that the pragmatic attitude of hackers has facilitated a hybrid innovation model that mixes community and for-profit ventures (Lin, 2006). It could be said, then, that the very fuzziness of their 'boundary object', or, to put it differently, their lack of a coherent, political analysis, has allowed a large, heterogeneous mass of people to agree on a few key issues, just sufficient for them to collaborate on a FOSS project.

[9]This statement can be illustrated by the TiVo case. The TiVo machine runs GNU/Linux and the company formally abides to the General Public License. The free license has been rendered meaningless, however, since the user is prevented on a hardware level from accessing the source code. Hackers have coined the term 'tivoisation' to describe this strategy by firms to follow the letter but break the spirit of the GPL.

References

Adorno, T. (1998) The sociology of knowledge and its consciousness, in: A. Arato and E. Gebhardt (Eds) *The Essential Frankfurt School Reader* (New York: Continuum).

Ashton, D. (2008) Policy, passion, and piracy: drawing lines around innovation in a knowledge-based economy, *eSharp*, 12.

Bakardjieva, M. (2005) *Internet Society—The Internet in Everyday Life* (London: Sage).

Barbrook, R. (2002) The regulation of liberty: free speech, free trade and free gifts on the Internet, *Science as Culture*, 11(2), pp. 150–177.

Barlow, P. (1996) *A Declaration of the Independence of the Cyberspace*. Available at: http:/homes.eff.org/~barlow/Declaration-Final.html (accessed 13 February 2009).

Barnes, B. (1977) *Interests and the Growth of Knowledge* (London: Routledge).

Barnes, B. (1981) On the 'hows' and 'whys' of cultural change (response to Woolgar), *Social Studies of Science*, 11(4), pp. 481–498.
Beck, U. (2000) *What is Globalization?* (Cambridge: Polity Press).
Berg, M. (1997) Of forms, containers and the electronic medical record: some tools for a sociology of the formal, *Science, Technology, & Human Values*, 22(3), pp. 403–433.
Berg, M. (1998) The politics of technology: on bringing social theory into technological design, *Science, Technology, & Human Values*, 23(4), pp. 456–490.
Brand, S. (1974) Fanatic life and symbolic death among the computer bums, *Cybernetic Frontiers* (London: Random House).
Braverman, H. (1974) *Labour and Monopoly Capital—The Degradation of Work in the Twentieth Century* (New York: Monthly Review Press).
Bromley, H. (2004) Border skirmishes—gender, new technologies, and the persistence of structure, in: R. Eglash, J. Croissant and G. Di Chiro (Eds) *Appropriating Technology—Vernacular Science and Social Power* (Minneapolis: University of Minnesota Press).
Brooks, F. (1995) *The Mythical Man-Month: Essays on Software Engineering* (Reading, MA: Addison-Wesley).
Brown, W. (2008) *Regulating Aversion: Tolerance in the Age of Identity and Empire* (Princeton, NJ: Princeton University Press).
Callon, M. (1999) The role of lay people in the production and dissemination of scientific knowledge, *Science, Technology, & Society*, 4(1), pp. 81–94.
Camara, G. (2004) Open source software production: fact & fiction, *Mute*, 27.
Cohen, S. (1972) *Folk Devils and Moral Panics: The Creation of the Mods and Rockers* (London: MacGibbon & Kee).
Derrida, J. (2003) The rhetoric of drugs, in: A. Alexander and M. Roberts (Eds) *High Culture—Reflections on Addiction and Modernity* (Albany: State University of New York Press).
DiBona, C., Cooper, D. and Stone, M. (Eds) (2006) *Open Sources: The Continuing Evolution* (Bejing: O'Reilly).
DiBona, C., Ockman, S. and Stone, M. (Eds) (1999) *Open Sources: Voices From the Open Source Revolution* (London: O'Reilly).
Dickson, J. (1981) Participation as a means of organizational control, *Journal of Management Studies*, 18(2), pp. 159–176.
Drahos, P. and Braithwaite, J. (2002) *Information Feudalism—Who Owns the Knowledge Economy* (London: Earthscan).
Edwards, P. (1996) *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press).
EFF (2006) *Unintended Consequences: Seven Years Under the DMCA*. Available at: www.eff.org/wp/unintended-consequences-seven-years-under-dmca (accessed 14 February 2009).
Eglash, R. (2009) Oppositional technophilia, *Social Epistemology*, 23(1), pp. 79–86.
Eglash, R., Croissant, J. and Di Chiro, G. (Eds) (2004) *Appropriating Technology—Vernacular Science and Social Power* (Minneapolis: University of Minnesota Press).
Ehn, P. (1992) Scandinavian design: on participation and skill, in: P. Adler and T. Winograd (Eds) *Usability: Turning Technology into Tools* (New York: Oxford University Press).
Elzinga, A. (1998) Theoretical perspectives: culture as a resource for technological change, in: M. Hård and A. Jamison (Eds) *The Intellectual Appropriation of Technology—Discourses on Modernity. 1990–1939* (Cambridge, MA: MIT Press).
Feller, J. (Ed) (2005) *Perspectives on Free and Open Source Software* (Cambridge, MA: MIT Press).
Fink, D. (1998) *Cutting into the Meatpacking Line: Workers and Change in the Rural Midwest* (Chapel Hill: University of North Carolina Press).
Frickel, S. and Moore, K. (2006) *The New Political Sociology of Science—Institutions, Networks, and Power* (Madison: University of Wisconsin Press).

Friedman, A. (1977) *Industry and Labour—Class Struggle at Work and Monopoly Capitalism* (London: McMillan).

Gillespie, T. (2004) Copyright and commerce: the DMCA, trusted systems, and the stabilization of distribution, *The Information Society*, 20(4), pp. 239–254.

Gillespie, T. (2006) Designed to 'effectively frustrate': copyright, technology and the agency of users, *New Media & Society*, 8(4), pp. 651–669.

Giuri, P., Ploner, M., Rullani, F. and Torrisi, S. (2006) Skills, division of labor and performance in collective inventions. Evidence from the Open Source Software Projects, *LEM Working Paper*.

Golinski, J. (1998) *Making Natural Knowledge—Constructivism and the History of Science* (Chicago: University of Chicago Press).

Gomart, E. and Hennion, A. (1999) A sociology of attachment: music amateurs, drug users, in: J. Law and J. Hassard (Eds) *Actor Network Theory and After* (Oxford: Blackwell).

Goode, E. and Ben-Yehuda, N. (1994) Moral panics: culture, politics, and social construction, *Annual Review of Sociology*, 20, pp. 149–171.

Greenbaum, J. and Kyng, M. (1991) *Design at Work: Cooperative Design for Computer Systems* (Hillsdale, NJ: Lawrence Earlbaum).

Grint, K. and Woolgar, S. (1997) *The Machine at Work—Technology, Work and Organisation* (Cambridge: Polity Press).

Hård, M. (1993) Beyond harmony and consensus: a social conflict approach to technology, *Science, Technology, & Human Values*, 18(4), pp. 408–432.

Harley, S. (1986) *Work Transformed—Automation and Labor in the Computer Age* (Lexington, MA: Lexington Books).

Heeles, P. (2002) Work ethics, soft capitalism and the 'turn to life', in: P. du Gay and M. Pryke (Eds) *Cultural Economy: Cultural Analysis and Commercial Life* (London: Sage).

Higgins, G. (2005) Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior*, 26(1), pp. 1–24.

Hinduja, S. (2006) *Music Piracy and Crime Theory* (New York: LFB Scholarly Publishers).

Holloway, J. (1992) Crisis, fetishism, class composition, in: W. Bonefeld, R. Gunn and K. Psychopedis (Eds) *Open Marxism,* Vol. 2 (London: Pluto Press).

Holloway, J. (2002) *Change the World without Taking Power: The Meaning of Revolution Today* (London: Pluto).

Hong, S. (1998) Unfaithful offsprings? Technologies and their trajectories, *Perspectives on Science*, 6(3), pp. 259–287.

Howison, J., Inoue, K. and Crowston, K. (2006) Social dynamics of free and open source team communications, in: *Proceedings of the IFIP 2nd International Conference on Open Source Software*, Vol. 203/2006 of IFIP International Federation for Information Processing, Lake Como, Italy, pp. 319–330.

Illich, I. (1973) *Tools for Conviviality* (London: Boyars).

Illich, I. (1977) *Disabling Professions* (London: Boyars).

The Jargon File. Available at: http://catb.org/jargon/html/index.html (accessed 29 June 2009).

Jasanoff, S. (Ed) (2004) *States of Knowledge: The Co-production of Science and the Social Order* (London: Routledge).

Jeremier, J., Knights, D. and Nord, W. (Eds) (1994) *Resistance & Power in Organisations* (London: Routledge).

Johnson, R. (1998) *User-Centred Technology—A Rhetorical Theory for Computers and other Mundane Artifacts* (New York: State University of New York Press).

Jordan, T. (2008) *Hacking—Digital Media and Technological Determinism* (Cambridge: Polity Press).

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

Kensing, F. and Blomberg, J. (1998) Participatory design: issues and concerns, *Computer Supported Cooperative Work*, 7(3–4), pp. 167–185.
Kirkegaard, S. (2006) Outlawing circumvention of technological measures going overboard: Hollywood style, *Computer Law & Security Report*, 22(1), pp. 46–56.
Kirkpatrick, G. (2004) *Critical Technology—A Social Theory of Personal Computing* (Aldershot: Ashgate).
Kirkpatrick, G. (2008) *Technology & Social Power* (London: Palgrave).
Klaue, K. (1999) Drugs, addictions, deviance and disease as social constructs, *Bulletin on Narcotics*, pp. 1–2.
Klemens, B. (2006) *Ma+h You Can't Use—Patents, Copyright, and Software* (Washington, DC: Brookings Institution Press).
Knights, D., Willmott, H. and Collinson, D. (Eds) (1985) *Job Redesign—Critical Perspectives on the Labour Process* (Aldershot: Gower).
Knights, D. and Vurdubakis, T. (1994) Foucault, power, resistance and all that, in: J. Jeremier, D. Knights and W. Nord (Eds) *Resistance & Power in Organisations* (London: Routledge).
Kogut, B. and Metiu, A. (2001) Open-source software development and distributed innovation, *Oxford Review of Economic Policy*, 17(2), pp. 248–264.
Kozlovic, A. (2003) Technophobic themes in pre-1990s computer films, *Science as Culture*, 12(3), pp. 341–373.
Kroah-Hartman, G., Corbet, J. and McPherson, A. (2008) *How Fast it is Going, Who is Doing it, What They are Doing, and Who is Sponsoring It*. Available at: www.linux-foundation.org/publications/linuxkerneldevelopment.php (accessed 24 February 2009).
Law, J. (Ed) (1986) *Power, Action, and Belief: A New Sociology of Knowledge* (London: Routledge).
Lessig, L. (2006) *Code and Other Laws of Cyberspace* (New York: Basic Books).
Levy, S. (1984) *Hackers: Heroes of the Computer Revolution* (London: Penguin).
Lilley, P. (2002) *Hacked, Attacked & Abused: Digital Crime Exposed* (London: Kogan Page).
Lin, Y. (2006) Hybrid innovation: the dynamics of collaboration between the FLOSS community and corporations, *Knowledge, Technology & Policy*, 18(4), pp. 86–100.
Littman, J. (1997) *The Fugitive Game—Online with Kevin Mitnick* (Boston: Little Brown).
Luthje, C., Herstatt, C. and von Hippel, E. (2005) User-innovators and 'local' information: the case of mountain biking, *Research Policy*, 34, pp. 951–956.
Maskus, K. (2000) *Intellectual Property Rights in the Global Economy. International Economics* (London: Heinemann Educational; Washington, DC: Institute for International Economics).
Matthew, D. (2002) *Globalising Intellectual Property Rights—The TRIPs Agreement* (London: Routledge).
McKay, G. (1994) *Senseless Acts of Beauty: Cultures of Resistance* (London: Verso).
McLean, C. and Hassard, J. (2004) Symmetrical absence/symmetrical absurdity: critical notes on the production of actor–network accounts, *Journal of Management Studies*, 41(3), pp. 493–519.
McLeod, K. (2003) Musical production, copyright, and the private ownership of culture, in: J. Lewis and T. Miller (Eds) *Critical Cultural Policy Studies—A Reader* (Oxford: Blackwell).
McLeod, K. (2007) *Freedom of Expression: Resistance and Repression in the Age of Intellectual Property* (New York: Doubleday).
Menn, J. (2003) *All the Rave: The Rise and Fall of Shawn Fanning's Napster* (New York: Crown Business).
Mirowski, P. and Nik-Khah, E. (2007) Markets made flesh—performativity, and a problem in science studies, augmented with consideration of the FCC auctions, in: D. McKenzie, F. Muniesa and L. Siu (Eds) *Do Economists Make Markets? On the Performativity of Economics* (Princeton, NJ: Princeton University Press).

Mirowski, P. and Sent, E. (2008) The commercialization of science and the response of STS, in: E. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman (Eds) *The Handbook of Science and Technology Studies*, 3rd ed. (Cambridge, MA: MIT Press).
Mollick, E. (2005) Tapping into the Underground, *MIT Sloan Management Review*, 46(4).
Moody, G. (2001) *Rebel Code, How Linus Torvald, Linux and the Open Source Movement are Outmastering Microsoft* (London: Allen Lane).
Mouffe, C. (2005) *On the Political* (London: Routledge).
Mueller, M. (2002) *Ruling the Root—Internet Governance and the Taming of Cyber-Space* (Cambridge, MA: MIT Press).
Mulholland, K. (2004) Workplace resistance in an Irish call centre: slammin', scammin', smokin', and leavin', *Work, Employment & Society*, 18(4), pp. 709–724.
Negri, A. (1996) Twenty theses on Marx: interpretation of the class situation today, in: S. Makdisi, C. Casarino and R. Karl (Eds) *Marxism Beyond Marxism* (New York: Routledge).
Newman, N. (2002) *Net Loss: Internet Prophets, Private Profits, and the Costs to Community* (University Park, PA: Pennsylvania State University Press).
Oberholzer-Gee, F. and Strumpf, K. (2007) The effect of file sharing on record sales: an empirical analysis, *Journal of Political Economy*, 115(1), pp. 1–42.
Oram, A. (Ed) (2001) *Peer-to-Peer—Harnessing the Power of Disruptive Technologies* (Cambridge, MA: O'Reilly).
Oudshoorn, N. and Pinch, T. (Eds) (2003) *How Users Matter—The Co-construction of Users and Technologies* (Cambridge, MA: MIT Press).
Oudshoorn, N. and Pinch, T. (2008) in: E. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman (Eds) *The Handbook of Science and Technology Studies*, 3rd ed. (Cambridge, MA: MIT Press).
Pestre, D. (2008) Challenges for the democratic management of technoscience: governance, participation and the political today, *Science as Culture*, 17(2), pp. 101–119.
Pitt, J. (2001) The dilemma of case studies: toward a Heraclitian philosophy of science, *Perspectives on Science*, 9(4), pp. 373–382.
Rabeharisoa, V. and Callon, M. (2003) Research 'in the wild' and the shaping of new social identities, *Technology in Society*, 25(2), pp. 193–204.
Rabeharisoa, V. and Callon, M. (2004) Patients and scientists in French muscular dystrophy research, in: J. Sheila (Ed) *States of Knowledge, The Co-production of Science and Social Order* (London: Routledge).
Radder, H. (1992) Normative reflexions on constructivist approaches to science and technology, *Social Studies of Science*, 22(1), pp. 141–173.
Ranciere, J. (1995) *On the Shores of Politics* (Verso: London).
Ranciere, J. (1998) *Disagreement: Politics and Philosophy* (Minneapolis: University of Minnesota Press).
Reith, G. (2004) Consumption and its discontents: addiction, identity and the problems of freedom, *The British Journal of Sociology*, 55(2), pp. 283–300.
Rheingold, H. (2000) *The Virtual Community—Homesteading on the Electronic Frontier* (Cambridge, MA: MIT Press).
Schmitt, C. (2007) *The Concept of the Political* (Chicago: University of Chicago Press).
Scott, J. (2004) *BBS the Documentary*, (Video documentary).
Sell, S. (2003) *Private Power, Public Law—The Globalization of Intellectual Property Rights* (Cambridge: Cambridge University Press).
Shah, A. (2004) UK's implementation of the anti-circumvention provisions of the EU Copyright Directive: an analysis, *Duke Law & Technology Review*, 1(22).
Shiller, D. (1999) *Digital Capitalism: Networking the Global Market System* (London: MIT Press).
Sismondo, S. (2004) *An Introduction to Science and Technology Studies* (Malden, MA: Blackwell).

Slack, J. (1984) *Communication Technologies & Society: Conceptions of Causality & the Politics of Technological Intervention* (Norwood, NJ: Ablex).

Stallman, R. (2002) *Free Software, Free Society: Selected Essays of Richard M. Stallman* (Boston, MA: Free Software Foundation).

Star, S. (1991) Power, technologies and the phenomenology of conventions: on being allergic to onions, in: J. Law (Ed) *A Sociology of Monsters: Essays on Power, Technology and Domination* (London: Routledge).

Stewart, D. (2005) Social status in an open source community, *American Sociological Review*, 70(5), pp. 823–842.

Taylor, P. (1999) *Hackers—Crime in the Digital Sublime* (London: Routledge).

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

Thomas, J. (2005) The moral ambiguity of social control in cyberspace: a retro-assessment of the 'golden age' of hacking, *New Media & Society*, 7(5), pp. 599–624.

Turkle, S. (1984) *The Second Self: Computers and the Human Spirit* (London: Granada).

von Hippel, E. (2005) *Democratizing Innovation* (Cambridge, MA: MIT Press).

Wall, D. (2007) *Cybercrime—The Transformation of Crime in the Information Age* (Cambridge: Polity Press).

Watson, R., Boudreau, M., York, P., Greiner, M. and Wynn, D. (2008) The business of open source, *Communications of the ACM*, 51(4), pp. 41–46.

Weber, S. (2004) *The Success of Open Source* (Cambridge, MA: Harvard University Press).

Weizenbaum, J. (1976) *Computer Power and Human Reason: From Judgement to Calculation* (San Francisco: Freeman).

Werskey, G. (2007) The Marxist critique of capitalist science: a history in three movements?, *Science as Culture*, 16(4), pp. 397–461.

West, J. and Lakhani, K. (2008) Getting clear about communities in open innovation, *Industry and Innovation*, 15(2), pp. 223–231.

Wilkinson, B. (1983) *The Shop-floor Politics of New Technology* (London: Heinemann Educational).

Winner, L. (1993) Upon opening the black box and finding it empty: social constructivism and the philosophy of science, *Science, Technology, & Human Values*, 18(3), pp. 362–378.

Wood, S. (Ed) (1982) *The Degradation of Work?—Skill, Deskilling and the Labour Process* (London: Hutchinson).

Woodhouse, E., Hess, D., Breyman, S. and Martin, B. (2002) Science studies and activism: possibilities and problems for reconstructivist agendas, *Social Studies of Science*, 32(2), pp. 297–319.

Woolgar, S. (1981) Interests and explanation in the social study of science, *Social Studies of Science*, 11(3), pp. 365–394.

Wright, S. (2002) *Storming Heaven—Class Composition and Struggle in Italian Autonomist Marxism* (London: Pluto Press).

Ylikoski, P. (2001) Understanding Interests and Causal Explanations, PhD Thesis. Available at: ethesis.helsinki.fi/julkaisut/val/kayta/vk/ylikoski/understa.pdf (accessed 24 February 2009).

Zizek, S. (1999) Carl Schmitt in the age of post-politics, in: C. Mouffe (Ed) *The Challenge of Carl Schmitt* (London: Verso).

Zizek, S. (2000) *The Ticklish Subject: The Absent Centre of Political Ontology* (New York: Verso).