Hackers against technology: Critique and recuperation in technological cycles

Maxigas
Internet Interdisciplinary Institute, Universitat Oberta de Catalunya, Barcelona, Spain

Abstract

I offer an interpretation of hackers' technological choices through a theoretical framework of critique and recuperation in technological cycles, building on prior research that brings the pragmatic sociology of Boltanski and Chiapello to bear on matters in Science and Technology Studies. I argue that contextualizing technology choices in the development of capitalism through innovation illuminates their political significance. I start with the counter-intuitive observation that some browser extensions popular with hackers, like RequestPolicy, make it considerably harder for them to look at websites. This observation showcases Luddite aspects of hackerdom, in that they are willing to 'break' popular websites that would otherwise 'cheat' on the user. In line with an undercurrent of hacker studies, in this case study I find hackers fighting technological progress, which they see as social decline.

Keywords

hackers, expertise, users, history of technology, recuperation, technology choices

Correspondence

Maxigas, Internet Interdisciplinary Institute, Universitat Oberta de Catalunya, Parc Mediterrani de la Tecnologia, Av. Carl Friedrich Gauss, 5, 08860 Castelldefels, Barcelona, Spain.

Email: maxigas@anargeek.net

Introduction

The story begins in a dark basement in Budapest.[1] The organization is one of many hacker clubs around the world – properly called hackerspaces – where sophisticated technology users and developers come together to socialize, learn and teach, tinker and work on projects (Davies, 2017; Smith et al., 2017). Hackerspace members distinguish themselves from makers and other DIY folks by emphasizing that they are both 'making and breaking' technologies (webmind, hacker, personal communication).

On one ordinary day in the hackerspace, members sat around a large table using laptops and having occasional conversations. While they were present in the space in their bodies, they also monitored the chat channel of the hackerspace to interact with each other and remote participants. One of the latter posted a link to the channel pointing to a news item related to security and privacy on a mainstream website. The first complaint in the room was that the link went to a blank page. Another participant suggested 'enabling JavaScript' in the web browser to see the content, but even then it would not load. Somebody else noticed that the website was pulling in content from other websites, something that these hackers' configuration automatically blocks through a specially crafted browser extension: RequestPolicy.[2] When this next obstacle was surmounted, it turned out that the website had an https certificate of questionable authenticity, so users could not even be sure if they were reading the authentic website or a forgery. By this point, a benevolent member opened the link in a sandboxed virtual machine running on his laptop, copied the article and pasted a plain text version on a safely configured web page managed by himself for the group to see. The conversation drifted from the content of the article to indignant complaints about the content delivery system: Why would users have to execute JavaScript programs, let their browsers leak information to six additional servers, and click through bogus authentication warnings just to see three pages of alphanumerics? The interpellations were along lines of: 'We have to fix the Internet.' 'The Industry went wrong.' 'The Web was not made for this.' Following the incident, alternative content delivery systems were considered and debated.

In the meantime, I was wondering to myself, 'Why does it take so much time and effort for these users to read an article on a mainstream news website, especially when they are supposed to be "good with computers"?' The ritualistic posturing around such a small issue is the kind of thing that anthropologists connect to larger frames of reference, to spell out what is at stake for hacker culture here. I will do so by referring to hacker goals of 'resisting the recuperation of the Internet by capital' (Bastani, 2011), in the face of 'an impending

---

1 The scene presented is based on my field notes from April 2012, when I participated in the activities of the Hungarian Autonomous Center for Knowledge (H.A.C.K.) as a founding member and budding anthropologist. See http://hsbp.org/

2 In this article I focus on only one particular browser extension: RequestPolicy, developed by Justin Samuel.

recuperation by Capitalism that must accommodate or restrict anonymity' (Wade, 2014: 9). The proposed framework of critique and recuperation in technological cycles allows a better understanding of the dynamic of innovation in informational capitalism, and by analyzing the empirical data I show how sophisticated users such as hackers can develop critical technology choices in response.

Thus, the main objective of the paper is to define a theoretical framework of critique and recuperation in technological cycles, and demonstrate its interpretative power on a concrete critical case study of hacker culture. The approach has been hinted at by Barron (2013) in connection to free software development, and proposed by Söderberg and Delfanti (2015) in the introduction to a special issue on 'Hacking Hacked'.

I construct the study primarily as a paradigmatic case (Flyvbjerg, 2006; see also Yin, 2002) of technology choices within hacker culture, in resistance to the digital imperative. Such a research strategy continues a tradition of paradigmatic case studies in Science and Technology Studies (STS), identified by Beaulieu et al. (2007). It is also a *critical* case in the sense that it shows hackers fighting technological progress – in stark contrast to their established image as disruptive innovators, early adopters and technology enthusiasts. In other words, here hacking appears is a critique rather than a championing of modernity.

Beyond purely theoretical concerns, my political motivation behind writing this paper is that the ideas of critique and recuperation in STS have so far only been mobilized in the service of pessimist interpretations – 'sociology against fatalism' (Boltanski and Chiapello, 2005: 529–536) – that ultimately justify existing social orders. I argue that analyzing a historical logic critically can reveal possibilities for resistance as well as realities of contestation. Thus, I offer hope in the face of explanations that may err on the side of social determinism.

Last but not least, I identify three factors that enable hackers to make technological choices that challenge the digital imperative. The combination of technical expertise, historical consciousness and shared values together allow for resistance against the recuperative historical logics of capitalism. Systematic analysis paves the way for the generalization of the theory. For instance, it becomes possible to explain the passivity of IT students who lack a historical horizon, or the desperate hacks of Amish who lack the technical expertise (Ems, 2014), and also to propose remedies for these shortfalls.

Data and methods

The vignette above is an instance of the typical use pattern of the RequestPolicy browser extension, indicative of the more general technological choices of hackers. I identified the pattern in empirical data gathered through participant observation in European hacker scenes between 2012 and 2015, scenes to which I gained access through prior experience as a contributor.

The people I studied are more actively and frequently engaged in hacker-themed activities than are the average participants of the same activities. Therefore, they are representative of hacker culture per se, rather than of the hacker population. My subjects were most commonly middle-aged, highly educated city-dwelling white males working as technology

professionals. They take part in the circuits of the scene as organizers, contributors and attendants (or significant boycotters) of various hacker-themed spaces, events and projects. In this capacity they consider themselves to be advanced and sophisticated computer users, even though many promote the browser extension presented in this case study as 'user friendly' to all computer users they encounter. While this browser extension has indeed many other casual users, these hackers go further along with the script built into the technology by explicitly problematizing the issues that the software highlights. Therefore, their degree of reflexivity on and identification with the technology sets them apart from other strands of privacy-conscious users and activist advocates.

Similar technical difficulties and verbal exchanges to that of the vignette above occurred during the hacker gathering 'Observe. Hack. Make.' organized near Geestmerambacht, Netherlands in 2013 (Maxigas, 2014a), as well as the Chaos Communication Congress in Berlin in the same year. Meanwhile, I was following on a daily basis the chat channels[3] that effectively serve as the social media of hackers (Maxigas, 2017), and found more traces of this type of interaction. For instance kwadronaut, who never visited the particular hackerspace in Budapest, recognized and summarized similar moments on the #tech channel of the Indymedia chat server thus: 'hey look at this , really cool/interesting/nice/fancy/sweet/..' me: "huh, it's an empty page?"' (IRC log, 2014-01-15 17:51 GMT). In this way the basis of the case study has been developed with the involvement of around 30 individuals from different hackerspaces or software development circles. Each enactment of these ritual interactions occured within a small group of five to eight participants over five to twenty minutes of discourse. It is reasonable to assume that such things are bound to happen every time users of this particular technological repertoire meet.

I presented preliminary results to practitioners at the FSCONS Free Society Conference in 2014 and the 5th Birthday of H.A.C.K. in 2015. These were opportunities to further test and refine my hypotheses based on the reactions of the target group of the study (2014b, 2015). Since participative observation is an interpretative methodology, my interpretation is one of many, but it is validated by the consistency of the facts that make it cling together, as well as by the self-recognition of its subjects in the narrative. While for narrative reasons I focus on what happened at H.A.C.K. one day as a typical example, I mobilize a much wider range of empirical material to construct a case around hackers as particular kind of sophisticated users.

Technological choices and the digital imperative

Sophisticated users' technology choices involve aspects of adoption and non-adoption which are informed by their engineering tastes and political values (Bailey and Leonardi, 2015). Hackers' enthusiastic responses to technology have been analysed at length in classic works (e.g. Coleman, 2012; Kelty, 2008; Levy, 1984; Turner, 2006). However, we can also learn from non-adoption – especially since resistance is more often seen as a politically

---

3 Almost a hundred Internet Relay Chat channels mainly associated with hackerspaces or conventions, such as #hackerspaces, #noisysq, or #techinc.

significant act than creation (Casemajor et al., 2015). Furthermore, it is the breaking of technologies that sets apart hackers from makers.

Oudshoorn and Pinch (2003: 16) state that non-use is a significant area in the analysis of technological change. Non-adoption – a wider term – can have as much impact on the development of a technology as use. Non-adoption often involves the development of *other* technologies and features which enable or aid non-use (Kline, 2003). Therefore, technology non-adoption may be as much of a technology-intensive process as technology adoption.

Wyatt (2008) classifies non-users as (voluntary) *rejecters* and *resisters*, as well as the (involuntarily) *excluded* and *expelled*. Rejecters are people who 'tried it and gave it up voluntarily' (p. 9). They are the most relevant to this study, since the task at hand is to understand how expert users – such as hackers – who are potential innovators come to reject innovations in their technology choices. More succinctly: What knowledge does it take to try out and then reject a technology? Wyatt rightly emphasizes that these users are the most important methodologically for understanding the political dimensions of non-adoption, summed up as *challenging the digital imperative*.

The digital imperative is Wyatt's application of the *technological imperative* concept formulated by Ellul (1964, 1980). Once (digital) technologies are introduced, we are compelled to use them and pursue what we come to see as their full potential – irrespective of the social consequences. The case below centres on the most elementary gesture of the digital imperative today, browsing the internet. I explore how hackers as non-adopters of new internet-making practices challenge the digital imperative as part of their sophisticated technology choices.

The 'people who choose not to use digital technologies remind us all that things "might have been otherwise"' (Wyatt, 2008: 11, citing Bijker and Law, 1992: 3). Non-users sketch out alternative development paths that technologies could have taken. While this is true in the present case, the choices of sophisticated users also remind us that things *were in fact otherwise*: They think that something went wrong. They feel that time is out of joint, and volunteer to set it right. Thus, I highlight that challenging the digital imperative can be attempting to correct what is seen as a failure in the history of technology, a constructive move.

Wyatt finds the digital imperative that non-adopters challenge in 'the idea that there is a single, digital logic for all individuals, organizations and countries' (Wyatt, 2008: 11). My interpretation involves a subtle shift in emphasis from the critique of modernity to the critique of capitalism: While the idea of Wyatt's digital imperative – that technological development leads to a better life — is an idea best ascribed to modernity, capital often mobilizes the same notion to make profit and overcome critique. Moreover, the situation is complicated by the fact that in this case the contestation of the digital imperative comes from its core. Hackers are so enthusiastic about digital technologies that they debate and question them vigorously.

As Lindsay (2003) observes, the triad of *nostalgia*, *efficiency* and *resistance* (or here, *rejection*) describes the negative technological choices of some hackers. I argue that in the case here, hackers' critical technology choices are rooted in late-1990s cyberculture

imaginaries and 1990s industry standards. Only a minority of users would champion the dial-in Bulletin Board Systems over the World Wide Web (Driscoll, 2016), but the users described here are unsatisfied with the *new* internet because from their perspective the *old* internet was in some respects better. Along similar lines, Dunbar-Hester (2009) describes how new waves of technologies are interpreted by politicized users in the light of older technologies, as they try to adapt their existing understanding of older ones to newer ones. However, she adds to the aforementioned triad another factor: *the perceived socio-political effects of technology* influence its adoption by activist and advocacy groups (Dunbar-Hester, 2009: 234).

Lindsay and Dunbar-Hester understand seasoned users as mediators between past and future, and between producers and potential users of technologies. Hackers' non-adoption as a high-profile rejection of certain functionalities may lead to the exploration of alternative pathways of technology development. Indeed, the high-profile non-adoption of third party requests through the RequestPolicy browser extension and similar solutions led to the development of the Do Not Track HTTP header standard through the World Wide Web Consortium (W3C) and its subsequent widespread implementation in major web browser software. I argue that the choice of alternative pathways is a political question, in that they participate in shaping the techno-political realities in which we are all immersed. I investigate how non-adoption, understood as a political act (Dunbar-Hester, 2009), can also motivate the development of new technologies (Kline, 2003; Lindsay, 2003). Drawing on the work of Kleif and Faulkner (2003), I also show how rejection might be uncomfortable even for sophisticated users for whom rising to the challenge also holds particular engineering pleasures.

Mediation and conflict between hackers, a small but privileged group of users, and firms, often virtual monopolies, are vulnerable to recuperative logics. In his study of technology-oriented and product-oriented movements, Hess concludes that community demands and development of technologies happen in a private-sector symbiosis. Even where these movements succeed in pushing a technology to the consumer market, they are recuperated in the process, resulting in 'object conflicts' about their proper design and use (Söderberg and Delfanti, 2015). Furthermore, Hess states that 'in general, the object conflicts are embedded in much more hidden processes, such as physicians' choices to offer specific types of programs' (Hess, 2005: 13). In line with Hess's observations, this case study does not capture a highly visible, articulated and organized opposition, but instead the hidden subtext of technological struggles where object conflicts unfold in everyday technology choices.

The theoretical insights I've surveyed above do not insert hackers' resistance to technology into the historical logic of innovation under informational capitalism. Therefore, in the next section I turn to literature rooted in the French pragmatic school of sociology, a sociology of critique that explicitly engages with the dynamics of innovation. I attempt to rearticulate its core tenets and formulate a new theoretical synthesis, showing how it is helpful for the systematic study of technological choice from an STS perspective.

Critique and recuperation in technological cycles

Boltanski (2009: xi) defines critique as unmasking the hermeneutic contradiction between the meanings of institutions and how those institutions work in practice, 'making it possible to challenge the reality of reality'. He criticizes the sociology of Bourdieu and others, arguing that its structural determinism disempowers actors (p. 2). In contrast, the sociology of critique empowers actors by studying how critique works in practice, increasing its consistency and expanding its possibilities. Thus Boltanski and Chiapello (2005) point to how critique is often undermined by capital during its implementation, a process they call recuperation.

Barron (2013) mobilizes the concepts of critique and recuperation to illuminate the contradictions in technological controversies driven by hackers. More than that, she argues that hackers are at the forefront of the contemporary network capitalism. Their ethos 'can be shown to embody "The New Spirit of Capitalism" in its most distilled form' (1). Therefore, understanding their critique and its recuperation is instrumental for mapping the dynamics between political struggles and the technological, cultural and ethical innovation driving the evolution of capital.

Boltanski and Chiapello (2005) identify recuperation as a cyclical logic in capitalism. Recuperation periodically re-energizes capitalism through a two-sided operation. On the one hand, critique is absorbed into capitalist ideology and practices. On the other hand, things that were previously not part of the capital accumulation process start to be valorized. Thus, capitalism answers to critique through restructuring in a way that simultaneously implements, but also neutralizes and eventually undermines that critique. Through their analysis of the critiques generated by the struggles around 1968 and the restructuration of capitalist legitimation and work organization in the following decades, Boltanski and Chiapello show how 'recuperation-implementation' works. Söderberg and Delfanti (2015) point out, in the introduction to a special section of *Science, Technology, & Human Values* on 'Hacking Hacked', that in a more general sense 'Boltanski and Chiapello take this concept further, *depicting the evolution of capitalism as strictly intertwined with the practices that oppose it*' (emphasis in original).

Recuperation-implementation involves the extraction of value from things that were earlier outside of the commodity sphere. The specific move is called commodification, and it is at the centre of my argument. The thing that just enters capital accumulation was 'authentic' before. Therefore, the commodification of authentic things is part of recuperation:

> [recuperation] proceeded in tandem with a commodification of *goods that had hitherto remained outside the commodity sphere* (the very reason they were deemed authentic): capitalism was to penetrate domains (tourism, cultural activities, personal services, leisure, etc.) which had hitherto remained comparatively external to mass commodity circulation. (Boltanski and Chiapello, 2005: 442, emphasis in original)

Following Barron (2013), I argue that, since technologies are an integral part of social processes, subsequent generations of technologies and associated deployment practices are instrumental in specific cases of commodification. Furthermore, Boltanski and Chiapello assert that when commodification 'sells out' things that were once authentic, it kindles

anxiety in some users who are sensitive to recuperation. In particular, commodification involves a secondary strategic intention that undermines the trust between the user and the tool at hand. Just as there is a material residue of commodification (for instance deployments of obsolete technologies), there is a corresponding affective residue. In short, the lack of authenticity causes anxiety in users:

> Commodification thus creates new forms of anxiety about the authenticity of things or persons ... authentic is that which has been made without a secondary strategic intention. (p. 447)

In my view, such anxiety can form the affective, aesthetic, cultural basis – the motivation – for non-adoption of commodifying new technologies. The authors of *The New Spirit of Capitalism* argue that commodification breeds anxiety because it simultaneously demands and destroys authenticity; but what if users found a way to bring such vicious circle to a halt? Echoing Bijker, Law and Wyatt's comments on non-adopters, Boltanski and Chiapello (2005: xliv) also advocate 'returning to the moment when things were decided, and making it clear that they could have taken a different turn'.

I suggest that while recuperation is a long-term dynamic of contemporary capitalism, it takes place iteratively and hence it can be shown to be at work in smaller cycles (Maxigas, 2017). Users who have the characteristics defined below, e.g. technical expertise, historical consciousness and shared values, may be able to take note of it (Maxigas, 2015: 208–215). *The New Spirit* raises these questions, though without proposing concrete remedies. Boltanski and Chiapello (2005: xliv) call for a 'sociology against fatalism', against the 'retreat ... into the receptive matrix of determinism, social, economic or biological'. To these determinisms now we can add technological determinism. Even if the overall recuperative logic of capitalism cannot easily be challenged, everyday rejection of micro-changes (like the non-adoption of commodifying technologies) can possibly thematize these problems and lead to reflection:

> In the course of this work, opportunities to resist micro-changes with ominous consequences also emerged that were missed by those who should have been especially vigilant about the risks entailed by these transformations - in particular, because they did not realize that the 'recuperation-implementation' by capitalism of some of their proposals required them in turn to reinvest in analysis and shift ground. (Boltanski and Chiapello, 2005: xliv)

Critical technology choices in themselves may not rest on the analysis of recuperation; that is where studies such as this one may contribute to struggles. However, the rejection of some mainstream technologies in favour of the adoption and development of others mounts a challenge to micro-changes – with ominous consequences – that bring recuperation-implementation to everyday life. In the next section I present empirical data to suggest that these micro-changes are detected through the affective residue of commodification.

Commodification undermines the trust between the user and the tool, raising the question arises, 'Who is using whom?' It is easy to see how products and services like free software tools and gratis digital platforms can exert anxiety about their authenticity in users, especially the users who are themselves involved in the production of free software and online platforms. In the following section I flesh out the case study, investigating the

collisions between technological frames and showing how the resulting debris can lead to the development of new technologies and the cultivation of political values.

Case study: The RequestPolicy browser extension

It is crucial to carefully characterize the delivery of complaints like 'huh, it's an empty page', since the analysis depends on it. Since hackers are distinguished by their technical expertise, it is hard to believe that they repeatedly encounter an insurmountable challenge in these situations. Subterfuge is more likely. They *know* what is going on perfectly well, but instead of quietly making the necessary adjustments to their machinery to accept the content fed into it, they choose to halt and act as though they have no idea what is going on, feigning surprise (here signified by 'huh'). There is a hint of work-to-rule practices in the gesture, where workers restrict themselves in order to lower efficiency and raise questions about the organization of production. Even though their equipment is configured to 'break' certain websites on their own screens, at the onset the hackers are startled and they will say so; after looking into the matter they make it clear that the website is at fault. Yes, they *know* that the website was supposed to work by the browser pulling it together from multiple sources. Indeed, they *know* that the website works well for internet users who do not to make special precautions against these mainstream industry practices, but that is exactly where the problem lies, they will tell you. In other words, the particular website is not buggy or broken according to the technological ideals – and technological practices – of the website makers, or even most of the website users. It is buggy and broken – or more precisely it becomes buggy and broken on the hackers' screen – according to the technological ideals of these particular users. Even though it is generally desirable for them to look professional and brag about their expertise, when they encounter a socially problematic technological choice, they start dragging their feet.

RequestPolicy is recommended by the Electronic Frontier Foundation, a respected authority in the hacker scene (Auerbach, 2013). Modern websites are digital patchworks and kaleidoscopes, inserting content from and leaking user information to a number of third party services that run on other servers. RequestPolicy breaks such mechanisms. Embedded YouTube videos, advertisements sold through DoubleClick, Google Analytics code gathering statistics about visitors, comments made through the Disqus service are all served from external servers operated by third parties. Third parties may or may not be independent entities, although thanks to recent market concentration, it often happens that the most significant number of external requests terminate at the servers of Google, Inc. – YouTube (video sharing), DoubleClick (advertisements), and Google Analytics (visitor statistics) are only some of its subsidiaries. Google uses the data it processes for free to enhance its targeted advertising offers, and the same data is provided to law enforcement agencies through a special interface (Ippolita, 2015: 7). As its author explains, RequestPolicy 'makes it so that you decide when your browser should obey commands by one website to make requests to other websites' (Samuel, 2013). It has two self-declared objectives: to enhance the users' security and to protect their privacy. It asserts that one webpage can only load contents from one domain – the very same domain which the user typed into the address bar. The documentation states the rationale behind the browser

extension clearly: 'It makes sense that your browser would only be communicating with the website whose domain you see in the address bar at the top of your browser' (Samuel, 2013).

In the following sections I identify three factors (marked by section headings) that allow hackers to identify with such a position and find such a technical feature meaningful. I begin each section with an introduction to the empirical context of the analysis, with the H.A.C.K. hackerspace in the foreground and information about the wider hacker culture around it in the background. I understand the factors themselves as the pillars for the semi-autonomy of hacker scenes, allowing participants to formulate their own positions within the wider history of technology – and even capitalism.

Technical expertise

Hackers are brought together by the fascination, but also the frustration, with technology. Consequently, hackerspaces, hacker conventions and the relevant chat channels are places of learning and debate. H.A.C.K. provides the material infrastructure and the social milieu for opening up and questioning technologies, such as a shared electronics laboratory and a bar, neither of which have clearly defined architectural boundaries – a common arrangement in hackerspaces. Consequently, members and visitors standing in front of a whiteboard covered in mathematical formulas with beer in one hand and whiteboard marker in the other are a common sight.

The users featured in my opening vignette end up reading, evaluating and discussing a technical text, empowered by their knowledge as much as their tools. Instead of reading the article, they are looking at how it is delivered to them: deciphering the medium instead of the message. Technical expertise is essential for mounting a challenge to technological innovation. The ability to break the protocols – through technical knowledge and material tools – of the underlying architecture of mass media is a necessary condition for establishing a reflective distance.

Kelty (2008) identifies such typical hacker behaviour as creating a *recursive public*. My interest is not in how such a public is organized, but rather how it can stage interventions into the scripts inscribed in everyday technologies, interrupting the intended functioning of a debated public sphere such as the web. The situation enacted around RequestPolicy artificially creates a moment of breakdown by 'returning to the moment when things were decided', where they can remind us that things 'might have been otherwise'. It halts the machine of supposedly linear technological progress, rendering inoperable the most basic gesture of the digital imperative: to browse websites endlessly in a smooth flow.

We can learn more from the technical breakdown caused by the RequestPolicy browser extension, and the social breakdown that follows when hackers are startled and start their commentary on the 'incident', than from hackers' reactions to the content of the webpage. The medium structures the agency of the average internet user to a greater degree than a mere news article, and the medium is certainly more relevant for the state and capital (Fuchs, 2012; Wittel, 2012): for media monopolies, the recording of everyday gestures is the basis of capital accumulation, and authorities use the same records for law enforcement. The RequestPolicy browser extension is a device that automatically brings to

the foreground these central issues of political economy and forces users to pay attention, and hackers seem to enact that script to its full potential.

Historical consciousness

Nostalgia may be a common trait of engineering cultures, but hacker circles are especially committed to historical continuity. Some hackerspaces maintain unique establishments such as the Museum of Functioning Informatics,[4] but even smaller hackerspaces – such as the one in Budapest – abound in old hardware in various states of repair, including at least one operational Commodore 64 microcomputer.[5] Similarly, the hackers' social media of choice, Internet Relay Chat, is a protocol and infrastructure dating back to 1988: the year before the World Wide Web was invented. These technological choices distinguish hacker clubs from similar shared machine shops such as Fab Labs, accelerators and incubators.

Justin Samuel, the author of RequestPolicy, claims that third party requests are socially harmful. However, the whole notion of blocking third party requests goes against the established best practices of the website operators, and against the DNA of popular blogging platforms, news sources and online applications of the Gmail type. Considered outside the context of discourse around privacy and security, the common sense articulated by RequestPolicy quickly loses its coherence. Reconsidered from the point of view of the industry's mainstream operations, or even from the perspective of the average internet user, hackers' adoption of the browser extension is a retrograde attempt to rewind web history: a *Luddite machine* that, as they say, 'breaks' the essential mechanisms of websites. As this snippet of conversation on an IRC channel shows, for the consumers, including hackers, it is a usability nightmare which transforms the browsing experience into a detective game that never ends:

```
# Channel0 – Channel name anonymised:
— Day changed Tue Feb 10 2015
…
19:23 * taggart curses dkg for showing him RequestPolicy
…
19:47 <dkg> i'd rather just stay off the web in general though
…
19:47 <dkg> and get my actual work done
19:47 <taggart> yeah, I should try that
19:47 <taggart> but when researching stuff it's hard, product
      and review sites are tons of js and remote requests
19:48 <taggart> I'm shopping for a new stove and it's painful
19:48 <taggart> I like the RequestPolicy idea of 'default to
      no remote requests'
19:48 <taggart> and the NoScript policy of 'default to
      no javascript'
19:49 <taggart> but damn it's painful.
```

---

4 Notable examples are found in the hackerspaces of Arnhem, the Netherlands (Hack42); Palazzolo Acreide, Sicily (FreakNet) and Montréal, Canada (Foulab).

5 SIDbox is a related H.A.C.K. project. See https://hsbp.org/SIDBox

For the producers, it defeats their business models, whether the informal and non-profit ones based on the accumulation of reputation (Arvidsson and Peitersen, 2013) or formal and for-profit ones based on the accumulation of capital (Tapscott and Williams, 2006). Modern business models in both areas require outsourcing complex problems critical for success like web analytics, advertising, multimedia content delivery or spam detection.[6] These business models allow 'lean organizations' to concentrate on their 'core competencies' and leave the burden of data gathering, analysis and intelligence to giant companies like Google. Perceived in this way, free services live up to the promise of the internet by enabling a growing number of users to maintain 'their own' websites. On the other hand, for media monopolies like Google, every public service is in search of a business model (Lovink, 2013). In the interpretation of Ippolita (2015: 7), the shift from the 1990s to the 2010s paradigm of internet making was characterized by the realization that providing a public service allows providers to gather information about their publics, data that through profiling can be turned into advertising revenue and intelligence.

Hackerspaces routinely provide their own local services such as wikis, mailing lists and chat channels. In H.A.C.K. all these run on computers owned and operated by members. In contrast, contemporary startup companies routinely outsource their infrastructure 'to the cloud' from the beginning. The adage that originated from the European Free Software Foundation answers to this tendency by stating that 'There is no cloud, just other people's computers.' The slogan is seen on stickers in the hacker club in Budapest, and virtually all the hacker conventions I visited during field work.[7]

It may be impossible for somebody who acquired technical expertise through conventional college education today to imagine making websites that serve their own content without relying on external services. In this context, technical expertise in itself is only a necessary but not a sufficient condition for the critical non-adoption of contemporary web technologies.

In addition to technical expertise, resistance to recuperation requires a community memory shaping aesthetic sensibilities. This is expressed in terms of nostalgic visions for the 'old internet' of the 1990s, including the industry practices of serving all the content from the website that the user is visiting. It is effectively these antiquated practices that RequestPolicy imposes on modern websites – RequestPolicy users invariably started making websites in the 1990s. Common calls to 'fix the internet' only make sense as a contrast to the allegedly working internet of the past. What changed?

On the one hand, in the 1990s most websites were produced by self-designated experts, often without official qualifications. The *webmaster* was an emblematic figure of the era: a single person crafting a site with control over all aspects of production. During the

---

6 As a response, tech-savvy news sources such as Wired Magazine started to refuse displaying articles to visitors who refuse to load ads through third party requests.

7 Attesting to the popularity of the slogan, the online Sexy Hackers a T-shirt version with the description 'Wear this shirt to educate the masses, or use it to start random debates on the merits of storage options.' See https://www.sexyhackers.com/products/shirt-there-is-no-cloud-its-just-someone-elses-computer

following decade, the role of the webmaster in the work process was broken up into backend and frontend developers, graphics designers, programmers and system administrators, user experience experts, search engine optimization gurus, etc. The third-party request is a precise instrument in imposing specialization. The overall effect of third-party requests and services is a decrease in the agency of the website operators and the responsibilities of the webmaster.

Power looms went hand-in-hand with the dismantling of the cottage industry in the time of the Luddites (Sale, 1996). Cottage industries allowed more control for craftsmen over the production process, and the proletarianization in which changing machinery played a crucial part divided the production process into discrete parts. Thompson (1963) emphasizes that breaking machines was not simply an industry dispute over wages, but a critique of a system of production that shaped the life world of the worker.

In the 1990s, the technical community was developing the basic protocols and platforms of the internet through mailing lists with liberal subscription policies (notably in the Internet Engineering Task Force and the W3C). These methods of standardization cultivated a sense of ownership and belonging in internet users and developers, and the spirit of cooperation and consensus empowered independent researchers to contribute to the process. By the end of the 2010s, freelancers and employees of small companies began to feel pressure by larger enterprises both on the website development market and the development of the underlying standards, and the collective feeling of political control had been lost. Major browser vendors were under heavy pressure from competition and responded by implementing new features unilaterally, without consulting the technical community at large, and before consensus could crystallize around a best practice. These shifts were symptoms of a market concentration that had slowly set in during the first decade of the new millennium.

On a larger scale, the initial critique against the mass media that fuelled enthusiasm about the internet included a claim that anybody could make their own website and become a node in a horizontal and decentralized network (Shirky, 2008). However, the massification of the medium led to corresponding compromises in what was to be reclaimed by individual users: from websites (1990s) through blogs (2000s) to posts on social media (2010s).[8] In graphic fashion, the window of opportunity for users to intervene shrank to smaller and smaller input boxes. It is true that the necessary expertise for contributing to the global conversation fell dramatically at the same time, but this fact is not appreciated by hackers. Being both producers and consumers, they often have the necessary expertise to make their voices heard, whatever it takes.

To summarize, the inherent ideal at the core of RequestPolicy thinking is the one-man *webmaster* of the 1990s who built and operated a website on her own, running the entire span of the necessary infrastructure in-house. I relate the widespread lament in hacker circles for the closure of the English language GeoCities service that provided free hosting for users to upload their own website to an expression of nostalgia for a platform belonging

---

8 Schematically, GeoCities.com hosted user generated websites with no constraints on functionality and aesthetics, Blogger.com hosted blogs moulded to themes, Facebook.com hosts uniform user profiles, while Twitter.com hosts mere messages.

to an earlier recuperative cycle. Ultimately, it seems to me that when hackers complain about how broken are some of the most popular websites today, it is only because they decided to go the extra mile and install a browser extension which breaks it for them, but restores ('fixes') some of the old Internet making practices.

Shared values

As shared values are negotiated based on technical expertise and informed by historical experiences, they coalesce into an engineering taste. Such taste forms the centre of the hacker identity, which is in turn articulated in an emblem prominently displayed in hackerspaces, conventions and online fora, the Glider (Raymond, 2014). The nondescript entrance of H.A.C.K. in Budapest is only identified by an A4 printout of the five dots arranged in a particular pattern, which appears again around the interior, as well as on members' tattoos. Displaying the Glider is a way to pledge adherence to the technological repertoire, use patterns and general engineering taste of hackerdom, even in face of the inherent practical difficulties and the inevitable social and market pressure from the outside.

Of course, challenging the digital imperative by way of the digital imperative has its advantages and disadvantages. RequestPolicy disrupts the smooth experience of internet browsing, which is a frustration to even the most nostalgic and expert users. The following snippet from a technical chat channel located on an activist server gives a hint of the affective involvement of 'downgrading the web' that RequestPolicy enforces:

```
# Channel1 – Channel name anonymized:
— Day changed Sat Oct 25 2014
18:43 <taggart> as dkg told me, RequestPolicy makes the internet
     unusable so you can get work done!
18:44 <taggart> so I started using it, but it mostly throws me
     into a fit of rage every day
18:44 <alex> haha
18:44 <alex> i love it
18:45 <alex> i just started boycotting sites like blogger.com
```

The browser extension allows for manually whitelisting certain requests that are essential for reaching the content, but this work has to be done incrementally and comes with the feeling of compromises on core values. Users report boycotting entire web platforms like Blogger, restricting their social life to acceptable areas of the internet. Requests for reposting content ('deep links') from these mainstream websites are common on chat channels frequented by hackers, as the introductory vignette shows. Therefore, I cannot help but notice that the interfaces between contemporary websites and the technological repertoire of hackers is clunky at best and dysfunctional at worst. Any diversion from mainstream use patterns can lead to extra work and much headache. Therefore, non-typical use patterns have to be justified through shared values. Technical expertise allows users to make and break technologies – their historical horizon to compare them – but shared values legitimize judgements.

While it is often frustrating, there is much pleasure to be found in breaking things to 'make a computer do what he wants – whether the computer wants to or not' (Graham, 2004).

Writing on engineering practice and pleasure, Kleif and Faulkner (2003) conclude that their subjects see technical work as an area where they can meet challenges, situations they characterize as highly uncertain, yet ultimately solvable. Struggling with these problems eventually grants a sense of certainty and mastery missing from other aspects of their lives. Their observations resonate with my ethnographic data: The simple existence of third party requests fills some hackers with feelings of insecurity, challenging the integrity and authenticity of data flows. Are the requests originating from the website hackers put in the address bar of the browser, or they are coming from somewhere else? To find out, they invent and resort to diagnostic tools such as the RequestPolicy browser extension.

The tool can restore certainty and lend a sense of mastery to the browsing experience: The user is looking at the content and nothing but the content she really asked for – whether the website wants it or not. Olia Lialina, a GIF artist in the 1990s and an archivist of 'old internet' aesthetics, gives lectures at hacker conferences and campaigns for the lost rights of the users, including 'The right to [s]ee the URL from which content is displayed'.[9] On the same page, Brendan Howell writes: 'Indeed and if you ever open the network tab in the developer view for some crappy big media web site it can be shocking to see all the tracking, ads and api crap that gets loaded from dozens of different servers.' RequestPolicy is a technical measure taken against such a 'shock'. However, it kicks into action every time the user opens a new webpage, and hence allows for replaying the historical drama many times a day in the context of everyday life. The repetitive manner of breaking and debugging websites in the course of browsing the web can explain why hackers would rant about the problems caused or discovered by RequestPolicy.

In this way RequestPolicy allows sophisticated users to exhibit their sophistication to each other and to uninitiated fellow users by declaring 'a blank page', instilling a stoppage and launching into a technical tirade. The appreciation of fine technical points like third-party requests is a sign of a good engineer, and the refusal of external requests as a point of principle is only meaningful in this specific milieu of hackers. Therefore, spending time configuring and discussing RequestPolicy can be interpreted as the cultivation of an in-group identity.

While these affective dynamics and identity constructions describe a wide range of engineering practices, hackers' disruption of the political economy of social media monopolies is not accidental, but rooted in shared values that underpin critical engineering practices. Hackers could choose – and indeed, many other types of hackers do choose – techno-politically irrelevant issues to distinguish themselves. Yet, the uncertainty caused by third-party requests is 'shocking' because it can lead to tracking (profiling based surveillance), selling (profiling based profiting) and in general losing mastery over the tools at hand. These are as much technical as social problems, even when described by hackers in technical terms and addressed through technical means. Indeed, Söderberg (2013) points out that hackers' political engagement – as much as that of capital – often comes cushioned in the language of technological rationality. The critical theory approach of pointing out

---

9 See http://userrights.contemporary-home-computing.org/okka1/see-the-url-from-which-content-is-displa#6dt5p

internal contradictions in the subjects' account (Boltanski, 2009: 1–18) is necessary to get at the political significance of such discourses and practices.

In summary, I have identified three factors in hackers' stance against external requests, a critique whose material residue is the RequestPolicy browser extension. Each is necessary but not sufficient in itself for questioning recuperative processes in technological cycles. First, *technical expertise* allows for breaking the protocols and using the breakdown to establish a critical distance. Second, *historical consciousness* allows for comparing older regimes to upcoming ones and deciding if one is more desirable than the other. Third, *shared values* guide interpretation and legitimize rejection – no doubt informed by the former two. Notably, all three factors are deeply rooted in the gesture of the digital imperative (the perceived necessity to use digital tools), yet running against its oppressive logic of technological determinism.

Discussion: Implications for critique and recuperation

My background narrative contrasted the *critique* articulated in the 1990s by internet users against mainstream media with the *recuperation-implementation* of their demands in the following decades by online media monopolies. Webmasters epitomized the ideal that everybody could build and maintain a website and could help others to do the same (commercially or otherwise). Data flows at this time originated from servers of the actual website. The proliferation of online platforms answered to the same *demand* for many-to-many communications and allowed for a growing population of Internet users to have their own voice.

The trade-off was that users lost control of the actual media through which communication takes place, and consequently the space of self-expression shrunk from websites to ever smaller messages. Today, the majority of data flows originate from and return to the same servers of a select group of platform providers, no matter what website the user puts in the URL bar of the browser. Boltanski and Chiapello conceptualizes this historical process as *implementation-recuperation*: The implementation of demands (many-to-many communications without media concentration) happens in the very same movement that recuperates them (through 'platformization' allowing metadata mining). I argue that platformization shows the critique and recuperation concepts at work in technological cycles over shorter time frames, making them beneficial for STS beyond the study of the epochal dimensions of the *The New Spirit of Capitalism*.

The use of the RequestPolicy browser extension is a gesture of resistance against – or at least defiance of – the historical logic of recuperation. Rejecting the use of external services provided by media monopolies for websites, hackers block data flows from third parties that offer to mediate them as obligatory passage points in the many-to-many communication. In that sense, they enforce the original idea of many-to-many communication in the strict sense, without intermediaries – the very demand articulated as a critique of mainstream media in the early days of the internet. Hence, they reject the recuperated implementation, which provides many-to-many communication, but only as

mediated through platforms (Gillespie, 2010) owned by social media monopolies (Lovink, 2013).

Even if these attempts fail in the larger scheme of things, they preserve both the analytical capabilities – one could say critical faculties – and the sense of agency that Boltanski and Chiapello deem crucial when closing their work with a call for 'sociology against fatalism' (2005: xliv and 529-536). Since accounts of critique and recuperation often err on the side of structural determinism, it is important to point out that the theory has been built to be empowering, and for this reason resistances have to be recognized. Critical technology choices of sophisticated users can fulfil this strategic function in studies of critique and recuperation in technological cycles.

In line with the cyclical fashion of critique and recuperation, resistance to recuperation is itself articulated as critique, whose material residue is the RequestPolicy browser extension. The critique of recuperation itself is best analysed in terms of the definitions given by Boltanski (2009). RequestPolicy automates an immanent critique by exposing the empirical contradiction of the user interface: While the user inputs one address in the address bar, many others are downloaded in the background. Hackers' discussions prompted by RequestPolicy, as additional operations, repeat a transcendent critique by comparing *what is* to to *what was* and therefore *what could be*. The positive meaning of many-to-many communication on the internet has been subverted during its implementation by covertly routing data flows to the same servers of media monopolies, which exploit such many-to-many communication between users for their own benefit.

In the 'old internet', visitor data was either a confidential, private matter between the webmaster and the user, or a public matter showcased on the website in the form of counters and similar gimmicks. Using Boltanski and Chiapello's definition, user data was outside of the commodity sphere – *authentic*. Now user data is a sought-after good with an established market, at the backbone of the most powerful corporations (Wittel, 2012). While implementing the critique against the mass media as one-to-many communication, a parallel process of *commodification* ensued as visitor data acquired market value (Fuchs, 2012). Hackers' material critique embodied in the RequestPolicy software technically prevents the commodification of visitor data. Discursively, it reflects on the inauthenticity of the web page, which is not only providing information to the user but also is collecting and aggregating information about her.

Such technology choices of sophisticated users, especially the element where they reject widely deployed web techniques, have strong affective implications, part of the subjective dimension of engaging with the historical logic of critique and recuperation in technological cycles. While resistance have been shown to result in new technologies, it also is tied to an identity articulated in opposition to contemporary internet-making practices. On the one hand, RequestPolicy generates the anxiety, caused by the loss of authenticity, described by Boltanski and Chiapello – its political-economic implications put such anxiety to work as a negative movement of blocking data flows (and therefore revenue). On the other hand, RequestPolicy is nominally a treatment and protection from the very anxiety caused by data flows of third party requests. The paradoxical affective dynamics around the technological

artefact, coupled with compulsive cycles of breakdown and repetition, are suggestive of a historical trauma.

In the final analysis, hackers' use of RequestPolicy is a *time machine*, which rewinds web history until the bifurcation at which it took a wrong turn – at least according to these sophisticated users. It is a monkey wrench thrown between the wheels of time, bearing an ironic resemblance to the Luddite machine breakers, the irony being that, in order to break some digital machines yet another layer of digital machines has to be implemented. This allows us to reconsider the concept of *reverse engineering* in a novel, historical light. In the case of RequestPolicy, we can see the technological landscape as a roboticized battleground where layers of technology implemented and installed by different social groups struggle for the control over the course of the history of technology. The browser extension is the last outpost of hackers, at the end of the technological pipeline connecting the hives of Google to the minds of users.

References

Arvidsson A and Peitersen N (2013) *The Ethical Economy: Rebuilding Value after the Crisis*. New York: Columbia University Press.

Auerbach D (2013) Tor browser attacked, users should update software immediately. Electronic Frontier Foundation advisory. Available at: https://www.eff.org/deeplinks/2013/08/tor-browser-attacked-users-should-update-software-immediately (accessed 14 August 2017).

Bailey DE and Leonardi PM (2015) *Technology Choices: Why Occupations Differ in their Embrace of New Technology*. Hardcover edition. Cambridge: MIT Press.

Barron A (2013) Free software production as critical social practice. *Economy and Society* 42(4): 597–625.

Bastani A (2011) The communication commons: Resisting the recuperation of the internet by capital. Article in openDemocracyUK., Available at: https://www.opendemocracy.net/ourkingdom/aaron-peters/communication-commons-resisting-recuperation-of-internet-by-capital (accessed 14 August 2017).

Beaulieu A, Scharnhorst A and Wouters P (2007) Not another case study: A middle-range interrogation of ethnographic case studies in the exploration of e-science. *Science, Technology & Human Values* 32(6): 672–692.

Bijker WE and Law J (eds) (1992) *Shaping Technology / Building Society: Studies in Sociotechnical Change*. Cambridge: MIT Press.

Boltanski L (2009) *On Critique: A Sociology of Emancipation*. First edition. Cambridge: Polity Press.

Boltanski L and Chiapello E (2005) *The New Spirit of Capitalism*. New York: Verso.

Casemajor N, Couture S, Delfin M, et al. (2015) Non-participation in digital media. Toward a framework of mediated political action. *Media, Culture & Society* 37(6): 850–866.

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

Davies SR (2017) Characterizing hacking: Mundane engagement in US hacker and makerspaces. *Science, Technology and Human Values* (21 April): 1–27.

Driscoll K (2016) Social media's dial-up ancestor: The bulletin board system. *IEEE Spectrum*, Available at: http://spectrum.ieee.org/computing/networks/social-medias-dialup-ancestor-the-bulletin-board-system (accessed 14 August 2017).

Dunbar-Hester C (2009) Free the spectrum! Activist encounters with old and new media technology. *New Media & Society* 11(1-2): 221–240.

Dunbar-Hester C (2014) *Low Power to the People: Pirates, Protest, and Politics in FM Radio Activism*. Cambridge: MIT Press.

Ellul J (1964) *The Technological Society*. New York: Vintage Books.

Ellul J (1980) *The Technological System*. New York: Continuum.

Ems L (2014) Amish workarounds: Toward a dynamic, contextualized view of technology use. *Journal of Amish and Plain Anabaptist Studies* 1(3): 42–58.

Flyvbjerg B (2006) Five misunderstandings about case-study research. *Qualitative Inquiry*, 12(2): 219–245.

Fuchs C (2012) The political economy of privacy on facebook. *Television & New Media*, 13(2): 139–159.

Gillespie T (2010) The politics of 'platforms'. *New Media & Society* 12(3): 347–364.

Graham P (2004) The word 'hacker'. Blog entry. Available at: http://www.paulgraham.com/gba.html (accessed 14 August 2017).

Hess DJ (2005) Technology- and product-oriented movements: Approximating social movement studies and STS. *Science, Technology and Human Values* 30(4): 515–535.

Ippolita (2015) *In the Facebook Aquarium: The Resistible Rise of Anarcho-Capitalism*. Revised and updated English edition. Institute for Network Cultures, Amsterdam. Available at: http://networkcultures.org/blog/publication/no-15-in-the-facebook-aquarium-the-resistible-rise-of-anarcho-capitalism-ippolita/ (accessed 14 August 2017).

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

Kleif T and Faulkner W (2003) 'I'm no athlete [but] i can make this thing dance!': Men's pleasures in technology. *Science, Technology and Human Values* 28(2): 296–325.

Kline R (2003) Resisting consumer technology in rural america: The telephone and electrification. In: Oudshoorn N and Pinch T (eds) *How Users Matter: The Co-Construction of Users and Technology*. Cambridge: MIT Press, 51–66.

Levy S (1984) *Hackers: Heroes of the Computer Revolution*. Anchor Press, Doubleday.

Lindsay C (2003) From the shadows: Users as designers, producers, marketers, distributors, and technical support. In: Oudshoorn N and Pinch T (eds) *How Users Matter: The Co-Construction of Users and Technology*. Cambridge: MIT Press, 29–50.

Lovink G (2013) A world beyond facebook: Introduction to the unlike us reader. In: Lovink G and Rasch M (eds) *Unlike Us Reader: Social Media Monopolies and their Alternatives*, INC reader #8, Amsterdam: Institute of Network Cultures.

Maxigas (2014a) Cultural stratigraphy: A historical rift in the hacker scene between hacklabs and hackerspaces. *Journal of Peer Production* (5). Available at: http://peerproduction.net/issues/issue-5-shared-machine-shops/editorial-section/cultural-stratigraphy-a-rift-between-shared-machine-shops/ (accessed 14 August 2017).

Maxigas (2014b) The luddite aspects of hackerdom: How to build time machines to alter the course of history. Lecture at Free Software, Free Society conference, Gothenborg, Sweden. Available at: http://slides.metatron.ai/luddite-aspects-of-hackerdom/#/ (accessed 14 August 2017).

Maxigas (2015) Peer production of open hardware: Unfinished artefacts and architectures in the hackerspaces. Doctoral dissertation, Barcelona: Universitat Oberta de Catalunya, Internet Interdisciplinary Institute. Available at: https://relay70.metatron.ai/maxigas_dissertation.pdf (accessed 14 August 2017).

Maxigas (2017) Keeping technological sovereignity: The case of internet relay chat. In: Haché A (ed.) *Technological Sovereignity 2: Case studies*, Dossier ritimo, Paris: Ritimo.

Oudshoorn N and Pinch T (eds) (2003) Introduction. In: *How Users Matter: The Co-Construction of Users and Technology*. Cambridge: MIT Press, 1–25.

Raymond ES (2014) The glider: A universal hacker emblem. Available at: http://www.catb.org/hacker-emblem/ (accessed 14 August 2017).

Sale K (1996) *Rebels Against the Future: The Luddites and Their War on the Industrial Revolution: Lessons for the Computer Age*. New York: Basic Books.

Samuel J (2013) RequestPolicy: Privacy benefits. Available at: https://www.requestpolicy.com/privacy.html (accessed 14 August 2017).

Shirky C (2008) *Here Comes Everybody: The Power of Organizing Without Organizations*. New York: Penguin Press.

Smith A, Fressoli M, Abrol D, et al. (2017) *Grassroots Innovation Movements*. First edition. New York: Routledge.

Söderberg J (2013) Determining social change: The role of technological determinism in the collective action framing of hackers. *New Media & Society* 15(8): 1277–1293.

Söderberg J and Delfanti A (2015) Hacking hacked! The life cycles of digital innovation. *Science, Technology and Human Values* 40(5): 1–6.

Tapscott D and Williams AD (2006) *Wikinomics: How Mass Collaboration Changes Everything*. New York: Penguin.

Thompson EP (1963) *The Making of the English Working Class*. Victor Gollancz.

Turner F (2006) *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. First edition. Chicago: University of Chicago.

Wade NS (2014) Postsubjective simulation and digital culture. Phd Dissertation. UC San Diego, Available at: http://escholarship.org/uc/item/1xh9v315.pdf (accessed 14 August 2017).

Wittel A (2012) Digital Marx: Toward a political economy of distributed media. *TripleC: Cognition, Communication, Co-operation* 10(2): 313–333.

Wyatt S (2008) Challenging the digital imperative: Inaugural lecture. Maastricht University, Available at: https://cris.maastrichtuniversity.nl/portal/files/1570128/guid-10497687-e159-472b-8046-e79dae21baca-ASSET1.0 (accessed 14 August 2017).

Yin RK (2002) *Case Study Research: Design and Methods*. Third edition. Thousand Oaks: Sage.

Author biography

Maxigas is a postdoctoral researcher in the CareNet group at the Internet Interdisciplinary Institute, Universitat Oberta de Catalunya. His current research lines are European Hacking History, the social history and contemporary use of the Internet Relay Chat protocol, and the role of classic cybernetics in shaping computing cultures. See: https://relay70.metatron.ai/