The Three Pillars of Functional Autonomy of Hackers

Johan Söderberg · Maxigas

Abstract We propose a conceptual framework for analysing the relationship between social emancipation and alternative technology development. Key is the “functional autonomy” of the collective of users and developers of the technology vis-a-vis state and capital. We draw on previous empirical work about three hacker projects to substantiate the claim that the functional autonomy of hackers rests on three “pillars of autonomy”: technical skill, shared values, and collective memory. These three pillars sustain the autonomy of a community of hackers so that it may successfully resist recuperation attempts by capital. We make this claim in contradistinction to looser constellations of users, citizen scientists, DIY hobbyists, etc., where the functional autonomy tends to be much weaker. Hence, in the latter case, we should expect the actors to be recuperated in short time. The emancipatory promises that they make in regard to their practices, and are often mirrored in the academic literature about user innovation, citizen science, etc., will then turn sour. From this observation, we develop a second-order reflection on the role of the scholar studying purportedly emancipatory technology projects. As against the popular “follow-the-actors” approach, we defend the continued need for scholarly critique. We do so with the caveat that critique must in part be conducted as self-critique.

Keywords Capitalism · Critique · Recuperation · Hacking · Autonomy · 3D printing

Introduction

In the following pages, we reflect on the pitfalls of attributing emancipatory potentialities to a broad class of DIY practices and bottom-up technology initiatives. We develop such a reflection by drawing on more than 15 years of experience studying hackers. Embedded in the word “hacking,” and key to the hacker identity, is the promise that freedom can be realised through the repurposing of tools and by routing around constraints and regulations. Variations on this idea recur across a wide range of bottom-up DIY practices and interventions in technology use. However, the industry has already anticipated the disruption stemming from unauthorised and non-prescribed uses of its products. Attempts by users to route around technical and legal constraints are routinely harnessed by firms and fed back into the development process.

The hacker subculture offers many examples of such a recuperative dynamic. Numerous scholars have shown that Silicon Valley owes its existence to a computer underground that emerged from the 1960s West
Coast counterculture, and from which the computer industry derived many of its ideas and innovations [1–3]. Likewise, the so-called “sharing economy” originates in experiments with commons-based, peer-to-peer production initiatives [4], and the dream of a personal, small-is-beautiful computer has grown into an ever-more fine-grained surveillance system [5]. Indeed, the list of such examples can become so long that it compels us to reflect upon the systematic importance of recuperation in the current iteration of “informational” capitalism [6–8].

We offer a theoretical contribution to this area by developing a conceptual framework for studying processes of recuperation. Recuperation operates by replacing the goals and values that were initially professed by a community of hackers (users, citizen scientists, etc.) with new ones, which are better aligned with the needs of capital accumulation and state control. As a direct consequence, the collective endeavour of the hackers is pulled in the direction of market demand and the constraints of mass production. Recuperation processes are often resisted by hackers, although typically in the form of infighting between different factions within the community. While one faction asserts its attachment to the original values and design goals of the project, another faction strives to accommodate that design to the external pressures, and considers this to be a criterion for the project’s (technical and commercial) success. Later in this article, we will identify “three pillars of autonomy,” as crucial in determining the outcome of such struggles. In order for a hacker community to maintain its functional autonomy vis-à-vis the computer industry upon which it nevertheless depends for its material subsistence, hackers need technical skills, shared values, and a collective memory.

Our key argument is that the conditions under which hackers sometimes resist recuperation attempts are typically not present in the many other settings that are being studied as cases of bottom-up DIY tinkering. The dizzying variety of names given to such actors in the academic literature—“users,” “hobbyists,” “makers,” etc.—bears witness to the absence of a shared frame of reference within which skills, values, and memory can be passed on from one cycle of struggle to the next. Since the three pillars of autonomy tend to be absent in the latter settings, we should expect the actors to be recuperated in a short time. Confirmation of this expectation is readily found in the vast backlog of interventions and practices that have had their original, emancipatory promises betrayed. Even so, the notion of recuperation remains under-theorised in the scholarly literature about unruly users and bottom-up technology development.

This brings us to the second theoretical contribution of the article: we will develop a second-order reflection on how the emancipatory claims surrounding bottom-up DIY practices are mirrored in the academic literature. The exact reproduction of the practitioners’ (limited) self-understanding has been codified in the follow-the-actors dictum of Science and Technology Studies (STS). With this methodological stricture, born out of a generalised mistrust of overarching, theoretical concepts, the STS scholar abdicates responsibility for guiding practice with theory. This outlook, together with the case-study approach, resonates with how scholarly inquiry is organised and financed under present-day “academic capitalism.” Reflection about technology is compartmentalised into one-off micro-studies, tailored to fit the average, 3-year timespan of an external research grant, and with an in-built, funding-driven selection bias of cases towards up-and-coming, emerging technologies (and markets). Long before the moment of betrayal arrives in the project, the scholarly community has lost interest, and moved on to do research on the next big thing. Our claim is that in this way the promise that freedom will come from a grassroots DIY intervention can be perpetually renewed in the academic literature, in spite of the many historical lessons suggesting otherwise.

In making this claim, we aspire to make a theoretical contribution to the STS field at large, with a bearing on empirical investigations that goes beyond the specific study of hackers to include, for instance, user studies, studies of citizen science, and design research.

**Theory on Recuperation**

We borrow the concept of “recuperation” from the French sociologists Luc Boltanski and Eve Chiapello, whose magisterial work *The New Spirit of Capitalism* provides the theoretical backbone for our inquiry. They have compellingly argued that capitalism advances by incorporating its critiques. Critique,
once recuperated, is made into a source of innovation and legitimacy for capitalism [9]. This basic idea can be productively applied to the kind of critique that is expressed in social-movement contestations of product design, standardisation, and alternative technology development. The hacker subculture makes up a subcategory of this phenomenon. The collaborative production of free software programs and open hardware devices showcases a kind of critique—the critique of intellectual property—that is embedded in development methodologies and technological design. Likewise, free software development and open hardware tinkering is emblematic of broader societal trends in that this “critique” is systematically recuperated and turned into a motor of corporate development. Computer firms are tailoring their business strategies around the opportunity to procure innovations from individual users and user communities. Methodologies of “open innovation” [10, 11], or even “outlaw innovation” [12], render the user-centric innovation model systematic. The more the industry grows dependent on open innovation processes, the more thoroughly it must manage the value-producing users and user communities. Methodologies of “open innovation” [10, 11], or even “outlaw innovation” [12], render the user-centric innovation model systematic. The more the industry grows dependent on open innovation processes, the more thoroughly it must manage the value-producing users and user communities. Step by step, user communities are being subsumed under capital’s valorisation process, just as waged labour was in earlier times.

For analytical purposes, we distinguish between three different temporalities or time horizons within which recuperation unfolds, and within which it is resisted. The shortest time horizon encompasses the lifecycle of an individual hacker project and its associated community of developers. The second time horizon spans a landscape of hacker projects and/or communities evolving in tandem with an associated branch of the industry. The third time horizon of recuperation processes, in keeping with Boltanski and Chiapello’s work, maps onto a periodisation of capitalism as the “spirit of the time.” This is the broader context for the struggles that play out across the two previous timescales. Needless to say, where the line should be drawn between one or the other can only be decided on a case-by-case basis. This heuristic serves to scale up the analysis from a single case study of a local contestation to the global situation that frames and gives meaning to the situated locality.

The first time horizon spans the lifecycle of an individual development project and the associated community of hackers and/or developers. This underscores a point made initially that an adequate study of a technical innovation must consider the whole biography of the development project, from start to finish, during the course of which project goals, individual motives, and the design of the technology itself are transformed [13]. The methodological principle of studying the full trajectory of social conflicts resonates with how the waxing and waning of popular mobilisations are studied in Social Movement Studies. A suggestive synthesis between Science and Technology Studies and Social Movement Studies has been devised by David Hess. He has come up with the concept “technology- and product-oriented movements” (TPMs) to describe civil-society mobilisations centred on grievances and making claims in relation to the creation and diffusion of alternative technologies. Hess highlights three phases in the co-evolution of a TPM and its conjoined product innovation. To start with, the goals of the TPM are co-articulated with those entrepreneurs and companies who are willing to create a market for the new product. Then, with the absorption of the innovation, the design and meaning of the technology are transformed under pressure from market and mass-production constraints. Finally, this transformation gives rise to “object conflicts” between the TPM and its for-profit allies, and between different fractions of the TPM. Conflicts revolve around the proper design and/or adoption of a transformed technology, as measured against the original grievances and values acclaimed by (a fraction of) the movement.

The second time horizon covers a longer timeframe, following the co-evolution of hacker culture taken as a whole in conjunction with the computer industry and other external actors (such as the state, military, etc.). A simple case study following the lifecycle of a single development project or community relates their internal dynamics to their immediate context. In contrast, a study following some development within hacker culture at large must relate this phenomenon to definitive historical moments. For instance, Steven Levy’s classic work on hackers identifies several phases in the history of hacking, spanning the period from the 1960s MIT hardware hackers to the emergence of free software in the
Thus, his iconic book covers scenes and communities with very different ethoses, cultural references, and political goals [14]. Most scholars have pinpointed the 1970s West Coast context as a key historical and geographical juncture for making sense of the early relationship between hackers and the computer industry [15]. For instance, by following the life trajectory of Stewart Brand and his associates, Fred Turner’s book *From Counterculture to Cyberculture* shows how the former culture branched off into the latter, giving impetus to the nascent computer industry in the process [1]. Indeed, the idea of building a small computer to foster free communication practices and new modes of community formation came out of the communalist longings of the Sixties counterculture [14, 16]. Cultural and organisational elements of the counterculture, which already resonated with tropes from computer science and cybernetics, were soon integrated into the computer industry, and came to fundamentally rewrite how business is conducted in this sector. This dispels the notion of a pristine hacker subculture that has been corrupted by the industry at some later point. There is compelling evidence that the two have evolved in tandem from day one. The more dependent the industry becomes on open innovation processes, the more effort is being put into managing such external sources of value, but hackers also come to occupy a more strategic position in the production process.

The third time horizon situates hacker practices within the evolving whole of capitalism. We borrow this idea from Luc Boltanski and Eve Chiapello’s interpretative framework, according to which capitalism is constantly driven to evolve in response to critique. The incorporation and adaptation of critique give capitalism the means to overcome its own, recurring impasses and to re-found itself on new, legitimate grounds. The spirit of the current, post-Fordist incarnation of capitalism came about in response to the upheavals of 1968. Numerous other authors have suggested a similar storyline, in which the ideals of the student movement, individual freedom, self-expression, etc., have been appropriated and integrated as the motor of consumerist societies [17]. Whereas Boltanski and Chiapello’s argument dwells on the evolution of organisational forms, these authors have had little to say about the role of technology in the processes they describe. The link to hackers has been proposed by Anne Barron, who suggests that the values embodied in free software development qualify as “a particularly pure form” of the new spirit of capitalism. The other side of the coin of the artistic and social critique of proprietary software and other forms of “closed innovation” systems is an emotional investment in “open” forms of capital accumulation. Thus, the oppositional stance is turned into an “ethical foundation for contemporary capitalism” [18, 19]. This generally held argument can be substantiated with examples of technical products and infrastructures originating in the antagonistic, yet symbiotic, relationship between hackers and the computer industry. A case in point is the development of mesh computer networks, distributed and anonymous retrieval systems, and video conferencing, all of which are derived from the outlawed practice of file sharing [20, 21]. Taken together, hackers have made major contributions to the material infrastructure of what Boltanski and Chiapello call “connexionist” capitalism.

The point of adopting an overarching, theoretical perspective like the one proposed here is that it draws attention to the historically developed framing conditions of the local case under study. It is indispensable to adopt a global perspective on local struggles in order for the emancipatory potential of the latter to be adequately assessed. There is no shortage of examples where struggles that appear to be emancipatory, when taken in their immediate context, turn out to have oppressive and exploitative consequences when exported to other locations and contexts. A case in point is the demand for flexible working conditions. Generally embraced by computer engineers as an improvement over nine-to-five office work, flexible working conditions translate into intensified exploitation when introduced into the lower tier of the “gig” economy. We contend that no DIY practice identified as emancipatory in the technology sector will remain so for very long, unless there is an analytical effort to expand the socio-political outlook of practitioners beyond their immediately given situation.

Functional Autonomy of Hacker Communities

Considered broadly, the proposal that alternative, bottom-up technologies for social change can emerge
from a setting that is concurrently said to be under the hegemonic control of state and capital is seemingly self-contradictory. By and large, hacker culture, norms, and practices, together with the underlying technological infrastructure, are all saturated through and through with hegemonic relations to the state and capital. Still, we cannot contend from this that resistance is futile. Here, we take a cue from factory workers’ resistance to the domination of capital at the point of production, as analysed in the tradition of labour process theory. The starting point of labour process theory is Karl Marx’s fragment on the “Results of the Direct Production Process,” where he distinguished between the formal and the real subsumption of labour under capital. The one thing that checks the total domination of capital over the production process, i.e., the real subsumption of labour under capital, is the de facto, if not de jure, functional autonomy that workers exercise through direct control of their tools, as well as through the knowledge they have about how to deploy those tools productively [22]. Factory workers are considered to enjoy some functional autonomy vis-à-vis their management, despite being enveloped by the contractual wage relation [23]—and the same reasoning applies to hackers. The historical parallel with struggles over tools and skills in the workplace is justified, since hackers, having been put to work by an open innovation model, are subsequently formally subsumed under capital’s valorisation process.

Functional autonomy is our answer to how critical engineering practices may arise from within hacker culture, in spite of this setting being predicated on a symbiotic relationship with the computer industry. A relatively high degree of autonomy means that hackers enjoy discretion in defining their common goals and choosing the proper means for solving tasks, i.e., functional control over the labour process. This claim is congruent with an established usage of the word “autonomy” in political philosophy, harking back to Rousseau and Kant [24]. A collective can be said to be “autonomous” if it has not submitted to any external authority other than the laws it has given to itself. The capacity of such a collective to set goals for its own shared undertaking and to direct its future-oriented process of becoming follows from this autonomy. Feminist scholars have objected to the bias towards a decontextualised, free-roaming rational mind that underlies the notion of “autonomy” in the political philosophy tradition [25]. We hope to sidestep this line of critique by drawing on the concept as it has been developed in the specific context of workplace studies. It goes without saying that the limited autonomy that workers may secure for themselves within the contractual employment relation will always be shaped by an economic and material sub-stratum. Applied to our context of inquiry, hackers are conditioned by the technical infrastructure upon which they draw, as well as the labour demand for their services (i.e., the necessity to work for subsistence and the position of the programmer within the social division of labour).

Recuperation encroaches upon the functional autonomy of hackers. Thus, the balance of forces is tilted so that their capacity to collectively determine the conditions under which they enter into a symbiotic relationship with the industry is weakened. This relationship is constantly being negotiated, without any prospect of it ever being settled in a final victory for either side. Companies strive to secure this external source of value production in order to minimise risks and optimise output. This harks back to Marx’s notes on the historical logic of capitalism. According to Marx, capital first engages external, non-capitalist forms of production, such as subsistence agriculture and artisan industries. Then, it gradually transforms the interior of the production process according to its own needs. The transformation of the production process into a properly capitalist one is called the passage from the formal to the real subsumption of labour under capital. Translated into our conceptual framework, hackers resist recuperation when they push back against capital’s drive to subsume their creative and cooperative activities under its valorisation process. The paradox is that capital depends on hackers resisting its relentless drive. If the functional autonomy of hackers were neutralised, so that they could not self-organise task allocation and choose their own methodologies for problem solving, they would cease to furnish capital with good ideas and development work. It is precisely the failings of the firm to organise production in-house in the most productive way that has sparked the outsourcing of innovation processes to commons-based, peer-production communities in the first place [26].

A recurring point of contestation in the symbiotic, yet antagonistic relationship between hackers
and industry is the core value of hacker culture that information should be freely disclosed. As advocates of free software licences never fail to point out, this dictum is compatible with selling software and making a profit from the transaction. A case in point, it is argued, is Red Hat, and other companies that provide commercial support services for free software. We agree that a principal commitment to the free disclosure of information does not rule out profit-making. Nevertheless, it tends to be at odds with the goal of profit maximisation. All else being equal, the highest profit can be reaped by a firm if it is free to choose when to disclose knowledge and when to monopolise it. This goes a long way towards explaining the constant feud over what kind of licence should be considered “free” (or “open”), and heated debates on whether or not the terms of the licence have been breached in any particular instance, etc. Battles over licence agreements are the most visible and obvious manifestation of social conflicts around information disclosure, but recuperation works on many different levels at once. Project leadership is challenged, competing associations are created, new names are invented to replace old ones, etc. Often, it is only in hindsight that it becomes evident how a hacker community has been recuperated. Conversely, in order to diagnose recuperation in time for strategic interventions, it is necessary to study recuperation processes simultaneously at different scales and across different time horizons—as sketched out in the paragraphs above.

A more in-depth investigation of social conflicts surrounding innovation and the recuperation of hackers’ functional autonomy requires analytical concepts such as the three pillars introduced below.

**Three Pillars of Functional Autonomy**

In what follows, we develop a reflection on the necessary conditions for hackers to successfully resist recuperation attempts, based on a summary of three case studies. The empirical material has been collected and presented separately in different contexts before. We draw on them here in order to illustrate what we elect to call the “three pillars of functional autonomy.”

The three pillars represent some indispensable prerequisites for a critical discourse on technology that can inform the resistance to recuperation. In other words, they refer to the necessary—but not necessarily sufficient—conditions for developing functional autonomy in the face of recuperative tendencies. These pillars are the following. First, expertise: hackers’ ability to understand and engage with a technology. Second, shared values and cultural references. Third, a historical horizon encompassing familiarity with older generations of the same technology. Having secured all three pillars, practitioners may acquire an independent vantage point that diverges from the hegemonic common sense permeating the industry, and the engineering profession at large. Upon them depend their ability to collectively pursue alternative trajectories of technological development and, hence, to make good on the promise that their technology is an emancipatory one.

The technical expertise of hackers is key. They need to preserve open, transparent software and hardware architectures, while at the same time passing on and continuously updating the required skills from one generation of hackers to the next. Only if those conditions are fulfilled can hackers bend systems, protocols, and standards to their will. This contributes to the functional autonomy of hackers in several ways. Understanding how something works is a prerequisite for judging its significance and ramifications. The technical expertise of hackers has allowed them to intervene in politics in more consequential ways than is the case with the “prefigurative politics” of many social movements. The paths taken by hackers in terms of technology choice have not only demonstrated the possibility of an alternative, but have on many occasions forced the computer industry to follow suit. To illustrate that technical expertise is a necessary, but insufficient condition for having autonomy, it is enough to consider career engineers. Typically, such a career spans three stages. They begin as hobbyists in their teens, attend university to study informatics (physics, etc.), and then end up with a job in a tech company or start their own firm. Tertiary education and professional training give them enough expertise to be able to understand and produce technology, which is the first pillar. However, since professional engineers are only familiar with the hegemonic interpretation of what technology is, they are unlikely to develop a critical stance towards the dominant infrastructure.
This highlights the importance of hackers sharing values and cultural references. It goes without saying that the phenomenon called “hacking” is heterogeneous. The cultural expressions of hackers have been transformed many times over, as the practice has spread to new geographical regions and engaged with new technological developments. We concur with Christopher Kelty that a commonality holds this variety together, which helps practitioners to recognise themselves as “hackers.” Ultimately, this common identity is verified in the capacity of hackers to come together from time to time and act in concert [27]. Independent technical expertise and cultural values may thrive, and be passed on under the hacker moniker. Their values are ethical and aesthetic at once, in the same gesture. For instance, free software code is judged to be both morally superior and more beautiful than proprietary “spaghetti” code. Shared values are cultivated in regular mass interactions online, such as mailing lists and chat rooms. However, these would not suffice on their own. Hacker culture requires physical meetings and conventions in order to reproduce itself, aptly described by Gabriella Coleman as “a ritual condensation and celebration of a lifeworld” [28]. Likewise, hackerspaces, together with other physical locations, such as shared machine shops, provide a material and symbolic milieu that reinforces identity formation. The iconic soldering iron, and fridges stocked with Club Mate, is two relevant examples [29, 30]. The critical importance of subcultural identity for sustaining the functional autonomy of hackers is underlined by the observation that this is chiefly what distinguishes them from the great variety of other kinds of actors who engage with technology under labels such as “citizen science” or “Do-It-Yourself.”

Below, we illustrate our general argument with three cases that exemplify the three pillars of autonomy. The first case, Internet Relay Chat, exemplifies the importance of technical expertise for successfully resisting recuperation attempts. The second case, open-source 3D printers, foregrounds the internal strife within the community over its shared values and goals as a central field of struggle against recuperation. The third case illustrates a breakdown in the transmission of shared memory during a displacement of hackers’ physical meeting spaces from hacklabs to hackerspaces.

Case Study 1: Internet Relay Chat (Expertise)

Internet Relay Chat (IRC) is a basic but flexible protocol for real-time written conversations. The social history of IRC is noteworthy, because its development, deployment, and maintenance have remained in the hands of the hacker community for an exceptionally long time [34]. It was first implemented in 1988, 1 year before the World Wide Web. IRC reached the height of its popularity as a general-purpose social media during the first Gulf War and the siege of Sarajevo (1992–1996). At this time, it performed various social functions. Many of these were later fulfilled by specialised programs and platforms, such as sharing news and reporting from the front lines, dating, following friends or file sharing. As the Internet grew and market consolidation set it, IRC faded from public view.

It remains, however, a key tool for contemporary peer-production communities [35]. Free software developers [36], hackerspace members [30], Wikipedia editors [37], and anonymous hacktivists [38] all rely on IRC for everyday backstage communication. Notably, the first group has always been on IRC, but the
latter three adopted it after the apparent demise of the medium. The continued use of IRC casts doubt on the ideology of innovation, which prescribes that technical progress goes hand in hand with social progress; or, failing that, technical progress is a historical driver that no humans—not even engineers—are in a position to refuse. Currently popular social networking platforms, such as Facebook and Twitter, offer broadly comparable features to IRC. Therefore, they appear to be a more obvious choice, yet they are being rejected by hackers. While IRC use may seem retrograde, it is actually the articulation of a powerful critique of mainstream social media monopolies.

The uneven distribution of media literacy explains why peer-production communities can continue to rely on IRC. However, in order to appreciate the significance of technical expertise, it is necessary to understand a few key design principles of the protocol itself. Like many other chat solutions, IRC is based on a client-server model, where servers syndicate messages to client programs. At the same time, IRC is unique in that it was designed as a streaming protocol replicating the functionality of Citizen Band radio. The terminology of “relay” instead of “server” and “channels” instead of “chat rooms” come from radio, rather than computing. The consequence is that servers make no attempt to store the messages that pass through them. Thus, clients only see the transmitted messages while they are connected to the server—if the client disconnects, new messages are lost. The user experience of being part of an asynchronous conversation within a community of peers is therefore dependent on whether or not the user can run a client software that is always connected to the server. No stable internet connection—no community involvement.

This was not a problem in the golden age of home computing characterised by desktop computers and domestic flat-rate ISDN uplinks, because users could just keep their computer running and their IRC client listening on the relevant IRC channels. It was precisely during this time, in the 1990s, that IRC was popular with all Internet users, supporting a variety of use cases. Since then, changes in the media landscape have ushered in an era of ubiquitous computing. People use the Internet from mobile devices roaming between wireless networks and mobile Internet connections. Moreover, since many users own at least two personal computers—a laptop and a phone—applications need to work on multiple devices simultaneously. Historically shifting assumptions about computers and networks have also shaped the context and character of IRC use.

Therefore, IRC has become increasingly inconvenient to use for most contemporary Internet users. There is an almost ritualistic manifestation of this phenomenon, which is well known in peer-production communities. Novice users log in to a channel and ask a question, but log out before the answer arrives, leaving both the supportive community and the users themselves frustrated. Meanwhile, members of peer-production communities stay permanently connected because their IRC clients run on their personal servers, instead of laptops or smartphones. They log in to their own servers in order to participate in the chat, and have a full backlog of channel activity available. It is relatively easy to develop and maintain such an IRC setup, but it requires basic familiarity with the command line interface and access to terminal servers. Since peer-production communities often work with such tools anyway, this is a small barrier to adoption for them, but a major hurdle for other users. The technical limitation of the protocol needs to be supplemented by the technical expertise of its users in order to deliver the community experience that made IRC legendary.

Technical expertise became a barrier to access in the context of the contemporary media landscape. On the one hand, it prevents the mainstream adoption of the protocol. On the other hand, the high barrier to access preserved IRC as a chat device that is developed, operated, and maintained by its users. Apart from making IRC hard to use, the streaming protocol design also thwarts the recuperation of the infrastructure into capital accumulation strategies. As mentioned before, the consequence of the streaming protocol design is that the IRC server forgets the conversations that are transmitted through it—it does not store the history of chat rooms, so called “backlogs.” This is not only a problem for mainstream users, because the centralised data collection of user activities is the very basis of surveillance capitalism. Commentators often construe such data as the fuel of the post-Fordist period of capitalism, arguing that “information is the new oil”; e.g., the surveillance capitalist business model depends on the valorisation of user-generated content. Since IRC stores no such content,
its technical design makes data mining, analysis, and valorisation impractical.

Indeed, major corporations such as Microsoft tried to extend surveillance capitalism to IRC, but these experiments invariably failed, leading to the development of alternative, proprietary chat devices such as MSN (colloquially known as Messenger). Currently, there is another, ongoing attempt at the recuperation of IRC, in the form of the centralised, proprietary platform Slack. However, for the moment, the technical expertise of peer-production communities, coupled with the limitations of the protocol design, has allowed them to continue to rely on the IRC infrastructure as they have done for decades, sheltered from both mainstream adoption and recuperation by capital.

Case Study 2: Personal Manufacturing (Values)

During the launch of a project to develop an open-source 3D printer in 2005, the goals set by the project leader could rightly be described as “civilisational.” More important than the technical innovation itself was the conceptual innovation of making an affordable, user-friendly, and ubiquitous machine tool capable of making a copy of itself. In engineering terms, this goal boiled down to designing the 3D printer so that it could be assembled from parts that had been printed on the same kind of machine. This gave the project its name, “RepRap,” an abbreviation of “self-
REPlicating RAPid prototype.” Drawing upon the notion of self-replication as the minimum condition of life, the engineers involved in the project spun a web of tropes, naming practices, and narratives borrowed from evolutionary biology. The evolutionary force of the self-replicating 3D printer was expected to develop and spread at such a rate that centralised, capital-intensive manufacturing would become as obsolete as the dinosaurs. In place of old-time factories, there would flourish a network of decentralised and agile user-manufacturers. At the beginning, rhetoric about taking back the means of production was not uncommon. A manifesto published at the same time as the development project announced the whole endeavour as “Darwinian Marxism” [39].

As hyperbolic as this might sound in hindsight, many of the engineers in the core development team subscribed to this idea in private. They dedicated a substantial amount of their spare time, resources, and attention towards designing solutions that would increase the reproducibility of parts. In the dedicated RepRap forum, innumerable skirmishes were fought over what kind of design was compatible with the overall goal of reaching the point of self-reproduction. This goal of self-reproduction was felt by some members of the core development team of RepRap to be a matter of life and death for the community. Design choices that did not conform to this idea were passionately decried in the forum. Parallels can be drawn with the often-heated discussions on free software development mailing lists over alleged breaches of the terms and conditions set out in the licence agreement.

Over the course of just 2 or 3 years, the values and goals of the RepRap community came under severe pressure from mounting consumer demand. The desktop 3D printing market attracted massive interest from entrepreneurs, venture capitalists, and even the US congress. The US president at the time, Barack Obama, claimed that this machine would bring manufacturing jobs back to the shores of America. The fallout in the community could be detected in numerous ways. Hobbyists’ efforts to self-organise a mail-order distribution network for printed machine parts were soon overtaken by eBay as the central coordination mechanism for selling parts. Start-up firms began to produce brand-name derivatives of the original RepRap machine. Soon, allegations began to show up on the forum that some firms were not sharing their in-house design improvements, which was required by the licence. Again, as we know from free software projects, the naming and shaming of offenders is an integral part of how a hacker community governs its commons. Morale broke down, however, after the project leader and undisputed chieftain of the RepRap community—Adrian Bowyer—attested a hands-off policy towards licence violations. Almost incidentally, he added that he owned stocks in one of the accused companies, MakerBot Industries. He justified his refusal to enforce community norms with the same narrative about self-propelling, evolutionary technological change that underwrote the Darwinian Marxist rationale of the whole project. Licences mattered little, he claimed, since closed designs were evolutionary dead-ends that would necessarily be overrun by open development efforts.

Although complaints kept cropping up, no one else had the authority to bring entrepreneurially minded
developers into line. Therefore, the grudging commentators became isolated. In the absence of an enforced standard of conduct, most of the developers in the core team, even those who had come to the project with an idealistic mindset, decided to embark upon the entrepreneurial route. Most of them went out of business shortly afterwards, when those start-up firms that had backing from venture capitalists or incumbent companies began to consolidate their hold over the growing market segment. By then, however, not much remained of a developers’ community that could have acted as a counterweight to the industry players. Closely connected with this development was the transformation of design priorities, from making printable machine parts towards making a marketable product suitable for mass production. Equally telling is that the “Darwinian Marxist” manifesto was pushed from the front page to the back end of the RepRap website. Rather than being announced as a way of reclaiming the means of production, desktop 3D printing was celebrated for enabling “customised manufacturing.”

The moral of the story is that community values and norms need to be enforced for functional autonomy to be preserved in a hostile environment. The lofty political vision claimed for the self-reproducing 3D printer, drawing on old engineering tropes about technology evolving along a pre-determined path, initially served as a rallying cry, but was later used to legitimise a laissez-faire attitude towards private gain and opportunism. The failure in the governance of the commons led to intrusions and the disintegration of the community, which was subsequently subsumed under capital’s valorisation process [40].

Case Study 3: Hacklabs and Hackerspaces (Memory)

The transition from hacklabs to hackerspaces is a showcase of the fragility of the transmission of shared historical memory from one setting or generation to the next. Hacklabs are ideologically and spatially integrated into social movements. Typically located in occupied social centres, they are part and parcel of the anarchist, autonomous, squatter movements. Participants are concerned with political technologies, e.g., the practical application and transformation of technologies to serve social movements. At the same time, they also take part in the everyday experience of struggles, from direct action at demonstrations to endless debates at meetings. As a consequence of their social position, hacklabs are explicitly political and subversive, practising a critique of private property as an anti-capitalist gesture [41]. Historically, the heyday of hacklabs was the 2000s. The first hacklabs, such as Freaknet in Catania—founded in 1995—existed earlier, but it took years before a wider movement emerged. Geographically, they are most numerous in Southern Europe. The surface of emergence for hacklabs was the hackmeetings in Italy and Spain around the turn of the millennium.

Hackerspaces are non-partisan rented club houses set up for the cultivation of technological creativity [42]. Typically located in rented post-industrial spaces, they still house a regular proportion of self-proclaimed activists and pursue their own strand of civil society activities. Participants are concerned with technological politics, e.g., representing the interests of their own social group of independent researchers and outsider engineers in controversies around net neutrality, software patents, or copyright extensions. As a consequence of their social position, hackerspaces are deliberately apolitical, presenting their critique of intellectual property in the guise of instrumental rationality [43]. Historically, the proliferation of hackerspaces can be observed in the 2000s, exploding in 2007. Proto-hackerspaces such as the c-base in Berlin—founded in 1995—existed earlier, but a movement successfully advocating for the replication of the model is a later development [29, 30, 44]. Geographically, the heartland of hackerspaces is in Germany, but the genre quickly spread to Central Europe and North America, acquiring a global presence by now. The surface of emergence for hackerspaces was the annual meetings of the Chaos Computer Club in Germany, and their counterparts in the Netherlands.

It is important to understand that the hacklab model that emerged around the turn of the millennium allowed for greater functional autonomy—defined as independence from hegemonic currents and the ability to produce one’s own culture, practices, and technology. However, such autonomy has been confined to the activist ghetto, given fewer opportunities for intervention and fewer resources for the development of alternatives than what is potentially available for hackerspaces. The hackerspace model seems to strike a balance between integration/interaction with larger social structures, and the maintenance of autonomy—
albeit at the cost of losing a consistent political perspective. A particularly telling tale about the transition from hacklabs to hackerspaces is the evolution of the scene in the Netherlands over the last few decades.

Whereas hacklabs—such as ASCII,1 PUSCII,2 and later SLUG3—had been accommodated in empty, squatted buildings or occupied social centres, more recently some hackerspaces have been renting below the market price from anti-squatting agencies. In particular, Nurdspace4 and Hack425 were housed in such venues. Anti-squatting agencies specialise in keeping a few tenants on below market-rate contracts in otherwise empty buildings in order to prevent the houses from being squatted. These anti-squatting agencies emerged as a market response to social struggles around housing. The squatter movement transformed the urban real-estate industry and the associated regulatory frameworks [45, 46]. Therefore, hacklabs and hackerspaces can be seen as antithetical from a political perspective, even though they are both shared machine workshops where technology enthusiasts meet. Nonetheless, the struggles around hacklabs and other autonomous spaces contributed in rich ways to the conditions for the emergence of the movement of hackerspaces, including personnel and imaginaries, as well as market conditions and policymaking.

The strategic importance of historical memory is revealed when one observes the discourse around hackerspaces. Hackerspaces are routinely perceived as the authentic, politicised alternative to other types of shared machine shops, such as makerspaces, FabLabs, media labs, and startup incubators. Participants and observers seem to agree on this point. By now, the very word “hacklab” is used as a synonym for hackerspaces (also called hackspaces in the UK). This perception has been institutionalised on Wikipedia, the Free Encyclopaedia. Following the demise of hacklabs and the rise of hackerspaces, the Wikipedia entries for the two have been merged with minimum commentary, retaining only the definition of hackerspaces [44 §5]. The historical horizon was cleaned up, so that hacklabs have been rapidly erased from hacker memory. Today, the non-profit hackerspaces constitute the front line in the resistance to recuperation, while a decade ago they benefited from the recuperation of anti-capitalist hacklabs. The role of historical memory is highlighted in this case as setting the baseline for calculating recuperation, which may inform tactics, demands, practices, and perceptions.

Concluding Discussion

On the basis of three case studies of hacker initiatives, we have proposed a conceptual framework for how alternative visions and practices of technology are systematically captured and fed back into the industry’s development process. The backbone of this framework is Boltanski and Chiapello’s theory of how capitalism transforms itself and overcomes limits with the help of recuperated critique. We have proposed an analytical distinction between three different time intervals within which processes of recuperation unfold in the hacker subculture, so that the resistance of hackers to recuperation attempts may be studied with more precision, and set in relation to capitalism as an evolving whole: “the spirit of the times.” The concept of recuperation has a great deal of explanatory power to offer for studies of the symbiotic, yet antagonistic, relation between the hacker subculture and the computer industry.

Recuperation aims to limit the functional autonomy of a community so that it can be subsumed into capital’s valorisation process. The autonomy of the collective is the defining limit between the formal and the real subsumption of labour under capital. When a hacker community has a large degree of autonomy, it may determine the ultimate goals of its collective efforts, and thus the general direction of its own future becoming. We have identified three pillars that support the functional

---

1 The Amsterdam Subversive Centre for Information Exchange (ASCII, 1999–2006), a hacklab or squatted Internet café in Amsterdam. https://hackstory.net/ASCII, https://scii.nl/
2 Progressive Utrecht Subversive Centre for Information Exchange (PUSCII, 1999–), a hacklab and Internet space hosted for a long time in the Ubica squatted social centre, now without a physical location. https://hackstory.net/PUSCII https://www.puscii.nl/
3 The Squatters’ Linux User Group (SLUG, 2007–), which fitted hacklabs into many occupied spaces over the years, helping activists to adopt free software and recycled hardware. https://slug.squat.net/places/index.html
4 Nurdspace (Never Underestimate Real Development Spaces) is the hackerspace in Wageningen, the Netherlands. Interview with dreamer on 2013-12-07 on location. https://nurdspace.nl/
5 Hack42 is the hackerspace in Arnhem, the Netherlands. Interview with dreamer on 2013-12-07 at the Nurdspace. https://hack42.nl/
autonomy of a hacker community: technical expertise, shared values, and historical memory. Taken together, these three pillars of autonomy enable hackers to cultivate critical opinions about predominant, technological designs, and engineering practices, as well as to pursue alternative pathways in technology development. With the term “functional autonomy,” we want to capture the fact that the political economy of hacking is intimately intertwined with those of state and capital, and yet, paradoxically, allow for a circumscribed room for manoeuvre wherein critical engineering practices may flourish.

Even when all three pillars of autonomy are firmly in place, the odds are stacked against the hackers, so that they often succumb to recuperation anyway. However, and this is a pivotal point in our argument, the same favourable conditions for putting up resistance to capital are seldom present in those looser constellations that are variously labelled “users,” “makers,” “citizen scientists,” etc. Unlike hackers, the latter do not draw from a common pool of technical skills, shared cultural values, and historical memory. Granted, the contingency unleashed by a novel design or an unanticipated application of a pre-existing product might open up a window of opportunity for non-incumbents to act. In due course, however, such challenges to the status quo will in all probability be settled on the terms of state and capital. The disturbance from unruly mis-users has always already been anticipated by the open innovation model. Likewise, the David-versus-Goliath narrative in which DIY and maker practices are awash has been fully integrated into the marketing strategies of entrepreneurs and firms.

In spite of a vast backlog of bottom-up interventions in science and technology that at various points in time have had their emancipatory claims voided, this historical lesson remains under-theorised in the scholarly literature on the subject. This invites a second-order reflection on how the configuration of the user [47], lay expertise [48], or critical making [49] has been discussed in Science and Technology Studies and neighbouring fields over the years. In our reading, this lacuna is due in part to the influential notion that STS scholars must take the statements of practitioners at face value. With his famous slogan, “Follow the actors!” Latour sought to dethrone the critic by banning the use of “overarching theoretical concepts.” As a consequence of this methodological stricture, the limited outlook of the actors under study is exactly reproduced by the analyst. The task for emancipatory technology studies must be a different one: to contribute with a theoretical and historical understanding of the structural constraints under which capitalism can be effectively contested, with the aim of strengthening practitioners’ ability to resist recuperation attempts. The conceptual framework that we are proposing here does not balk at pointing out the compromised subject position of the practitioner, but on the condition that this analytical procedure is coupled with an inquiry into the critic’s own, compromised subject position. After all, both are operating under the same structural constraints of capitalism.

Funding Open access funding provided by University of Gothenburg.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Turner F (2006) From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism. University of Chicago Press, Chicago
2. Coleman G (2014) The new Snowden revelation is dangerous for Anonymous—and for all of us. Wired, 4th February. https://www.wired.com/2014/02/comes-around-goes-around-latest-snowden-revelation-isn't-just-dangerous-anonymous-us/
3. Liu A (2004) The laws of cool. University of Chicago Press, Chicago
4. O’Neil M, Zacchirolsi S (2017) Making lovework: Editorial notes for the JoPP issue on peer production and work. J Peer Prod (10):1–3. http://peerproduction.net/issues/issue-10-peer-production-and-work/editorial-notes/
5. Fuchs C, Boersma K, Albrechtslund A, Sandoval M (eds) (2011) Internet and surveillance: The challenges of Web 2.0 and social media. Routledge, New York
6. Söderberg J, Delfanti A (2015) Hacking hacked! The life cycles of digital innovation. Sci Technol Hum Val 40(5):793–798. https://doi.org/10.1177/0162243915595091
7. Söderberg J, Delfanti A (2015) Repurposing the hacker: Three temporalities of recuperation. UC Davis, Previously Published Works. https://eprints.cdlib.org/uc/item/9c86493g
8. Maxigas, (2017) Hackers against technology: Critique and recuperation in technological cycles. Social Studies of Science 47(6):841–860. https://doi.org/10.1177/0306312717736387
9. Boltanski L, Chiapello E (2005) The new spirit of capitalism. Verso, New York
10. Chesbrough HW (2003) Open innovation: The new imperative for creating and profiting from technology. Hardcover. Harvard Business Review Press, Watertown, MA
11. von Hippel E (2005) Democratizing innovation. MIT Press, Cambridge, MA and London
12. Flowers S (2008) Harnessing the hackers: The emergence and exploitation of outlaw innovation. Research Policy 37(2):177–193. https://doi.org/10.1016/j.respol.2007.10.006
13. Oost EV, Verhaegh S, Oudshoorn N (2009) From innovation community to community innovation: User-initiated innovation in wireless Leiden. Science, Technology, & Human Values 34(2):182–205. https://doi.org/10.1177/0162243907311556
14. Levy S (1984) Hackers: Heroes of the computer revolution. Anchor Press, Doubleday, New York, NY
15. Zandbergen D (2011) New edge: Technology and spirituality in the San Francisco Bay area. Doctoral dissertation, University of Leiden, Leiden.
16. Flichy P (2007) The internet imaginaire. MIT Press, Cambridge
17. Harvey D (2005) A brief history of neoliberalism. Oxford University Press, Oxford
18. Barron A (2013) Free software production as critical social practice. Eco Soc 42(4):597–625
19. Tkacz N (2012) From open source to open government: A critique of open politics. Ephemera 12(4):386–405
20. Söderberg J (2017) Comparing two cases of outlaw innovation: File sharing and legal highs. In: Godin B, Vinck D (eds) Critical studies of innovation: Alternative approaches to the pro-innovation bias. Edward Elgar, Cheltenham, UK, pp 116–136
21. Schwarz J (2014) Filesharing: Innovations in media consumption. Routledge, London
22. Aronowitz S (2015) Against orthodoxy: Social theory and its discontents – Marx. Braverman and the logic of capital, Macmillan, London
23. Montgomery D (1976) Workers’ control of machine production in the nineteenth century. Labor Hist 17(4):485–509
24. Rosich G (2019) The contested history of autonomy. Bloomsbury, London
25. Denbow J (2015) Governed through choice: Autonomy, technology, and the politics of reproduction. New York University Press, New York
26. Gill R, Pratt A (2008) In the social factory? Immortal labour, precariousness and cultural work. Theory Cult Soc 25(78):1–30
27. Kelty C (2008) Two bits: The cultural significance of free software. Duke University Press, Durham, NC
28. Coleman G (2010) The hacker conference: A ritual condensation and celebration of a lifeworld. Anthropological Quarterly 83(1):47–72
29. Thomas G (2014) How a German soda became hackers’ fuel of choice. Vice Magazine, 10th February.
30. Maxigas (2015) Peer production of open hardware: Unfinished artefacts and architectures in the hackerspaces. Doctoral dissertation, Universitat Oberta de Catalunya, Internet Interdisciplinary Institute, Barcelona.
31. Dunbar-Hester C (2014) Low power to the people: Pirates, protest, and politics in FM radio activism. MIT Press, Cambridge, MA
32. Lindtner S, Li D (2012) Created in China: The makings of China’s hackerspace community. Intersections XIX 6:5–49. https://doi.org/10.1145/2377783.2377789
33. Pip S, Xin G (2018) Makerspaces and urban ideology: The institutional shaping of Fab-Labs in China and Northern Ireland. J Peer Prod. 12 (July). http://peerproduction.net/wp-content/uploads/2018/07/jopp_issue12_sheu_gu.pdf
34. Maxigas (2017) Keeping technological sovereignty: The case of Internet Relay Chat. In: Haché A (ed) Technological sovereignty, vol 2. Ritimo, Paris, pp 67–81
35. Maxigas, Latzko-Toth G (2020) Trusted commons: Why ‘old’ social media matter. Internet Policy Review 9 (4). https://policyreview.info/articles/analysis/trusted-commons-why-old-social-media-matter
36. Coleman G (2012) Coding freedom: The ethics and aesthetics of hacking. Princeton University Press, Princeton, NJ
37. Broughton J (2008) Wikipedia reader’s guide: The missing manual, 1st edn. Pogue Press and O’Reilly Media, Sebastopol, CA
38. Dagdelen D (2012) Anonymous, Wikileaks and operation payback: A path to political action through IRC and Twitter. Paper presented at the IPP2012: “Big Data, Big Challenges?”, Oxford Internet Institute, Oxford, UK.
39. Bowyer A (2004) Wealth without money: The background to the Bath replicating rapid prototyper project. RepRap project wiki. https://reprap.org/wiki/Wealth_Without_Money
40. Söderberg J (2014) Reproducing wealth without money, one 3D printer at a time: The cunning of instrumental reason. J Peer Prod 4 (January). http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/reproducing-wealth-without-money/
41. Maxigas (2015) Hacklabs and squats: Engineering counter-cultures in autonomous spaces. In: Moore A, Smart A (eds) Making room: Cultural production in occupied spaces. Other Forms & the Journal of Aesthetics and Protest, Los Angeles, CA, pp. 328–341. http://joaap.org/press/makingroom.htm
42. Davies SR (2017) Hackerspaces: Making the maker movement. Polity, Cambridge
43. Söderberg J (2013) Determining social change: The role of technological determinism in the collective action framing of hackers. New Media Soc 15(8):1277–1293. https://doi.org/10.1177/1461444812470093
44. Maxigas (2012) Hacklabs and hackerspaces: Tracing two genealogies. J Peer Prod 2 (July). http://peerproduction.net/issues/issue-2/peer-reviewed-papers/hacklabs-and-hackerspaces/
45. Owens L (2009) Cracking under pressure: Narrating the decline of the Amsterdam squatters’ movement. Amsterdam University Press, Amsterdam

46. López MAM (2013) The squatters’ movement in Europe: A durable struggle for social autonomy in urban politics. Antipode 45(4):866–887. https://doi.org/10.1111/j.1467-8330.2012.01060.x

47. Woolgar S (1990) Configuring the user: The case of usability trials. Sociol Rev 38(1):58–99. https://doi.org/10.1111/j.1467-954X.1990.tb03349.x

48. Wynne B (1992) Misunderstood misunderstanding: Social identities and public uptake of science. Public Understanding of Science 1(3):281–304. https://doi.org/10.1088/0963-6625/1/3/004

49. Ratto M (2011) Critical making: Conceptual and material studies in technology and social life. The Information Society 27(4):252–260. https://doi.org/10.1080/01972243.2011.583819

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.