Preprint. Published as:
Hansen, Ejvind: "Hackers in Hiding: a Foucaultian Analysis"
***Philosophy & Technology*, 29 (1), pp. 5-19, 2016.**
http://dx.doi.org/10.1007/s13347-014-0182-7

Title and Abstract:
Hackers in Hiding: A Foucaultian Analysis

On several occasions Michel Foucault advocated a methodological turn towards what he called a "happy positivism". Foucault's emphasis on the surface does not deny the importance of structures of hiding, but understands it as a game in which the structures of hiding are viewed as contingently given. In this paper I will analyse the conflict between the hacker movement and the field of corporate interests. I argue that the introduction of graphical user interfaces and the maintaining of copyright interests are the contingent background of the ongoing conflict. By bracketing the analyses of hidden intentional structures, the happy positivist is thus able to facilitate deeper understandings of the prevailing structures of hiding.

Keywords:
Michel Foucault, hiding, hacking, business-ethics, open source.

Biographical note:
Ejvind Hansen is research director at the Danish School of Media and Journalism, where his focus is on the cultural implications of digital communication. In 2005 he defended his PhD dissertation, *Embedded Critique in a Tensed World*, in which he investigated the conditions for the critique of modernity and postmodernity constructed in Critical Theory, in the aftermath of certain insights into the embeddedness of our practices. His work is generally situated in the field of critical- and poststructuralist theory.

Anonymized references:
Hansen, E., 2005a, Embedded Critique in a Tensed World, 2005. unpublished PhD.-thesis.
Hansen, E., 2005b, "The Foucault-Habermas Debate: the Reflexive and Receptive Aspects of Critique", *Telos* 130, pp. 63-83.

Foucaultian Analyses of Hackers in Hiding

I. Foucaultian analysis of hackers in hiding

Some social phenomena rely on hiding. The hacker phenomenon is an example of this. Partly because some hackers operate in the hide; partly because some hackers reveal information others try to keep in the hiding. In other words, if there were no such thing as keeping a secret and using it to obtain power, hackers would not exist. Hackers straddle the precarious social value of the secret. They are defined by the fact that they try to counteract secrets, that is, that they try to gain unauthorized encryption knowledge, while a subgroup of hackers (blackhat hackers) also defines itself by maintaining a secret or hidden presence.

Since the existence of social phenomena that rely on hiding is so obvious it was in some respects quite paradoxical that Michel Foucault in his theoretical considerations emphasized a focus on the immediately apparent. This emphasis raises the question: what about those social phenomena that rely on hiding? If the focus on surfaces in Foucault's work actually denies him the ability to analyse such phenomena, it would be a serious problem with his work.[1]

In this paper, I will, however, demonstrate that surface analyses can indeed help us reflecting upon structures of hiding. I will argue that the bracketing of structures of hiding can help us understand ways in which they are contingent. Foucault's emphasis on the 'surface' and rejection of the reification of repression, concealment and disguise does not deny the importance of structures of hiding. On the contrary it focusses on them and investigates the ways in which they are contingent products of other aspects of the social apparatuses. By patiently uncovering the genealogies of positively given phenomena and events, it becomes possible to trace the social space in which the structures of hiding emerge. This overturns a long tradition in which the empirically given was understood as contingent on some essence that was structurally hidden. That concealment was the essential metaphysical fact, while the surface structure was the contingent 'shell' that had to be thrown away. The Foucaultian move changes the direction of dependence, and thus sees the hidden as a social product, which in turn produces effects.

When applied on the case of hackers, the Foucaultian approach can help us deconstruct some of the elements that constitute a struggle between hackers and proponents of more traditional business values. Two such elements are (a) the hiding of the code that constitutes software applications and (b) the hiding of (malicious, blackhat) hackers who are thought of as operating in the hide. The surface analyses presented in this paper will demonstrate the contingent background of both these elements, whereby the struggle itself turns out to be contingent. Applying this approach on the hacker phenomenon I will analyse routes that could be taken in the conflict between the hackers and the Internet commercial community that would sort through the demand for transparency, lack of filters and lack of boundaries, on the one side, and the regime of intellectual property rights advanced by business groups in the computing and cyberspace field, on the other.

II. The Hacker Phenomenon

The history of hacker cultures is complex. The mainstream image of hackers, propagated by Hollywood movies and the popular press, portrays them as selfish, thievish, dangerous persons.[2] Closer sociological and philosophical studies of hacker cultures reveal, however, much more complex structures of intentionality.[3] Originally hackers were programmers who made "hacks" – i.e. small, quickly programmed, utilities for certain rather specific purposes. In the early days of computer development (the 1960s and 1970s) hackers made important breakthroughs in computing

1 Critiques of Foucault's positivist strain can be found in Habermas 1985 and Flynn 1987.
2 An example of this can be found in Schwartz 2008. For another reflection on the emergence of this narrative, see also Wark 2004, esp. §73+271.
3 E.g. in Himanen 2001 and Wark 2004.

and computerbased networks.[4] Hackers were often affiliated with universities and the exchange of products happened through mechanisms that resemble scientific exchanges. The results were made publicly available in order to be improved by other hackers, and the personal reward was prestige and recognition. It has thus been argued that they were organized in a gift-culture rather than a traditional exchange culture (Raymond 2001, pp. 80-82; Himanen 2001, ch. 3):

> status is determined not by what you control but by *what you give away* (Raymond 2001, p. 80 – italics in the original).

However, the world in which hacking came of age co-existed with commercial businesses, like IBM, which managed vast and profitable computing machines and services, mainly for governments and large businesses. This peaceful co-existence was changed when PCs, which were developed outside of the penumbra of the established computer corporations, came on line, which rapidly led to them being connected. The shift to the mass sale of PCs is often associated with Bill Gates (the founder of Microsoft), who together with Paul Allen[5] developed a BASIC operating system for the Altair computer. Gates and Allen did not want to give away their product, but instead charged a fee for the software, thereby challenging the commons that had hitherto reigned among computing amateurs. Instead, they claimed property rights on the software they developed, in spite of the fact that, at this point, it was not certain what "commodity" was actually being paid for. Copying Gates and Allen's software did not deprive them of the use of the code – as would be the case in traditional robbery.

The special thing about information is that information can be shared without diminution. Gates and Allen claimed that, though computing had expanded and improved on the commons principle, it would never gain the concentrated marketing and improvement that would be entailed by the monopoly rent traditionally vested in an author or inventor with a copyright or a patent. In order to preserve economic gains for the designers and distributors, the Microsoft people – as well as other commercial interests – argued that it was necessary to take legal control of the distribution of software, or in essence, of codes.

Their main worry was thus control or protection of information (or more specifically: software[6]). The question is then: how do one protect information? The traditional answer has been by keeping it hidden (Thomas 2002, p. 39). In buying software the consumer, in effect, is actually contracting to pay a fee for *access* to an information product, but the information is not owned by the purchaser and cannot, legally, be distributed by the purchaser to those who have not paid a fee. Some agents are allowed to access the information product (because they have paid the license fee) while others are prevented from accessing the information. For those who are prevented from accessing the information, it will remain hidden. In other words, a wall is erected that *keeps information hidden* from those potential users that have not paid a fee (Thomas 2002, p. 39; see also ch. 3).

To sum it up, the commercial approach relies on the idea that the patent holder has the right to keep information (code) hidden in order to protect it, and hereby profitably exploit the information product that she offers. The conflict could be seen as one between the hacker ethos and the business ethos.[7] The hacker slogan, "information ought to be free", encodes an imperative: information itself

4 This is certainly not to say that the development of computing and the Internet was *solely* driven by hackers. Military interests were also important factors in the development (Abbate 2000). However, in this context we focus on the role played by hackers.

5 Monte Davidoff was also hired to program the mathematical routines.

6 In the present context I take it that it is fair to conflate *information* and *software,* since I contemplate the social exchanges that happen through computers and the Internet. In that context it makes sense to think of software merely as one among other kinds of information (such as texts, sounds, graphical expressions, etc.).

7 Historical events are never as simple as they appear in historical descriptions. It is thus probably not fair to claim that the tension between hacker- and business ethics was born as a clear cut when Gates and Allen published the Altair BASIC. In this connection the story, however, merely serves to illustrate the tension – not to give an exact account of its origin.

here is something like thoughts: it is impervious to the logic of property. To make it submit to the regime of property perverts both information and the legitimacy of property. On the other hand, proponents of informational proprietary rights argue that information should be among those things that can be patented. They reason that, just as with the invention of physical things, the design of a new software program involves development costs for material and labour such as is envisioned under patent laws meant to encourage innovation by allowing monopoly rights to the patent holder over a certain period of time.

We can distinguish two general hacking strategies within the hacking community. The first is defined by direct action, when hackers attack the commercial or state side by breaking through the systems of secrecy that have been put up in order to control the code (in recent years the most prominent example of this has been Wikileaks' publication of Iraq- and Afghan war documents (2010) and diplomatic exchanges (2010) (Leigh 2011) and to some extent also Edward Snowden's release of NSA material[8]). The second is defined by the open source movement, in which alternatives to proprietary applications are designed to be shared freely by being downloaded from the Internet. Within the first category it makes sense to distinguish between (1a) intrusions that aim at improving the defences of privacy (whitehat hackers) and (1b) intrusions that aim at the demolition of the security walls erected to guard private, propertized information.[9] The first group generally collaborates with the business approach (indeed, they are often employed by businesses) and I will thus not consider them in the following.

It is important to notice that hacker activities in the spirit of the original commons movement is driven by a desire to reverse the commercialization of information that arose as the economic and legal framework in tandem with the emergence of a massive, interconnected computing network that has penetrated all spheres of social life. From this point of view, the hacker acts in obedience to a political and ethical rationale that she views as greater than the letter of the law – making this parallel to civil disobedience. Seen from the business side of the conflict, computing property – software and architecture – is no different than any other commodity, and its unauthorized seizure or use is *theft.*

A compromise position between the two might grant certain points to the corporate case and examine certain subtleties in the hacker case, which responds to the deeply felt anxiety that the commercialization of information might entail the loss of some of the gains that have come from computers and the Internet.[10]

Thus, those acts of well publicized vandalism committed by some hackers should not blind us to the fact that hackers do not necessarily 'profit' from their activity – they are motivated, in part, by an ethical concern. They are less like thieves, then, in spite of the corporate perspective. Theirs is an endeavour to force the *revision* of the legal framework of proprietary rights (Thomas 2002, ch. 6; Galloway 2004, ch. 5; Vegh 2003). Blackhat hackers (at least those with a political agenda) see

8 Snowden was originally a hacker of the (1a)-type (Drew and Shane 2013), but then used his skills to reveal information that the state-authorities wanted to keep hidden.

9 This is the root of the classic public villainous image of the hacker, in which hackers are interpreted as "intruders" into private properties and domains. Hackers themselves often distinguish between hackers and crackers, where crackers are the ones who commit illegal activities, while hackers are *challenging* the prevailing system of legal controls, but without actually committing crimes. (e.g. Raymond 1996). From a political perspective I understand the motive behind this distinction (legal hackers do not want to be viewed as criminals). From the philosophical perspective I am pursuing, what counts is the common aspiration to "let information be free" – illegally or through the hacker commons.

10 Some of these gains and worries are articulated in Zittrain 2006 and 2009, even though he does not explicitly relate it to the hacker cultures. Zittrain demonstrates that the generative character of computer- and Internet-technologies is threatened. Computer- and Internet-technologies have traditionally been generative in the sense that the hardware is left open to unforeseen uses due to the openness to new kinds of software. Zittrain demonstrates how control-oriented commercial players have diminished this aspect of the technologies.

their work in terms of civil disobedience rather than as a crime.[11] The point is, in other words, that even though blackhat hacker activities are illegal, we do not understand these activities very adequately if our reflections end here.

While philosophers and cultural communications scholars have long observed that hacker cultures are complex, these subtleties are lost on the mainstream image of hackers, which generally goes along with the corporate version. In addition, of course, as the user population on the Internet includes almost the whole population of the developed world, more users have experience of the purely mischievous side of hacking – vira, trojans, spam, etc. To the extent that all Internet misbehaviour has been conflated with hackers, the hacker image has suffered. (Thomas 2002, ch. 6; Saco 2002, ch. 4; Ross 1991). From an older understanding of hackers as obsessed, creative nerds, we have now come to understand them as pathological, dangerous, hidden persons with mythic computer skills. How did this shift come about?

Various explanations of this question have been articulated. One reason may certainly be that some hackers commit unlawful acts.[12] At other times theorists have referred to the agendas of commercial interests (Ross 1991). According to gardner.com worldwide security software revenue has increased 111% from 2004-2008.[13] Software vendors thus have a large material stake in promoting general hacker anxiety, and do some by painting as menacing and dark a picture of hackers as possible. Given this balance sheet, it is not surprising to notice that the rhetoric of these vendors against the hackers is to the dark side.[14]

I will, however, demonstrate how a Foucaultian surface analysis might deconstruct the underlying tensions: It is true that the hacker phenomenon is founded on structures of hiding – structures that prevent certain issues from being positively accessible. The surface analysis will, however, show the contingency of the structures of hiding. Before doing this, we will, however, have to look into Foucault's account of the happy positivism.

III. Foucault's Account of the Surface Analysis

In his methodological reflections Foucault repeatedly stressed that nothing is *essentially* hidden in social relations. It was this position that motivated him to describe himself as a *happy positivist* (Foucault 1969, pp. 164-5; 1971, p. 72; repeated as "science positiviste" in Foucault 1990, p. 42). His self-affiliation with the term "positivism" was not intense. In fact it was primarily introduced as a polemical response to a critical review of his *Les mots et les choses*, but the focus upon the immediately given structures and phenomena (at the cost of deep hidden structures) was also emphasized in later writings (Foucault 1963, pp. xii-xiv; 1971, pp. 53-5; Foucault 1976, pp. 121-35; 1977a, pp. 179; 1984, p. 575; 2004, p. 21).[15]

---

11 The relationship between hackers and civil disobedience has been reflected on several occasions – e.g. in Taylor 1999; Klang 2004; Vegh 2003. See also Bedau 1991.

12 In the hacker literature, it is common to refer to the Morris Worm as the point where hackers lost their public innocence: on November 2, 1988, R.T. Morris launched an Internet-worm that, apparently by mistake, infected many systems, with subsequent repair costs ranging from $200 to more than $53,000 for each infected system.

13 http://www.gartner.com/it/page.jsp?id=496491, http://www.gartner.com/it/page.jsp?id=697307, http://www.gartner.com/it/page.jsp?id=1031712

14 Examples of this can be found on the following links:
Symantec: https://forums.symantec.com/syment/blog/article?blog.id=grab_bag&thread.id=98
http://eval.symantec.com/mktginfo/enterprise/fact_sheets/ent-datasheet_cybercrime_security_threat_trends_for_2008_01-2008.en-us.pdf
McAfee: http://www.avertlabs.com/research/blog/index.php/2008/01/07/a-banner-year-for-malware-digital-threats-and-the-security-industry/
Trend Micro: http://blog.trendmicro.com/will-2008-really-be-the-year-of-the-rat/
Kaspersky: http://www.kaspersky.com/news?id=207575629

15 It may be objected against this list of references that they are not comparable, because they are taken from quite differing contexts, and Foucault often emphasized (e.g. in Foucault 1969, p. 28) that it was important to approach differing phenomena in differing ways. That is true, but still he did actually at some instances articulate methodological reflections, and the dispersion of references shows that this was a continuous aspect of his approach.

Foucault's positivism indicates a focus on the positively given in order to identify the circumstances in which the hidden is produced, and in which the hidden produces its effects. Foucault does not hereby mean to deny the reality or significance of hidden entities. Foucault's positivism should thus not be conflated with the logical positivism, although it shares with the latter the common starting point that hidden (social or metaphysical) structures always are contingently founded and should be revealed as such. However, unlike the traditional positivists, Foucault does not dream of a world of absolute transparency. He does not think that contingent structures necessarily should – or could – be avoided. The "happiness" of his positivism means that he seeks to reveal what is *made possible* through the social and metaphysical structures in order to understand the surfaces better – not necessarily to avoid such structures in general.[16]

Foucault wants to investigate the "monuments" in their monumentality:

> To be brief, then, let us say that history, in its traditional form, undertook to 'memorise' the *monuments* of the past, transform them into *documents*, and lend speech to those traces which, in themselves, are often not verbal, or which say in silence something other than what they actually say; in our time, history is that which transforms *documents* into *monuments*. (Foucault 1969, pp. 14-5 – italics in the original)[17]

In this passage Foucault describes a decisive aspect of the positivist turn of his approach. Instead of focussing upon what the objects of research might be saying *between* the lines (the implicit, hidden messages), it should be the aim of the analyst to focus upon the objects as they are produced in their actual positive shape. According to Foucault, traditional historical analyses tend to focus upon the *significance* of the studied objects – in their connection to other objects, or what they are "saying" in the ongoing historical "discourse". The problem with this approach is that it *reduces* the objects; the horizon of analysis is limited to demonstrate how the objects *connect* to existing discursive formations. Instead of focussing upon the underlying meanings (how the objects *document* certain ongoing discourses), Foucault suggests that we analyse the objects in their own positively given being (as *monuments* in themselves).

Another, related, aspect of this approach is the rejection of the implicit claim in traditional approaches that the most truthful approach towards the analysed object is the interpretive approach.[18] Foucault deprecates the notion that the analyst's job is to discover the existence of hidden (mystical) grounds for the appearance of visible objects. We do not have to analyse an object on the assumption that it expresses something necessarily hidden; even though it may be true that some mechanisms are *actually* hidden, they are not *necessarily* so.

Even though it is indeed possible to reveal hidden structures, and that they can be revealed through interpretation, the hidden character of the structures does not mean that they are *essential* in some sense. The aim of Foucault's positivism is thus to defuse the confusion of hiding and essentiality (Foucault 1969, pp. 164-5; 1971, p. 72). The focus upon the positively given guides the analysis towards the seemingly disparate, the singular, the modes of succession, the speed of the dispersion of discourses, and away from positing hidden mechanisms that are *universally* significant and apply according to an atemporal logic. In analysing the positively given the only interesting questions concerns its actual insistence in some prevailing discursive formation. The gain of such analyses is that by bracketing transcendental unities, it becomes possible to detect new aspects of

16 Unlike logical positivsts, Foucault does not subscribe to Occams razor.

17 Translated by Alan Sheridan in *The Archaeology of Knowledge*, London: Tavistock Publications Ltd., pp. 8-9.

18 Even though Don Ihde to some extent draws on Foucault's work, Ihde's turn towards a material hermeneutics (e.g. in Ihde 1998) would thus probably not gain Foucault's approval. And in the same vein with Andrew Feenberg: Even though Foucault might be sympathetic with Feenbergs point that we should stay open for the search of different *potentials* of technology (Feenberg 2002); and that there is too much focus on "goals" in the development of technology (Feenberg 1992), he would be more reluctant as to the claim that a interpretive search for meaning is the obvious theoretical approach when analysing technology.

social relations, because it becomes possible to articulate new kinds of questions.

However, what about the hacker? Hackers are understood under the assumption, by both hackers and their corporate enemies, that what is hidden thereby gains more power, as if from the hiding itself. Is it possible, then, to analyse the hacker phenomenon on positivist assumptions?

> What is needed is a study of power in its external visage, at the point where it is in direct and immediate relationship with that which we can provisionally call its object, its target, its field of application, there – that is to say – where it installs itself and produces its real effects (Foucault 1977a, p. 179[19]; see also Foucault 1969, pp. 142-5).

Foucault's main interest is to examine power in its immediately visible forms – rather than to postulate that power is 'held' by something going on beneath the surface. Given that this seems to contravene the assumption of both hackers and their opponents in the computing world one wonders whether this does not contradict the Foucaultian premises and makes it impossible, proceeding from such premises, to analyse hacker cultures as a social phenomenon?

In the following section I will argue that, however strong the appearance, we would do better to adopt a Foucaultian approach by dispensing with ontological claims about concealment. This puts us in a much stronger position to understand the relation between hackers and the general computing community.

Foucault's position was not that the hidden phenomena do not have an existence or relevance in social practice, which would transform a methodological claim into one about some criteria of what does and does not really exist. To rule out hidden phenomena as a sort of delusion would certainly demonstrate an outrageous ignorance as to important aspects of power relations – especially in an approach such as Foucault's, where the question is about the relationship between power and knowledge.[20] Foucault's mission was rather to bring the structures of hiding into play, and in so doing making clear that structures of hiding are products of power struggles. The structures of hiding are contingent answers to a desire of informational protection. Any claim to universal validity made on their behalf is subverted by the contingent position in the historical trajectories. Through the analytic presupposition that the hidden always is based on visible sources, the hidden loses its mystifying essential status and takes its place as a factor of the struggles that define regimes of control; thus the hidden becomes definitionally contingent. For in fact the question is not whether hidden phenomena exist – it is rather how they exist as products of contingent power struggles.

IV. Analysing the Hacker Phenomenon as Structures of Hiding

I will demonstrate how this analysis of the visible and the hidden as forms traversed by the structures of control may help us theorize the conflict between the Internet commercial community and the hacker community, with their different ethical orientations and different views of concealment. Both sides rely functionally on structures of hiding, but neither of them are universally valid. A Foucaultian analysis of this setting will take into account (1) which *types* of hiding are in play, and (2) which power struggles have led to them – in order to show how the object of analysis is contingent.

But what is the larger issue governing what is kept hidden? On the one hand, proponents of commercial interests have joined the project of propertization with the secrecy approach to software and information in order to control both its potential to be copied and its functioning. On the other hand, the opposing side, in this paper represented by the hackers, also operates within various paradigms of hiding; the blackhat hacker who breaks through the propertized defences operates in

19 The translation of the passage is taken from Kelly 1994, p. 35.

20 Foucault's awareness of this is obvious in Foucault 1976 where he (among other things) discusses the logics of censorship (p. 111) and how ars erotica constitutes a knowledge that must be kept secret (p. 77).

the hiding, in order not to be "caught".

Hackers are thus thought of as hiding from the public attention. However, the Foucaultian quest for surface analyses urges us to reflect upon the power structures that have led to this situation. Which structures facilitate the hiding of the hackers? Here, we can gain help from reflection upon prevailing social relationships that define the social space of the hidden in the total cyberworld picture. In particular, we should attend to the gap between end- and expert users in the computer world. When hacking started getting noticed in the 1970s, pure end-users (with no programming insights) were a relatively small group. However, after the PC revolution, end-users, in one way or another, comprise most of the adult population of developed countries.

The introduction of graphical user interfaces has accentuated this situation by making computers accessible to users who have no coding skills or knowledge whatsoever.[21] The introduction of a graphical interface as a new surface interpretation of computationally mediated communication on the one hand creates vast new affordances for computers, making them much more valuable to end-users. At the same time, however, this increases the gap between the sensual representation that is the end-user experience and the computational mechanisms that are the vehicle for that experience. We know that *something* is "going on" beneath the graphical surface, but we generally have no understanding whatsoever of the meaning of the bits of code we might encounter in our ordinary routines, or of the way the system works (this point is also articulated in Stallman 2002, p. 49-50). Users with mainstream technical abilities are thus at the mercy of expertise advice. This exposure is coupled with a disturbing sense that one depends on *something* that is going on beneath the surface (behind the interface) which one does not understand.

The combination of vulnerability and dependence gives rise to a feeling of lack of control among end-users. Although the codes and devices that run the computer are not technically hidden, they seem to be going on underneath the overt computer experience, and they seem utterly incomprehensible to anyone without a specialized understanding of computing. Hence, for the end-user, the black box of the computing mechanism is one that gives rise to mysteries and mythologies, especially when some routine breaks down – when something doesn't work.

The prevailing mainstream account of hackers feeds directly into these anxieties. An important aspect of the anxiety about hackers is that they are able to do things with computers of which the user has no comprehension – and due to various rootkit techniques they can do it in disguise (Hoglund/Butler 2005). We are therefore always exposed to the potential threat of hacker interference – and often, we do not even know when it is happening. The popular image of hackers is of people using their specialized skill to affect hidden changes at a distance, using the technology of connectivity that is intrinsic to personal computing; this is an important part of the mythology that surrounds them (Thomas 2002, pp. 32-3+45+153).[22]

In this reading, the struggle between hacker- and traditional business ethics is based on certain structures that code what is manifest or hidden. On the one hand, hackers are easily slotted into a paranoid narrative because they operate on a code level behind the curtains of graphical interfaces – i.e. on a level that is opaque to the average end-user. On the other hand, the commercial owners of the information (the software) take interest in maintaining these structures of hiding, because the limited knowledge of the fundamental codes makes it possible for them to protect their copyright interests.

The opaqueness of the underlying computational operations is thus partly a product of the success of the graphical user interfaces: The graphical user interfaces have opened the world of computers to people who are not computationally literate. However, at the same time, the opaqueness has been further accentuated by the corporate interest in erecting the bars to access the codes in order to sustain their copyright interests. In the traditional business approach, to commodify code requires that it must be secured – that is, it must be kept hidden – in order to

21 This is a point elaborated in Thomas 2002, ch. 2 & 6.

22 An elaborated account of how the unknown builds anxieties, can be found in Douglas 1992.

prevent others from plagiarizing it. It is in this way that the prevailing structures of hiding is merged with the prevailing paradigm of computer use.[23]

The surface analysis thus reveals how present structures of hiding on the one hand emerge through a successful incorporation of a graphical surfaces (or interfaces) that facilitate the entry to the computer world for lay users, while at the same time alienating the users from the underlying computational structures. On the other hand it is accentuated by commercial interests in protecting the copyright interests of the owners. Both interests are legitimate. The question is, however, if the prevailing structures of hiding are the best answers. In the next section, I will suggest that this diagnose could be used prescriptively to suggest changing the structures of hiding. The payoff to seeing how contingent concealment is on the manifest surface is that we can further see the hidden as variable, produced, and changeable.

V. Restructuring the Structures of Hiding

So far, I have diagnosed the enunciative function of the prevailing structures of hiding in the field of software development with reference to the historical trajectory of computing. It was made clear that the graphical surface facilitated the entry of lay users to the computer world, but at the same time alienated the users from the computational structures. Hackers derive their strategy and charisma from their concealment, which is made possible by the absolute separation between the users and the code. Furthermore it was shown that the business approach exercises its patent rights by hiding the code in order to generate revenue by selling information products.

Given these factors, it now remains to be reflected how these surface analyses can help reconfigure the prevailing structures? I will argue that the impulse motivating the *open source* movement is an attempt to do just this. The open source movement arose from within the hacker movement as a compromise formation that acknowledged the legitimacy of commerce while at the same time preserving, as much as possible, the information commons (Perens 1999, p. 173; see also Raymond 1999).

The surface analyses in the preceding sections revealed that the conflict between business- and hacker ethics is based on strategies in the game of hiding that partly derive from the evolving graphical user interfaces, partly derive from the copyright motive in software development. The hacker, concealed in the world of code, produces anxiety in the very end-user that she claims to serve.

Now, the gains of the graphical user interfaces obviously refutes a return to non-graphical user interfaces; it is, however, not certain that we only should have a choice between accessing the software through graphical interfaces or through binary executable code. Furthermore, the copyright motive might be reconfigured. As a consequence of the conflict, some proponents of the hacker community suggested that the criterion of traditional copyright should be *replaced* with a criterion of "prosperity and freedom of the public in general" (Stallman 1991). They argue that the freedom of agents in society should be the main goal when developing information and society, and even though it is understandable that programmers and companies want be paid for developing it, the payment should not come at the cost of the general freedom in society (Stallman 2002, pp. 36-41 + 50).

From the Foucaultian perspective, the attempt to avoid structures of hiding is not realistic. Structures of hiding may certainly have unhappy consequences, but the case with graphical userinterfaces shows that they also facilitate new kinds of productive relations. Rather than trying to solve the problem by denying structures of hiding, we should thus turn our attention towards reflections upon alternative structures that may support the benefits, but avoid the drawbacks.

Alternatives to the commercial approach will therefore also be shaped by the parameter of concealment. Rather than seeking to dissolve the commercial culture of hiding, one might try to see

23 The complicated discussion about the fruitfulness of patents is related to these questions. See for example Fine 2001; Hall 2003; Stallman 2004; Stallman 2005; Lessig 2006.

whether the actual structures of hiding could be reconfigured in ways that could satisfy both sides of the conflict. I suggest that the open source movement might be seen as such a suggestion.

The open source movement is a movement that creates software that is made available for anybody to use and modify, because the source code is made freely available. The idea behind this movement is to find a way around the barrier that separates experts (programmers) and end-users. By making the source code available more people will be able to contribute in the development of the software.

Most people are certainly not able to read the source code. The point is, however, that insofar as the sources are openly accessible the separation between end-users and coding experts will not be as clear-cut: Some users will actually be able to read the code – even though they cannot code themselves; other end-users will be able to help in testing, commenting and suggesting new features. Due to the open source licenses (that prohibit *exclusive* appropriation of the software) end-users who are interested in the functionality of the software have both the narrow interest of making better products for themselves and the community interest of contributing to the progress of the computing project.

The open source movement was initiated as an attempt to fuse the interests of the hackers and the commercial entrepreneurs (Raymond 2001, pp 113ff). On the one hand, software is made free for unlimited copying, on the other hand commercial entrepreneurs save engineering expenses because they can draw on previously developed software and the inputs from users. Through a reconstruction of the interface between end-users and experts, the structures of hiding are also reconstructed, hereby potentially dissolving the conflict between corporate and hacker ethics

As demonstrated in the previous sections, the relationship between hacker- and commercial cultures is decisively shaped by the role played by the hidden: on the one hand the traditional business-approach claims the necessity of keeping information hidden in order to gain a return on the investment in their development; on the other hand hackers claim that the information is by its nature a good that ought to be freely available, being in fact at the base of social liberty – it is our ability to access information that helps us innovate and create, and its concealment harms our creative nature. By creating software in open source environments, we demythologise the central all knowing software engineer, and also the enemy of the all knowing software engineer, the stealthy hacker.

As I have argued, the double mythologization stems from the fact that something is going on behind our backs. But if the code is publicly available, this anxiety loses its social embodiment. The motive for mythologization and demonization is thus no longer valid. We (or the experts in whom we trust[24]) can read the code, and see what is actually going on. The open source approach is important, because it diminishes the threat profile of the Other.

This is not to say that the open source movement creates a field of absolute transparency in our social relations. If all information was equally available to everybody, commercial entrepreneurs would find it difficult to generate revenues. Brands like Red Hat, JBoss, MySQL, eZ Publish, ZOPE and Trolltech (among others) have succeeded in developing business models in which they in various ways convince the public that even though they make their software freely available, it might still be beneficial to pay for various kinds of services.[25] The brands thus still carry certain special insights or skills that are valued (due to their close affiliation with the development of the code) – their product is, however, not connected to the hiding of the code. The aim of the turn towards open source software is not to preclude the commercial side of the above sketched

24 The open source approach does not *prevent* meritocratic hierarchies. The interests and agendas of experts would, however, be diversified by the shift towards open source production.

25 Some open source software vendors chose to give away the code for free (i.e. without any payment for the *license* as such), and then they gain revenue from selling *services,* such as training and support (the RedHat-model – Young 1999). In this case Redhat is able to generate revenue because even though we all may download their software, they have (as developers) still some special informational insigts, which make them qualified as supporters in cases of trouble with the software.

opposition. The aim is rather to reformat the basis of the opposition between information as commons and software as commodity by showing that one approach doesn't necessarily negate the other. Indeed, when looking at existing open source vendors, it is clear that the open source approach can be assimilated to profit seeking organizations.

VI. Positivist Surface analyses as a Way to Diversify Social Structures

It should now be clear that positivist surface analyses can indeed deal with social phenomena that are defined through their situation in structures of hiding; the positivist surface analyses may actually help us better understand existing social phenomena. By refusing to take the structures of hiding as our primary cause, we can understand them as secondary products of the surface phenomenon. On the surface, we trace the prevailing antagonisms that are mirrored in the structures of hiding. The surface analyses reveal the contingent sources of the prevailing structures (in this case: the graphical user interface, and the copyright motives), and it thus becomes possible to develop approaches that do not have to take sides in the struggle. It becomes possible to resolve the conflict either by showing both sides to be wrong, or (as in the open source movement) by taking the worries of both sides into account.

As I have argued elsewhere (xxxAnonymized reference 2005a – esp. pp. 183-4; Anonymized reference 2005bxxx) Foucault's positivism and rejection of *universal* normative institutions[26] should be understood as an attempt to diversify social forms of interaction. It equips us with a new mindset for reacting to and resisting our subjection by realising that power is never one-sided and total. Powerrelations and -structures are never ahistorically given. Or, in the words of Foucault:

> "Maybe our problem is now to discover that the self is nothing else than the historical correlation of the technology built in our history. Maybe the problem is to change those technologies. And in this case, one of the main political problems would be nowadays, in the strict sense of the word, the politics of ourselves." (Foucault 1993, pp. 222-3).

Foucault's point is thus that technologies of the self – and therefore also of the "other" – is a product of historical correlations that involve such things as changes in the episteme, regulations of governance, the infrastructure of technology and its unexpected results, and tactical narratives used to enlist allies or demonize enemies. The surface analyst analyses the immediately given social phenomena (such as the struggle between agents from the business sectors and hacker movements) without trying to interpret them as signs of something else. By analysing them in their own terms it becomes possible to reflect the worries and anxieties out of which they emerged. Just as hackers have been demonized through attributing to them a set of dangerous and thievish aspirations, hackers often tend to attribute the commercial agents such evil motives as greed, selfishness, etc. Needless to say, such attributions of "hidden" intentionality does not inspire fruitful dialogical exchanges.

This is where Foucaultian surface analysis becomes relevant. By taking the phenomena as monuments that do not require some transformation into an interpretive text in which the "truth" of the monument's message is revealed, the analyst brackets the search for hidden intentionalities and lets the appearances and events speak for themselves. This does not mean that the analyst reaches some kind of "neutral" starting point; to the contrary: the analyst seeks to acknowledge the monuments in their self-understanding (accepts the self-interpretation of the investigated phenomena) and uses this data to give a comprehensible account of it – without trying to overcome or ignore the inherent self-contradictions, self-delusions and tactical and strategic shapings. These seemingly problematic or incoherent elements are seen not as problems to be solved, but as solutions that are problematic. The work of the happy positivist can then serve as a tool for further contemplations about the sustainability of prevailing structures.

26 Which is not the same as rejection of normative institutions per se.

By bracketing the analyses of hidden intentional structures, the happy positivist is thus able to facilitate deeper understandings of the prevailing structures of hiding.
xxxx lav ny litteraturliste xxxxx

References

Abbate, J., 2000. Inventing the Internet, Cambridge, Mass., USA: The MIT Press.

Bedau, H.A., 2002. Civil disobedience in focus, London, New York: Routledge.

Douglas, M., 1992. Risk and Blame: Essays in Cultural Theory, New York: Routledge.

Drew, C. & Shane, S., 2013. Résumé Shows Snowden Honed Hacking Skills. The New York Times.

Feenberg, A., 1992. Subversive rationalization: Technology, Power and Democracy. Inquiry: An Interdisciplinary Journal of Philosophy, 35(3-4), pp.301–322.

Feenberg, A., 2002. Transforming technology : a critical theory revisited, New York, N.Y.: Oxford University Press.

Fine, G.S., 2001. To Issue or not to Issue: Analysis of the Business Method Patent Controversy on the Internet. Boston College Law Review, 42(5), pp.1195–1214.

Flynn, B.C., 1987. Foucault and the Body Politic. Man and World, 20, pp.65–84.

Foucault, M., 1977. Cours du 7 et 14 janvier 1976. In D. Defert, F. Ewald, & J. Lagrange, eds. Dits et écrits 1954-1988. Paris: Galimard, pp. 160–189.

Foucault, M., 1969a. L'archéologie du savoir, Paris: Gallimard.

Foucault, M., 1976. La volonté de savoir. Histoire de la sexualité I, Paris: Gallimard.

Foucault, M., 1971. L'ordre du discours : Leçon inaugurale au collège de France prononcée le 2 décembre 1970., Paris: Gallimard.

Foucault, M., Naissance de la biopolitique : cours au Collège de France (1978-1979) F. Ewald, A. Fontana, & M. Senellart, eds., Paris : Gallimard : Seuil, c2004.

Foucault, M., 1963. Naissance de la clinique: une archéologie du regard médical, Paris: Presses Universitaires de France.

Foucault, M., 1990. Qu'est-ce que la critique? (Critique et Aufklarung). Bulletin de la Societe Francaise de Philosophie, 84(2), pp.35–63.

Foucault, M., 1984. Qu'est-ce que les Lumières? In D. Defert, F. Ewald, & J. Lagrange, eds. Dits et écrits 1954-1988. Paris: Galimard, pp. 562–578.

Foucault, M., 1969b. Qu'est-ce qu'un auteur? In D. Defert, F. Ewald, & J. Lagrange, eds. Dits et écrits 1954-1988. Paris: Galimard, pp. 789–821.

Foucault, M., 1998. The history of sexuality, London: Penguin Books.

Galloway, A.R., 2004. Protocol : how control exists after decentralization, Cambridge, Mass.: MIT Press.

Habermas, J., 1985. Der philosophische Diskurs der Moderne: zwölf Vorlesungen, Frankfurt am Main: Suhrkamp.

Hall, B.H., 2003. Business Method Patents, Innovation, and Policy,

Himanen, P., 2001. The hacker ethic and the spirit of the information age, New York: Random House.

Hoglund, G. & Butler, J., 2005. Rootkits : subverting the Windows kernel, Upper Saddle River, NJ: Addison-Wesley.

Ihde, D., 1998. Expanding hermeneutics: visualism in science, Evanston, Ill: Northwestern University Press.

Kelly, M., 1994. Critique and power : recasting the Foucault/Habermas Debate, Cambridge, Mass.: MIT Press.

Klang, M., 2004. Civil disobedience online. Journal of Information, Communication and Ethics in Society, 2(2), pp.75–83.

Leigh, D., 2011. Wikileaks: inside Julian Assange's war on secrecy 1st ed., New York: Public

Affairs.
Lessig, L., 2006. Code : version 2.0, New York, N.Y.: Basic Books.
Perens, B., 1999. The Open Source Definition. In C. DiBona, S. Ockman, & M. Stone, eds. Open Sources: Voices from the Open Source Revolution. Beijing: O'Reilly Media, Inc., pp. 171–188.
Raymond, E.S., 1999. A Brief History of Hackerdom. In C. DiBona, S. Ockman, & M. Stone, eds. Open Sources: Voices from the Open Source Revolution. Beijing: O'Reilly Media, Inc., pp. 19–29.
Raymond, E.S., 2001. The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary, Revised Edition 2. edition., Sebastopol: O'Reilly Media, Inc.
Raymond, E.S., 1996. The New hacker's dictionary, Cambridge, Mass.: MIT Press.
Ross, A., 1991. Hacking Away at the Counterculture. In C. Penley & A. Ross, eds. Technoculture. Minnesota: University of Minnesota Press, pp. 107–134.
Saco, D., 2002. Cybering democracy : public space and the Internet, Minneapolis: University of Minnesota Press.
Schwartz, M., 2008. The Trolls Among Us,
Stallman, R., 2005. Patent absurdity,
Stallman, R., 2004. The Dangers of Software Patents,
Stallman, R., 1991. Why Software Should Be Free. Available at: http://www.gnu.org/philosophy/shouldbefree.html [Accessed December 7, 2011].
Stallman, R.M., 2002. Free Software, Free Society: Selected Essays of Richard M. Stallman J. Gay, ed., Boston, Mass.: GNU Press.
Taylor, P.A., 1999. Hackers: crime in the digital sublime, London: Routledge.
Thomas, D., 2002. Hacker culture, Minneapolis: University of Minnesota Press.
Wark, M., 2004. A hacker manifesto, Cambridge, Mass.: Harvard University Press.
Young, R., 1999. Giving It Away. How Red Hat Software Stumbled Across a New Economic Model and Helped Improve an Industry. In C. DiBona, S. Ockman, & M. Stone, eds. Open Sources. Voices from the Revolution. Sebastopol: O'Reilly Media, Inc., pp. 113–125.
Zittrain, J., 2008. The future of the Internet : And how to stop it, New Haven Conn.: Yale University Press.
Zittrain, J.L., 2006. The Generative Internet. Harvard Law Review, 119, pp.1974–2040.
xxxxxxxxxxxxxx Anonymized reference xxxxxxxxxxxxx
xxxxxxxxxxxxxx Anonymized reference xxxxxxxxxxxxx