Ecosystems for Innovation: An ethnographic study of Hackerspaces

(working title)

Daniel Angel

December 12, 2013

Contents

1 Introduction

The rise and mass adoption of the Internet as a multimedia tool for communications has allowed humanity to socialise and collaborate in novel ways that would have been unimaginable just a few years ago. Less than a decade after the Internet ceased to be the exclusive domain of University members and a handful of corporations, people from around the world began to communicate in ways that were, before that, seen only as the stuff of science fiction: video conferencing, three-dimensional environments and media convergence enabled millions to interact and come together in creative and often unforeseen ways (Blackman 1998; Syvertsen 2003; Dowding 2001).

Groups of like-minded individuals, until then separated by the tyranny of physical distance, almost spontaneously realised that they could now come together to design, author, produce, compile and share wonderful things: computer software, works of art and even, to paraphrase Wikipedia, "the sum of all human knowledge" —all done remotely from the comfort of everyday people's homes and offices.

Unsurprisingly, interest in these groups grew considerably. Academic journals of varied disciplines began publishing increasing numbers of works on the topic. From a sociological perspective, much of the interest focused on the rise of a new type of "Habermasian" Public Sphere (Dahlberg 2001b; Poster 2001; Gimmler 2001), arguing that the Internet had become (or had the potential to become) a public forum for exchanging ideas, discussing and debating, yet one that required no physical presence. Many scholars (myself included) jumped on this bandwagon, praising *Networked Publics* as well-fit, if not ideal, means (places) for discussion and collaboration (boyd 2008; Ito 2008; Moreira *et al.* 2009; Angel 2009).

In the wake of this revolution, it seemed like physical presence began to be seen as a luxury: it was nice to have, but far from a necessity. Yet there were still numerous voices critical of some of the more triumphant claims of the death of distance. Some argued that, while the Internet presented interesting opportunities for enhancing and complementing physical interaction, it could not completely replace it (Dahlberg 2001b,a; Dahlgren 2005). Others strongly maintained that physical proximity was a key factor in technological development and skills transmission (Howells 2000; Oinas 2000; Morgan 2004). Having been a strong supporter of mediated learning environments, I began to reconsider my position after hearing about Hackerspaces.

I first came across the term *Hackerspace* in 2009, while browsing Boing-Boing[1], an online magazine and blog describing itself as "a directory of wonderful things" where a post, written by one Mitch Altman, read:

[1] See

> If youve never been to a hacker conference or a hacker space [sic], you may wonder what a bunch of hackers would do when they get together. Hackers are a very large group of individuals all around the planet who love learning about technology, making it better, and sharing it with the world (...) Hacker spaces are popping up all over the world. These past 12 months have seen so many renting their own space: Philadelphia, New York City, Kansas City, Toronto, San Francisco, Montreal, DC, Vancouver, Paris, Boston, Providence, Chicago (...) [There are] well over 100 spaces on planet Earth where people can get together and share, learn, and work on the next cool thing (Johnson 2009).

I immediately became curious. These were the same people about whom I was writing for my Master's Thesis: Free/Open Source programmers, hobbyists and enthusiasts. Right before my eyes, they were gathering again, *away* from Networked Publics and back into the real world. But why? Physical co-presence in a common shared space surely presented logistical challenges. First, it required funding, which mostly appeared to come out of members' own pockets. Second, the task of setting up communal spaces had to require a high degree of coordination, management and a significant enough number of interested people. Yet, against what I considered to be tough odds, these spaces were emerging all over the world, at a rate that was hard to keep track of [2].

There is no single or all-encompassing definition as to what a hackerspace is. Hackerspaces.org, perhaps the most comprehensive online resource, defines them as "community-operated physical places, where people can meet and work on their projects" (Hackerspaces.org 2011). Indeed, hackerspaces are diverse and eclectic places. Mitch Altman —who turned out to be an old-school hacker and hackerspace pioneer, founder of the Noisebridge hackerspace in San Francisco commented: "It's not easy to say what a hackerspace is, exactly. *You know it when you're in one*" (Altman 2011).

Wired magazine rightfully compares hackerspaces to the artist collectives of the 1960s and 1970s, "located in rented studios, lofts or semi-commercial spaces, hacker spaces (sic) tend to be loosely organized, governed by consensus, and infused with an almost utopian spirit of cooperation and sharing ...almost a fight club for nerds" (Tweney 2009). In essence, hackerspaces are communities of relatively young people —30 years is the mean (Moilanen 2010), skilled in several activities, mostly having to do with electronics and computer technology (programming languages, hardware hacking, soldering) who come together, under one roof, to *socialise*,

[2] Altman's 2009 estimation of 100 hackerspaces has indeed become obsolete. Hackerspaces.org lists 394 active spaces across the world and many more in "planned" status.

learn and *make things*.

1.1 Ecosystems for Innovation: Relevance of the *Hackerspace* Phenomenon

> *I don't need to remind you of the essence of competition. It's always been quite simple. Any kid working in a garage anywhere in the world with a good idea can put us out of business.*
>
> Gary Winston. From the movie *Antitrust*

In determining whether the phenomenon of hackerspaces is worthy of academic study or simply a passing fad, one has to consider its relevance within a set context as well as its current dimensions. Contextually, hackerspaces present a significant opportunity to understand people's needs for physical contact in a world where such contact is no longer essential for a growing number of activities, to the point of causing the term *decentralisation* to become somewhat of an academic buzzword. Studying hackerspaces will allow for an interesting assessment of the efficacy of online learning in informal environments and how it fares against the traditional physical learning experience while providing insight on hackers' motivations and their need for face-to-face interaction.

Furthermore, their growth rate and presence in all continents certainly suggests that they transcend local cultures and economic boundaries. While still mostly a western phenomenon, hackerspaces have recently emerged in locations as culturally and economically diverse as Yemen, China, Nepal, Mexico and Perú, amongst many others. Interestingly, and despite their wide international expansion, scholarly work involving hackerspaces has been relatively slow to catch up.

In considering hackerspaces' pertinence as study-worthy communities entirely from a sociological perspective, one may overlook their potential for breeding valuable research and technology. It is not difficult to see apparent similarities between hackerspaces and the mythical garages that have come to symbolise the rise of several hi-tech giants. While some writers argue that "garage stories" are nothing more than foundational myths, albeit ones that are encouraged as "pedagogical tools to train and inspire the young" (Kenney 2000, p.239), the tale of genesis in a garage (or dorm room or as a grad project) does suggest increasingly low barriers of entry to an industry where multi-billion dollar corporations can rise in just a few years (Bahrami & Evans 2000). Indeed, several hackerspaces across the world are involved in projects with real scientific and economic potential: Melbourne hackers are backing a serious effort to land a privately-funded rover on the moon (Connected Community 2011) while others have

invented and marketed several successful devices such as the TV-be-gone (Bodzin 2004) and the MakerBot 3D printer (Ginn 2011).

I share Kalish's (2010) view that hackerspaces are community-led ecosystems for learning, research and innovation. Whilst the current body of academic work directly dealing with hackerspaces is scarce, interest is growing fast. As detailed in section [enter refernence], I have come across several papers and study proposals in academic literature. Media interest also seems to be growing swiftly in the form of magazine articles (Tweney 2009; Dougherty 2010), mainstream television news (Ginn 2011) and a documentary currently in production (Bunker 2011). Furthermore, the recent avalanche of attention garnered by *Wikileaks*, has directed attention towards the organisation's hacker origins and the concept of *hacktivism*. Indeed, hackerspaces are at a stage where they *beg* to be the subject of serious and profound academic enquiry.

1.2 Of Hackers and Hackerspaces

Long before the media machineries began associating the word *hacker* with high-tech crime, various groups of well-intentioned, smart and motivated individuals describing each other as hackers played a pivotal role imagining and spawning what people now call the digital revolution. Steven Levy (1984) has traced the origin of the word to the notorious Tech Model Railroad Club —one of the very first groups of computer enthusiasts— at the Massachusetts Institute of Technology. A *hack* was defined by members of the TMRC as "an article or project without constructive end" and "a project undertaken on bad self-advice".

This work is *not* about vandals, "cybercriminals" or, as Clifford Stoll (1989) chooses to call them, "varmints". Instead, it takes an interest in the newer generations of technologically-savvy do-it-yourselfers, heirs to a well-documented tradition of creating, tinkering, making and modifying machines, circuitry, computers and art-inspired artefacts as well as the spaces they have recently begun to occupy: grassroots, independent physical environments in which they meet and socialise, share information and build (sometimes) elegant machines and computer programmes, brought together by a common affinity towards science, technology, politics and the arts.

Partly due to the widespread stereotype of hackers as criminals, it is not widely known that theirs is a culture of institutional origin (Thomas 2002), that stands atop strong philosophical foundations that date back to the late 1950s, influenced by several movements and currents before that. In 1984, Steven Levy coined the term "Hacker Ethic" to describe a pre-existing, yet unwritten compendium of the principles by which hackers abided. These principles revolved around notions of free information and knowledge, inherent apprehension towards authority and the formal establishment and

a then-uncommon enchantment with science and technology. While the basic dogmas of the Hacker Ethic remain in essence to this day, scholars, intellectuals and younger hackers have re-interpreted and elaborated on them, accumulating in the process a vast conceptual and theoretical foundation from which this work benefits.

The advent of hackerspaces, however, seems to signal a turn back to the essence of the original Hacker Ethic. Most notably, a resurgent interest in hardware, re-vitalised in part by dropping costs of materials and widespread availability of instructional material online (Kuznetsov & Paulos 2011). Yet there seems to be more to the hackerspace phenomenon.

The purpose of this work is thus to gain understanding into these relatively new environments and the people who conform them in the hopes of studying how their relationships, interactions and social exchanges contribute to facilitate learning and skills-building within their own habitats and further, to examine how such skills can ultimately lead to potentially significant discoveries and inventions. So far, governments and formal educational institutions seem mostly unaware or uninterested in hackerspaces. It is the intention of this work to shed light on what I hypothesise to be serious incubators for highly skilled and motivated individuals working on potentially ground-breaking innovations.

2 Coming of Age of a Subculture

At first glance, a clear evolutionary link between the hacker subculture and bohemians, as first described in the early 19th Century is dim. In studying the history of Australia's bohemian tradition, Tony Moore (2007) analysed the relationship between 19th Century-style bohemians and the multitude of subcultural and countercultural movements born with the generation of baby boomers, from the late 1950s on. While technologically-minded hackers may be at odds with Roszak's (1969) critique of the state of the society he lived in, which he described as being a harmful, or rather, dulling *technocracy*, many of the bohemian traits identified by Moore seem as compatible with the early MIT hacker ethos as they were with those of the writers, artists and activists that inherited the values and customs of the bohemian legacy. In this chapter I argue that hackers are indeed unlikely heirs of that legacy too. I also analyse how the nuances and cultural traits of their origins manifest in the present, leading to the origin of modern-day hackerspaces.

2.1 Hacker Origins and Philosophy

The tradition of hacking has its origins within a formal academic environment. Indeed, the word "hacker" as a descriptor of the creative, technologically-savvy and computer enthusiasts first became used at the Massachusetts Institute of Technology, where it derived from the older tradition of harmless and ingenious pranks some students devised (and still devise) at the University's campus (Levy 1984)[3].

As a result of the media-fuelled adoption of the term as a synonym for computer criminal, its meaning within academic boundaries is heterogeneous at best and discordant at worst. Some scholars and researchers in the field of information technology and computer security have chosen to follow the media's trend, using the term to allude to malicious cyber-intruders, thus making literature on the subculture that originated at MIT in the late 1950s extremely difficult to distinguish.

In his book *Hacker Culture*, author Douglas Thomas (2002) takes a rather neutral stance on the etymological divergences of the word, choosing instead to focus on the consequences of such divergences: "the very definition of the term 'hacker' is widely and fiercely disputed by both critics and participants in the computer underground". In his view, this "gives a clue to both the significance and the mercurial nature of the subculture itself". Such eclectic positions, however, add an additional layer of complexity to

[3] *Hacking*, in this context, is a wonderful MIT tradition whereby students come up with elaborate jokes that demonstrate their technical prowess as well as their sense of humour. One example of a memorable hack was the placement of a police car on the top of the Institute's *Great Dome*. For a full list of hacks, see .

the task of performing a thorough literature review on *any* of the word's conveyed meanings.

Indeed, the concept of hackers as a collective is filled with almost as many contradictions as the word itself. While it would be easy to place them on the more formal side of Theodore Roszak's (1969) cultural division of the post-war years, as members of a closed inner circle, or, more aptly, a techno-elite, I aim to prove that, in fact, hackers are quite the opposite, having more in common with Roszak's counterculture. Other scholars, such as McKenzie Wark (2004) have gone as far as describing hackers as a digital age Marx-style *proletariat* where "vectiorialists" (capitalists) control and exploit their labour and profit from it.

Steven Levy's *Hackers: Heroes of the Computer Revolution* (1984) is widely recognised as a fundamental, landmark piece of literature when it comes to historically documenting the emergence of the original hackers as an identifiable group and subculture. While not academic in nature, Levy's work can not only be considered an obligatory reference but also a document of historical significance itself, having provided an initial written declaration of philosophical principles, to which he dedicated an entire chapter of his book. Levy coined the term 'The Hacker Ethic' to describe set of undeclared maxims that seemed to have originated in parallel with the movement itself, when early hackers lurked building 26 at MIT, hoping to harness unused, idle time from one of the first (and very primitive) computers ever assembled:

> "...the dozen or so hackers were reluctant to acknowledge that their tiny society, on intimate terms with [the computer], had been slowly and implicitly piecing together a body of concepts, beliefs and mores.
>
> The precepts of this revolutionary Hacker Ethic were not so much debated as silently agreed upon. No manifestos were issued. No missionaries tried to gather converts."

If not the first, Levy was certainly amongst the earliest theorists who saw the necessity to explicitly declare those "concepts, beliefs and mores", *The Hacker Ethic*, consisting of six precepts:

1. Access to computers —and anything which might teach you something about the way the world works— should be unlimited and total. Always yield to the Hands-On Imperative!
2. All information should be free
3. Mistrust Authority - Promote Decentralization
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position

5. You can create art and beauty in a computer

6. Computers can change your life for the better

Inherent in such principles were ideas of freedom of information, contempt for the establishment and technological determinism. I suggest that the Hacker Ethic provides a clear, coherent basis upon which to perform an analytical dissection of the emergence of the hacker movement. Precepts 1 and 2 summarise the movement's views on issues of freedom, with an emphasis on information as well as their opposition to restrictions imposed by copyright and patent law.

Hackers were born within —and still share close ties to— academia. Across the world, universities still foster and cherish the sharing of information. Gift economies are prevalent amongst academics, who continually build upon each other's work and who, just like those first hackers, are flattered —not threatened— to see others use and expand their own work.

Precepts 3 to 5 present an interesting perspective on Hackers' worldviews, particularly when it comes to their relation with the wider spectrum of society. By making a personal interpretation of these three principles, I conclude that today's Hackers are heirs to the wider bohemian tradition that begun in Europe during the 19th Century and subsequently evolved into the 1960s and 1970s countercultural movements, with which they shared similar views, tastes and political ideas.

Lastly, I judge the sixth precept to represent a growing trend towards technological determinism, reflective of the growing view that human and social development are closely tied to the advance of technology.

2.2 Heirs of the Bohemian Tradition

2.2.1 One Counterculture, Many Subcultures

In 1969, Theodore Roszak described the growing rebelliousness of the baby boomer generation as a *counter-culture*: "a culture so radically disaffiliated from the mainstream assumptions of our society that it scarcely looks to many as a culture at all, but takes on the alarming appearance of a barbaric intrusion". Such disaffiliation was certainly not new: 19th Century bohemians (and others before them) already held many of the social grievances described by Roszac. It was, however, the sheer scale of the new movements —strengthened in numbers by the offspring of couples formed in the post-war years— that made the 1960s manifestations particularly powerful, even if, in reality, most of those movements were heterogeneous in nature.

As argued by various scholars (McGregor 1975; Spates 1976; Eder 1990), a single, uniform counterculture as proposed by Roszak was nothing more than a gross generalisation. Hebdige (1987, p.148) further argued that the

term came to represent an "amalgam of 'alternative' middle-class youth cultures" in macro-political opposition to what has been called the "the establishment", "straight society" or simply, "the mainstream". Yet others, like Marchant (2003, p.87–88) have criticised this view as over simplifying.

In this context, I take a practical approach and view individual movements as different, specific subcultures, all of which are enclaved in a countercultural social scope. Therefore, as eclectic as such groups were, opposition (whether backed by micro or macro-political action) was indeed their strongest bond. In this sense, hackers, bohemians, students and hippies were no different. As will be argued, such disdain for established traditions, authorities and the prevailing social order offered them empowerment yet came with a sense of irony, as many of the movements (hackers included) were born either inside or as a result of established institutions. Hackers' genesis, for instance, took place inside universities and in many cases with the financial and technical support of much-loathed institutions like the U.S. Department of Defence.

2.2.2 Contempt for the Establishment

Despite this element of irony, denial of established values, institutions and customs became the driving force for the self-identification of all movements of the time. In his Doctoral Thesis, Tony Moore examined the cultural *status quo* that bohemians before them both challenged and benefited from:

> ...bohemians performed publicly an imagined or hoped for personal autonomy from art markets that involved style, behaviour, art, social formations and even politics that transgressed and subverted, *but never overturned*, bourgeois society (Moore 2007, p.10). [emphasis added]

By publicly expressing contempt for that society and positioning themselves as social outsiders, such characters —who had long before acquired a sense of group identity— managed to leverage a sense of "forbidden fascination" exerted in the wider social strata by means of "coded fashion and recreation that could be read by the initiated" (Moore 2007, p.17). Upon the dawn of the 1960s movements, such codes were further disseminated and strengthened by the powerful effects of the mass media.

As political awareness increasingly grew amongst many subcultural movements, condemnation of mainstream values became not only more outspoken but action-driven, shifting from a rather tolerant acceptance of the prevailing *status-quo* towards a more politicised resistance that culminated in the protests of May of 1968 in France, the violent, anti-Vietnam intervention demonstrations in university campuses across North America

and the radicalisation of many movements across Latin America, where the very real possibility of the overturning of bourgeois society spurred revolutions and dictatorships whose consequences are felt to this day.

Drawing parallels between these events and the emergence of hackerism is not a simple task —one not made any less complicated by the fact that the amount of scholarly works on the subject is rather modest, particularly when compared to other movements of the time. The limited amount of resources available nevertheless sheds some light on the issue of hackers' analogous disdain for established orders. Levy (1984), for instance, provided a sound starting point with his Hacker Ethic. The third maxim, "Mistrust authority. Promote decentralization", sheds extra light on the link between hackers and the wider countercultural spectrum.

This link becomes clearer by examining the history of the dawn of hackers, whose rhetoric, like that of many other movements of the time, became increasingly politicised during the 1960s and 1970s. Hackers imagined a world "where computers would lead the way to a new, liberating lifestyle" (Levy 1984, p.168). Much like other movements, they envisioned a way out of the social constraints of society, yet did so in their own, unique way, believing computers to be the main vehicle with which to achieve this.

In addition, *Hackers* bluntly documents behaviour that is quite contrary to Roszak's concept of "technocracy". MIT hackers, Levy argued strongly, held passionate and vocal disdain for Weber-style bureaucracy. The focus of such disdain was inevitably embodied by International Business Machines (IBM) —the devil they knew best, and later by countless more companies as well as the corporate culture they seemed to represent. In describing hackers' loathing for IBM types, Levy commented:

> All you had to do was look at someone in the IBM world, and note the button-down white shirt, the neatly pinned black tie, the hair carefully held in place, and the tray of punchcards in hand. (Levy 1984, p.42)

Interestingly, this exact same stereotype is referenced by Roszak in his book. Upon discussing the nature of "grown-upness" he describes countercultural youth as having "better ideas than GM or IBM seem able to offer", describing them as a "scruffy, uncouth, and often half-mad lot" (Roszak 1969, p.32). Hackers' choice of clothes and odd sense of style thus followed a conscious effort to distance themselves from the formality of the corporate environment, embodied by the stereotype of the IBM employee, in the same sense as hippies and others rebelled themselves by opposing the idiosyncrasies and fashions of 1950s suburban America (Heath & Potter 2005, p.34). Their anti-establishment sentiments differed, however, in one fundamental way when compared to those of other subcultural groups of the time: their inherent motivations.

Beats, hippies and even anti-war protesters' unease seemed to stem from evolving views on Marxist and Freudian theories. Countercultural interpretations of Freud saw culture, or rather, civilisation as a sort of straitjacket constraining individuality and freedom (Heath & Potter 2005). Hackers instead viewed individual freedom as achievable *through* the more pressing matter of freedom of information. Thus, just as individuality was crucial for the development of group identity and sense of belonging in the case of the former, freedom of information became hackers' foremost foundational dogma. In practice, no single subculture would have thrived in its absence.

2.2.3 The Criminal and the Carnivalesque

Hackers are curious by nature. They satisfy their curiosity by engaging in acts of discovery, whether that means solving a problem or deciphering the inner workings of a machine or network. While, every so often, a hacker may break the law, there seems to be a wide mis-representation of hackers —true hackers— as criminals. This negative connotation has its origins some time in the 1980s. Richard Stallman (2002b) explains:

> ...when I say I am a hacker, people often think I am making a naughty admission, presenting myself specifically as a security breaker. How did this confusion develop?
>
> Around 1980, when the news media took notice of hackers, they fixated on one narrow aspect of real hacking: the security breaking which some hackers occasionally did. They ignored all the rest of hacking, and took the term to mean breaking security, no more and no less. The media have since spread that definition, disregarding our attempts to correct them. As a result, most people have a mistaken idea of what we hackers actually do and what we think.

While the media may have been responsible for spreading the negative connotation, validation for the practice seems to have been the result of the publishing of three landmark books about computer criminals (Thomas 2002, p.xiii). Katie Hafner and John Markoff's *Cyberpunk* (1991), William Gibson's iconic novel, *Neuromancer* (1984) and Clifford Stoll's *The Cuckoo's Egg* (1989). All three books referred to their characters as "hackers", making little effort to draw a clear semantic distinction between their respective characters (real and fictional) and the wider hacker subculture.

Stoll, a scholar, mathematician and astrophysicist, proficient in several computer languages and technologies was aware of the emerging trend and the irritation it caused amongst self-confessed hackers, yet chose to

follow it. "A computer wizard?", he asked sarcastically at the beginning of his book. "Not me —I'm an astronomer" (Stoll 1989, p. 1).

Perhaps as a wilful effort to appease the outcry, Stoll justified his decision with an apologetic opening paragraph:

> What word describes someone who breaks into computers? Old style software wizards are proud to be called hackers and resent the scofflaws who have appropriated the word. On the networks, wizards refer to these hoodlums of our electronic age as "crackers" or "cyberpunks". In the Netherlands, there's the term "computervredebreuk" —literally, computer peace disturbance. Me? The idea of a vandal breaking into my computer system makes me think of words like "varmint", "reprobate" and "swine". (Stoll 1989, p.11)

Throughout his book, Steven Levy provides a detailed rationale for hackers' contempt for security, arguing that it lied not in a desire to break the law, steal or cause mayhem, but rather as a result of common beliefs about the free flow of information and its benefits. Richard Stallman articulately summarised this mantra:

> Hackers typically had little respect for the silly rules that administrators like to impose, so they looked for ways around. For instance, when computers at MIT started to have "security" (that is, restrictions on what users could do), some hackers found clever ways to bypass the security, partly so they could use the computers freely, and partly just for the sake of cleverness (hacking does not need to be useful). (...)
>
> In the hacker's paradise, the glory days of the Artificial Intelligence Lab, there was no security breaking, because there was no security to break.

To those original hackers, some intrusions were not only morally justified, they were necessary. Their motivations were driven by the satisfaction of a legitimate thirst for knowledge. None of the original hackers would have considered exploiting systems for profit or malice: their goal was to eliminate "the odious concept of passwords", arguing that systems —and the underlying technology behind them— belonged "not to the author but to all users of the machine" (Levy 1984, p.127), echoing a socialist rhetoric.

Early bohemians suffered from the same predicaments, albeit on a different scale and with notably different consequences. Marx, argues Tony Moore, used the term "*le bohème*" to refer to a "vagabond character, with a strong connotation of poverty and even criminality". To some degree, Marx mis-understood the bohemian ideology and lifestyle.

Yet, it seems that, in some cases, notions of criminality were at least partly self-imposed: vehicles for "acting out" a part that would wilfully separate them and their prospects from "more conventional artists" (Moore 2007, p.30). By engaging in *carnivalesque* practices that would go on to become collective rituals, bohemians embraced the power that came out of their cultural transformation. Many of these rituals and attitudes also became suitable targets for media speculation, resulting in simplified and often imprecise portrayals, which, as with hackers, lead to the formation of simple stereotypes.

This process also facilitated mechanisms of cultural "co-optation", by which images, accessories and garments were stripped of their cultural significance to be sold for profit (Heath & Potter 2005). Subcultural movements from the 1960s and 1970s hence unwillingly facilitated the massification of a consumer culture that borrowed and appropriated whatever could be marketable about them.

Early hackerism lacked the histrionic sophistication required to engage in carnivalesque displays. Driven by more pragmatic principles, the hacker subculture saw no benefit from the acquisition of symbolic capital beyond the boundaries of its own, narrow field of interest. Hackers did not wish to spread their ideas by "converting" anyone, nor did they aspire for recognition beyond their small circles of peers. All this led to their characterisation as reticent, isolated and non-social. The Jargon File[4], written in the third person, presents a view that seems to be diametrically opposed to images of flamboyant bohemians and artists:

> Hackers have relatively little ability to identify emotionally with other people. This may be because hackers generally aren't much like 'other people'. Unsurprisingly, hackers also tend towards self-absorption, intellectual arrogance, and impatience with people and tasks perceived to be wasting their time. (Raymond & Steele 1993, p.743)

From this perspective, it is hard to equate hackers with sexually liberated, free-loving hippies, descendants of the dandies or flâneurs of yesteryear. Yet, things have changed. In spite of this apparent contradiction, the

[4]The *Jargon File* is another landmark document in hacker history. The multi-authored text file was first started some time in the late 1970s. Originally conceived as a sort of dictionary to describe hacker slang, the Jargon File became a living document —a historical account of the movement, written by hackers themselves. While difficult to cite and interpret because of its many authors and versions, the Jargon File does have historical value as a witness to the birth of the movement. A polished, organised and citable version of the file was originally published as a book in 1983 by Guy Steele and re-published in the early 1990s by Eric S. Raymond. The file (and by extension, the book) provides a window to early hacker culture as seen by themselves. In that sense, it is a priceless historical resource. In this work, the Jargon File shall refer to Steele's and Raymond's *The new hacker's dictionary* (1993).

hacker subculture has greatly evolved in recent years. The result has led to a shift media portrayals and a more benevolent general perception, albeit under the more general and vague "geek" label.

2.2.4 Revenge of the Nerds: A Tale of Co-optation

As the meaning of the word *hacker* shifted as a result of the influence of the mass media (Kinney 1993), the original nuances associated with it tended to shift towards other words, more vague in definition and, initially, charged with a high negative overtone, namely "nerd" and "geek". Steven Levy noticed this shift upon re-visiting his book in 2010:

> The kind of hacker I wrote about was motivated by the desire to learn and build, not steal and destroy. On the positive side of the ledger, this friendly hacker type has also become a cultural icon —the fuzzy, genial whiz kid who wields a keyboard to get Jack Bauer out of a jam, or the brainy billionaire in a T-shirt— even if today he's more likely to be called a geek. (Levy 2010)

It can be argued that, today, the essential meaning of all three words, "hacker", "nerd" and "geek" is closely intertwined, much like a Venn diagram, where large areas of each seamlessly intersect. Yet, nuances and applications give each a unique set of values that ultimately convey similar but particular concepts, having co-evolved during the past three decades. Kendall (1999) notes that "Nerd" became a relatively common term in "TV shows about teens" since at least the mid-1970s, yet, it was only during the mid-1980s when it came to describe people "overly involved with, and skilled in the use of computers". This is precisely the time when the original meaning of the word "hacker" began to shift.

Similarly, Kendall notes the relative closeness of "geek" and "nerd", while noting that the former has a much less negative connotation. To make her point, Kendall cites a character Douglas Coupland's novel, *Microserfs* (1995), who provides an interesting view of the differences between the two: "geek implies hireability, whereas nerd doesn't necessarily mean your skills are 100 percent sellable. Geek implies wealth". To the uninitiated, however, the two differ starkly from "hacker".

Writers of the Jargon File, on the other hand, were quite aware of the nuances and subtleties with regard to the meaning of each of the three words, as well as their points of intersection, as demonstrated by the following quote:

> ...many hackers have difficulties maintaining stable relationships. At worst, they can produce the classic geek: withdrawn, relationally incompetent, sexually frustrated, and desperately unhappy when not submerged in his or her craft. Fortunately,

> this extreme is far less common than mainstream folklore paints it but almost all hackers will recognize something of themselves in [the stereotype] (Raymond & Steele 1993, p.744).

In recent years, however, the *geek* label has become an interesting example of linguistic and social reclamation, one that has come to be a source of pride and, increasingly, even "coolness", in a way that is analogous to what happened with other pejorative terms and the collectivities they described, such as "queer" and "gay" in the case of homosexuals (Brontsema 2004).

Building upon Bourdieu's concept of *cultural capital*, Sarah Thornton (1996) coined the term *subcultural capital*, defining it as the "hipness" that operates outside Bourdieu's main *fields*, but that rather thrives within "less privileged domains" (Thornton 1996, p. 11–14). The author argued that, while not as easily convertible into other forms of capital (economic, for instance[5]) and unbound by class, subcultural capital is gained from performing selective consumption and engaging in media appropriation, particularly amongst younger people. The growing (but still niche) market that has risen for goods that link their consumers with the geek label ("geek cred") in the form of cryptic messages and references only interpretable by a selected few (Tocci 2007), is a prime example of this trend.

While still in its infancy, such development is no different from the commercial frenzy that followed cultural appropriation processes stemming from countercultural movements of the 1960s and 1970s, resulting in fruitful commercial endeavours. According to Moore (2007, p.91), a "loyal countercultural market" was swiftly exploited by savvy entrepreneurs who understood that the image they projected —one of individualism and authenticity— had tremendous commercial potential. Heath & Potter (2005) suggest that, following such processes of commercial co-optation, the core principles of these movements were overshadowed by their aesthetics:

> ...the hipster, cooling his heels in a jazz club, comes to be seen as a more profound critic of modern society than the civil rights activist working to enlist voters or the feminist politician campaigning for a constitutional amendment (Heath & Potter 2005, p.32).

The *faux* link between countercultures, they argued, along with Freud's concept of *eros* and "the revolution" became extremely beneficial for marketers and capitalists of all shapes and sizes, all eager to benefit from whatever was considered to be in opposition to the so-called mainstream.

The trend was predictably reflected in the media. The Broadway musical *Hair* became a massive success when brought to Sydney in 1969, benefiting from the society-wide appeal with the lure of the *hippie* ideology of sex,

[5]Thornton does provide examples in which her subcultural capital as the *hipness* factor, can be converted into economic capital such as the case of DJs or fashion designers.

drugs, music *and* social revolution (Moore 2007, p.104). Likewise, today's "geek-oriented" audiovisual works generate enormous amounts of interest. Situation comedies such as *The Big Bang Theory* in the United States and *The I.T Crowd* in the United Kingdom became commercial hits (Rodman 2009; Smith 2006).

The "geek chic" phenomenon thus seems to be experiencing the same kind of co-optation processes by means of intervention by the entertainment industrial muscle, while the subcultural values remain alive online and in small groups such as those created by hackerspaces. Having a strong record of participation online separates the wannabes from the real hackers or geeks (Tocci 2007). Indeed, an active Reddit[6] or Github[7] account can be seen as a "personal badge of pride". Furthermore, political involvement seems to have risen recently. Not-for-profit initiatives such as *Civic Commons*[8] —a group that aims to help governments by achieving efficiency and transparency through IT infrastructures, is one of many examples of this trend.

2.2.5 Hackers and Capitalism

Hackers have traditionally held little contempt for capitalism itself. Rather, their disdain is directed towards certain practices that are common (but not necessary) within the system, namely excessive bureaucracy and restriction of access to information. Perhaps as a result of his depiction of hackers' unorganised beginnings, Steven Levy has failed to make this distinction, suggesting —inaccurately— a general incompatibility between the original principles of hackerism and capitalist practices. Indeed, hackers have historically dealt with capitalism in a manner not unlike that with which they treat other aspects of their life: by applying creativity and lawful subversion[9] and achieving unexpected results.

It is only when commercial practices become at odds with The Hacker Ethic that clashes or ideological conflicts between the two worlds arise. Richard Stallman, intellectual leader of the movement and known for his reluctance towards even the slightest compromise, best summed it up by declaring that "redistributing free software is a good and legitimate activity; if you do it, you might as well make a profit from it" (Stallman 2002a, p. 65).

Stallman's statement reveals the *hack* on capitalism, as it applies to software: by allowing freely-distributable programs to openly compete against

[6] See

[7] See

[8] See

[9] I use this oxymoronic term deliberately to emphasise the contradiction many subcultures experience in regards to their political stance and rhetoric as described throughout this chapter.

proprietary ones, hackers have forced software companies to either join the trend, leverage their existing market shares by locking in customers (Lee & Mendelson 2008) or come up with alternative revenue strategies. Ever pragmatists, such is the way hackers exercise defiance: by abiding and subverting creatively within the boundaries of the law: practising hands-on evolution rather than revolution.

Levy's failure to recognise this fact is surprising, given that *Hackers* constantly hints at it. One can read, for instance, how hackers' attitudes towards IBM deeply contrasted those towards another corporation, DEC (Digital Equipment Corporation), for which they held a sense of admiration, perceiving it as being less laden with bureaucracy, more efficient and even worthy of admiration, to the point where some of the original MIT members sought and found paid positions within it.

Needless to say, much has happened since the 1984 release of the book. Its recent 25th anniversary was celebrated with an article in Wired Magazine (that later became an addendum to the new edition) in which Levy re-visited many of his subjects, while also introducing new, younger characters, portrayed as part of an ongoing generational shift. In his article, Levy acknowledges that new hackers have assumed a less bellicose position towards businesses, but still fails to specify the source of the initial opposition —*some practices* as opposed to the system itself:

> . . . hacking's values [today] aren't threatened by business —they have conquered business. Seat-of-the-pants problem-solving. Decentralized decisionmaking. Emphasizing quality of work over quality of wardrobe. These are all hacker ideals, and they have all infiltrated the working world (Levy 2010).

The "hacker ideals" Levy speaks about have never been in conflict with the "working world". Indeed, some of his initial subjects went on to found and lead multi-billion dollar corporations, while many others tried but failed to achieve the same goal —a quarter of a century earlier.

This unacknowledged communion, however, has not meant complete assimilation or passive acceptance. In a fashion not unlike that of other movements of the 1960s and early 1970s, hackers have indeed been known for expressing frustration towards peers whom they perceive as having "sold out" or become "corrupted". Tony Moore argues that countercultural contempt for the establishment has not traditionally been filled with true revolutionary sentiments, since the very existence of well-established institutions is essential as reference parameter from which to rebel against. Without a manifest presence of such institutions there can be no rebelliousness. To hackers, The Man does not necessarily mean The Business or The Government by itself. Instead, it is the *over-bureaucratic* business or the *secretive* government agency. Thus, the "sell-outs", in hackers' eyes, are those

who associate themselves with institutions seen as contrary to the Hacker Ethic, itself not immune to the passage of time.

2.2.6 Nostalgia

As the Hacker Ethic slowly evolves and reshapes itself, so do hackers' group identities. This includes natural and somewhat expected manifestations of denial from the part of older members, who often fail to recognise younger ones as genuine representatives of their group. Inherent in this progression of constant adoption, evolution and denial may be a process of mythification as theorised by Lave & Wenger (1991), who argue that generational shifts amongst communities often tend to spur criticism in the form of nostalgic complaint regarding newcomers' corruption of the original ideals. From this perspective, accusations from the ranks of original or older Hackers towards younger ones in terms of "selling out" should come as no surprise and instead be seen as a predictable pattern consistent not only with other coeval groups but historically with almost any collectivity.

By the year 1984, when Steven Levy released *Hackers*, at least three major generational shifts had taken place amongst the ranks of the hackers at MIT and California, while many other groups had begun forming around the world. The unique character of Levy's book lies in the fact that it served both as an initial manifesto and as a way to preserve and spread what had been to that point a mostly oral tradition, thus helping perpetuate the original mythology.

As an epilogue to *Hackers*, Levy documented the story of Richard Stallman, "the last of the true hackers", a man so committed to the movement and its ideals that he dedicated his entire life to —quite literally— spreading its gospel[10]. Stallman grew dissatisfied with what he described as "the decay of the Hacker Ethic" (Levy 1984, p.415). Where his peers (and elders) moved on from true hackerism to join bureaucratic and tight organisations, he remained (and still remains) unmoved in his convictions and ideals.

Stallman is best known for his perseverance, relentlessness and for authoring the *GNU GPL* —the widely-used free software license. As a result, he has become both a source of inspiration and aversion (on account of his perceived intransigence and zeal) amongst those close to the movement, in the process achieving the status of a mythical "founding father" (Jackson 1998). While his case shares many characteristics with the processes of mythification from other subcultures, Stallman's is unique in a number of ways. He is, no doubt, the last *active* representative of the original MIT faction that started the hacker subculture, even if his activities these days have more to do with preaching than with hands-on software hacking.

[10]Stallman is known for parodying traditional religious rituals and icons, jokingly dressing up as *Saint iGNUtius* (using a large robe and an old disk drive platter as a halo), whom, he proclaims, is the leader of *The Church of EMACS*. See .

Seen from a wider perspective, Stallman's merit lies in his capacity to convert his own nostalgia into a constant and permanent driving force for activism. In *Hackers* as well as in its new addendum, Levy portrays Stallman as someone filled with nostalgia and angst: "(his) eyes moistened as he described the decay of the Hacker Ethic" (Levy 1984, p.415) and even some suicidal tendencies. He has been quoted to say:

> I have certainly wished I had killed myself when I was born. In terms of effect on the world, it's very good that I've lived. And so I guess, if I could go back in time and prevent my birth, I wouldn't do it. But I sure wish I hadn't had so much pain. (Levy 2010)

Through his quote, Stallman also candidly acknowledges his labour as a leader of the movement. Indeed, it is not few would deny that his efforts have been a necessary cause in ensuring the continuity of the lifestyle and principles developed in the early days of the MIT Railroad club. "What happened to the hackers of yesteryear?", Levy asked himself. "Many had gone to work for businesses, implicitly accepting the compromises that such work entailed"[11]. Contrastingly, Stallman has never ceased to see himself as the enforcer of a messianic mission to preserve and expand his own interpretation of the Hacker Ethic.

2.3 Freedom of Information, Freedom of Software

The hacker subculture's country of origin has deep implications when it comes to their views on freedom of information. Prior to the Copyright Act of 1976, the United States held an undeclared tradition of disdain towards restrictions on the use of information. Its democratic foundations have, for centuries, equated access to information to accountability and good government. Furthermore, as a result of its revolutionary origins, the government explicitly encouraged copyright violations for works coming from abroad. According to Khan (2006), the country's first copyright act declared that 'nothing in this act shall be construed to extend to prohibit the importation or vending, reprinting or publishing within the United States, of any map, chart, book or books ...by any person not a citizen of the United States'.

Today, the situation is clearly quite different. The United States went from being a net importer of cultural works to being perhaps their largest exporter. This, combined with the decline of manufacturing in developed nations has led to increasing zeal over the control of cultural material, regardless of the format, resulting in increasing restrictions in terms of its

[11] As I have argued earlier, I believe "working for businesses" does not necessarily imply a compromise on the part of hackers.

distribution and flow, and achieving an effect of artificial scarcity and commodification. Ideas, along with cultural works, are perceived as sources of tangible monetary value and competitive advantages that are to be carefully controlled and prudently rationed.

The implications of cultural commodification beyond their effects on hackers are perhaps beyond the scope of this work, yet increasing restrictions applied to cultural and creative works have undoubtedly had tangible consequences on society as a whole.

For hackers, however, the free flow of information constitutes a necessary cause. In his book, *A Hacker Manifesto*, McKenzie Wark (2004) describes this situation as the motive force for this century's class struggle, in his opinion being waged by "manufacturers" of cultural works —hackers— and the beneficiaries of their production (or rather, commercialisation), referred to as vectorialists. On cultural commodification, Wark argues that 'commodified life dispossess the worker of the information traditionally passed on outside the realm of private property as culture' (Wark 2004, v. 28), drawing clear parallels to Marx's workers' struggle, yet not about means of production, but rather, 'freeing information from its material constraints' (Wark 2004, v.4).

Wark's analysis —while extremely enlightening— falls short on account of its abstraction. To fully understand the issue of freedom of information in the context of the origins of hackerism, one finds more concrete precedents by turning, again, to Steven Levy's book. As Levy (Levy 1984, p.5) recalls, the movement itself was born out of contempt for the "priest-like" figures who sought to monopolise and restrict the use of computer resources[12]. As outsiders, the very first Hackers were denied the possibility of using and studying the powerful new machines, having to resort to clandestine tactics to sneak inside the buildings late at night to gain access to the room-sized contraptions.

As it flourished, hackerism embraced the mantra of free-flowing information, building its own young subculture on top of it. The Artificial Intelligence Laboratory at MIT became the unofficial headquarters of the group, a place where constant cooperative competition, respectful acknowledgement of others' achievements and a mentality of studying and building upon what existed became a non-negotiable norm.

Yet, as personal computers became more and more popular, the trend began to be reversed. By the time Steward Brand famously coined the phrase *Information Wants to be Free* in 1984 (Wagner 2003), the computer revolution was in full swing. Apple had led the massification of personal computers and was already a multi-million-dollar company, while IBM and others attempted to catch up with varying degrees of success. As a result,

[12]Use of the word "priest" draws an implicit parallel between ancient means of control through literacy and today, through The Computer.

software became a priced asset —one that had to be guarded by means of withholding its source.

Pressure to preserve increasingly large amounts of software as trade secrets reached even the sacred confines of the Artificial Intelligence Lab, where many, headed by the relentless Stallman, refused to give in to the trend, becoming, in the process, some of its most vocal critics. Stallman's 1985 *GNU Manifesto* became not only a declaration of principles:

> I consider that the golden rule requires that if I like a program I must share it with other people who like it. ...I refuse to break solidarity with other users in this way. I cannot in good conscience sign a non-disclosure agreement or a software license agreement.

But also a call to arms amongst hackers to fight those restrictions the way they knew how to:

> GNU, which stands for Gnu's Not Unix, is the name for the complete Unix-compatible software system which I am writing so that I can give it away free to everyone who can use it. Several other volunteers are helping me. ...So that I can continue to use computers without dishonor, I have decided to put together a sufficient body of free software so that I will be able to get along without any software that is not free.

The document described his vision of a world where sharing information was to be considered an act of neighbourly kindness rather than a crime. It also presented a detailed outline of his strategy, which began with his pledge to write GNU, a free replacement to Unix[13], from the ground up —a monumental task— along with his resolution to resign from the Artificial Intelligence Laboratory at MIT in order to avoid 'any legal excuse to prevent me from giving GNU away' (Stallman 1985).

While the essence of the GNU Manifesto remains current to this day, Stallman's philosophical and strategic plans have grown and matured. Today, he is considered a pioneer and the father of *free software*[14], not only due to his initiative to write GNU but also, to a great degree, for having authored the immensely popular *GPL*, or GNU General Public License, the first *copyleft* software license. Known for being a clever *hack* on copyright

[13]Unix was, back then, the prevailing operating system. With the advent of GNU/Linux and Mac OS X, Unix, or rather Unix-like systems, have become immensely relevant once again.

[14]Whilst, in practice, *free software* and *open-source software* may be used interchangeably, the former is usually associated with those whose concerns are more philosophical, like Stallman, while the latter is used by advocates who see more practical benefits to its use.

law, the GPL uses the restrictions copyright grants on works such as software to ensure that its terms, which mandate any derivative works to remain open, are upheld and respected.

Within the *Jargon File* (Raymond & Steele 1993, p.334), the case for information openness is argued in the entry that references the Hacker Ethic: 'it is an ethical duty of hackers to share their expertise by writing open-source and facilitating access to information and to computing resources wherever possible'. While the presence of the term *open-source* can lead the reader to conclude that this was a rather late addition to the file[15], it serves as evidence to the fact that the ethos has remained unchanged to this day, and throughout the history of the subculture, despite claims, such as Levy's own recent commentary to his own text, that hacker values no longer centre around freedom of information but solely on the desire for tinkering and exploring (Levy 2010).

As mentioned earlier, the GPL is perhaps the first example of this trend, which can be considered one of the pillars of the movement known today as *copyleft*. As a system for countering what is perceived to be an excessively and increasingly restrictive copyright law, copyleft confronts these restrictions *from within*, by imposing limits to *lack* of openness, disclosure and sharing to works that are licensed by any one of the many flavours of licenses available to choose from.

Young hackers who today remain faithful to the essence of the Hacker Ethic regard never-ending pressure for increasing restrictions on the flow of information much with the same eyes, something to be not only opposed to and protested but also, "subverted" and "transgressed".

2.4 Hackers and Education: It's Complicated

By virtue of their very origins, hackers have an interestingly contradictory stance when it comes to formal education. As has been argued earlier, their very genesis is the product of a University environment, yet it came to be as a defiance of traditional structures. Brian Harvey (1986) elaborates on the etymology of the word, as it originated and evolved in the 1950s and 60s, whilst pointing out an interesting contrast:

> Popular opinion at MIT posited that there are two kinds of students, tools and hackers. A "tool" is someone who attends class regularly, is always to be found in the library when no class is meeting, and gets straight As. A "hacker" is the opposite: someone who never goes to class, who in fact sleeps all day, and who spends the night pursuing *recreational activities* rather than studying. (emphasis added)

[15]The term 'open source' was coined in 1998. See Open Source Initiative (2012)

It is the very nature of hackers' recreational activities that leads to their learning experiences. Hackers will not follow the path of least resistance, which, in their case, represents the traditional go-to-class, do-your-homework mantra of the classic academic model, but will, in contrast, be mostly driven by large amounts of intellectual curiosity, which in turn is a source of pleasure. This abundant source of intrinsic motivation creates a number of both benefits and challenges.

Benefits, whilst seemingly clear, deserve mention. Hungarian psychologist Mihaly Csikszentmihalyi famously correlated enjoyment of an activity to increased concentration and ability through what he described as a state of "flow" (Csikszentmihalyi 1975). Flow is achieved when an individual's skills are appropriate for the task at hand, but are met with a certain amount of challenge, itself a pathway to discovery and learning. Flow, thus, requires the use of individuals' skills to the point where their activities are performed "naturally", without conscious inner reflection, resulting in increased performance and faster learning curves. Hackers have noticed this phenomenon, in their own way, and named it accordingly. The Jargon File elaborates:

> **Hack mode**: a Zenlike state of total focus on The Problem that may be achieved when one is hacking (this is why every good hacker is part mystic). Ability to enter such concentration at will correlates strongly with wizardliness (Raymond & Steele 1993, p.331)

Lakhani & Wolf (2003) have further proposed that curiosity-driven hackers can also become more creative. Basing their argument on the work of Amabile (1996), they suggest curiosity leads to *heuristic* approaches to problem solving in hackers, in opposition to otherwise *algorithmic* resolutions. As an example, the authors point to the development of a printer driver —a task not easily perceivable as *creative* by someone not connected to the project. Yet, anyone who is directly involved with the challenge can appreciate the creative effort that goes into it. Levy (1984, pp.13–33) argues that hackers apply most of their creativity in the process known as "program bumming"[16]. Indeed, he goes as as far as describing program bumming as "artful", in concordance to principle five of *The Hacker Ethic*, "You can create art and beauty in a computer".

In spite of these benefits, however, aversion for established curricula comes at a price. Hackers' engagement in a project or activity can quickly fade if they find something more interesting to devote their attention to. Whilst, as discussed, their focus and concentration may be abundant, their

[16]To "bum" a program is to reduce it to the absolute fewest number of lines without affecting its outcome.

commitment may not necessarily match the trend. In his landmark essay *The Cathedral and the Bazaar*, Raymond (1999), documented several instances of Free/Open Source software that were, for one reason or another, abandoned by their founders. Indeed, one of the guidelines the author suggests for writing good software using the *Bazaar* method[17] states that "When you lose interest in a program, your last duty to it is to hand it off to a competent successor" (Raymond 1999, p.6).

Raymond recognised the problem of loss of commitment and sought to propose a suitable solution to constant abandonment of what constituted, even in 1999, a vast repository of free software. He did not attempt to change developers' minds about such abandonment, as, while not making this explicit, he likely recognised this as an inherent hacker characteristic. In light of this fact, every hacker project —be it hardware produced out of a hackerspace or a distributed software effort— needs to find suitable strategies for torch-handing. This may be done by organising contingencies around the inherently meritocratic nature of their relationships.

Indeed, principle number 4 of *The Hacker Ethic* states that "Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position". As Levy himself has suggested, this trait stems not from a desire to do the right thing, but is, in fact, a rather pragmatic approach on their part. By welcoming and embracing those who are good at their craft, hackers satisfy their general state of intellectual curiosity and advance their projects forward. This will, in most cases, result in a red tape-free, intellectually stimulating environment. Furthermore, this practice goes hand in hand with peer-based group learning, a process which has greatly evolved, alongside technology.

With the emergence of the world wide web and prior to the popularisation of hacker conventions, simply known as *cons* and the dawn of hackerspaces, sharing and learning processes began taking place online. Hackers were no longer restricted to working with and acquiring knowledge from peers who were physically close. This led to an explosion of information flow and the increasing complexity of software projects, which ultimately resulted in the creation of the Linux kernel, among many others. This shift had obvious consequences in how hackers learned and cooperated. They became more isolated in the physical sense and their interactions became mediated by networked publics. In detailing how this relates to their education, Himanen (2001, p.75) called this phenomenon "The Net Academy", in reference to Plato's Academy. Using this term, Himanen envisaged an educational model, that is, a model for higher education, based

[17] Raymond contrasts the traditional top-down approach to building software, common back then in corporate environment and likened to the building of a large cathedral, to the then-revolutionary bottom-up method devised by Linus Torvalds for the Linux kernel, seemingly disorganised and mostly de-centralised, likened by Raymond to a "great babbling bazaar of differing agendas and approaches" (Raymond 1999, p.3).

even more closely on hacker principles: more horizontal, more open and less formally structured, thus allowing pupils to follow their own interests.

If one is to judge by results yielded, the model is, indeed, highly successful —at least with regards to the production of software. The GNU/Linux operating system has gone from being a fringe project to powering most of the web's infrastructure, not to mention a wide array of devices such as mobile phones[18], home appliances and even spaceships (Debian Project, The 1997). Furthermore, many of today's large corporations (Apple, IBM, Google, Facebook) as well as up and coming start-ups all benefit from and contribute to the Free/Open Source software environment.

It remains to be seen, however, if these methods for learning and making are equally successful under the newer circumstances created by the emergence of hackerspaces. The historical evidence seen throughout the dawn and flourishing of the subculture in the times pre-dating the web certainly seem to suggest so, yet the challenges and opportunities of this new phenomenon deserve their own analysis, the first step of which is to understand how hackerspaces came to be.

2.5 Hackerspaces

> *The virtual is the true domain of the Hacker. It is from the virtual that the Hacker produces ever-new expressions of the actual. To the Hacker, what is represented as being real is always partial, limited, perhaps even false. (...) To hack is to release the virtual into the actual, to express the difference of the real*
>
> McKenzie Wark (2004, v.74)

> *Indeed, serious hackers primarily exist as hackers on-line*
>
> Manuel Castells (2001)

Statements not unlike the two epigraphs above are common in academic literature from the first half of the 2000s. It is important, thus, to understand how and why hackerspaces have thrived when physical presence in the context of co-operative commons-based collaboration was widely declared irrelevant.

While, in their most recent incarnation, hackerspaces are a relatively recent phenomenon, there is ample precedent for them. Those who form them see their spaces as a natural evolutionary step stemming from hippie

[18] Google's Android operating system, which represented, as of September, 2011, 56% of the mobile market (Jackson 2011), is powered by GNU and Linux.

communes. Hacker and artist Johannes Grenzfurthner argues that hackerspaces (along with squat houses, alternative cafes, farming cooperatives, etc.) "established a tight network for an alternative lifestyle within the heart of bourgeois darkness" (Grenzfurthner 2009).

Nick Farr sees today's hackerspaces as a "third wave" in a reference to the work of Alvin Toffler, referencing early precursor spaces in both North America and Europe as first and second waves respectively. Whilst Farr's analysis is fascinating, I choose to view the origin of hackerspaces from a different perspective and argue that they are the product of two distinct sets of circumstances: a reconsideration of the death of distance paradigm and the increasingly low cost of electronic hardware.

The latest wave of hackerspaces (what Farr calls the "third wave") came to be as a result of very specific circumstances. In 2007, a group of 35 North American hackers (led by Farr himself) embarked on a trip to Europe in what came to be known as *hackers on a plane*. Their purpose was to physically attend a conference, the CCC, or *Chaos Communications Camp*, which was to be held in Germany and organised by the famed *Chaos Computer Club*. Upon their return, several of these hackers decided to apply what they witnessed and learnt while in Germany and founded some of the most iconic spaces in the United States: Mitch Altman started Noisebridge in the bay area, Bre Pettis began NYC Resistor in New York and Farr founded HacDC in Washington DC. From there, the trend began to quickly spread across the world.

The *Chaos Computer Club* itself is considered the European precursor to modern day hackerspaces. Before its foundation in 1981, earlier groups of young computer enthusiasts had formed in the United States, most notably MIT's Tech Model Railroad Club and the California-based Homebrew Computer Club. Yet, of all three, not only is the CCC the only surviving club, it also shares a direct "evolutionary" link to hackerspaces (Pettis 2011, p.84–86).

Wau Holland founded the CCC in West Berlin in 1981 together with a group of people who took an interest in technological advances, particularly those related to computers. During those days Germans saw the computer revolution as means to "bring about more surveillance and fascism" (Pettis 2011, p.84), yet the hackers of the CCC became interested in the machine's liberating potential. Prior to the spread of the Internet, their attention focused on "opening" tightly-regulated and monopolised early network communications through custom designed and built modems, using plumbing pipes for coupling telephone headsets.

These aptly-named "dataloos" then served as devices through which Germans connected their home computers. Yet, even as networks grew in size, the CCC always remained a tight group of individuals whose main connection was made possible by the bonds of mutual co-presence. The rise of the web did not hinder this trend; rather, it strengthened it, as local

groups began to spawn across Germany and neighbouring countries. The trend was reinforced by the institution of *Chaos Communications Congresses* (indoors) and *Chaos Communications Camps* (outdoors). Like the clubs themselves, these events greatly benefited from the dawn of the web:

> The dot-com boom was ramping up and CCC grew from about 250 people to 1500. There is a regional group in every city and because the first meeting of the CCC happened on a Tuesday, all the groups meet weekly on Tuesdays. While Tuesday CCC meetings are for members only, many regional branches have a public night for talk and discussion either weekly or monthly on a Thursday (Pettis 2011, p.84).

As direct descendants of the CCC, today's hackerspaces are organised around the exact same ethos. To members, the convenience of the web makes it not a means of isolation but a conduit for facilitating assembly, which itself fosters an environment ideally suited for experimentation, not only with software but physical objects as well. Indeed, Moilanen's (2010) survey of hackerspaces confirms that "hardware development and hacking" is the single most common activity within these spaces. The trend clearly contradicts Steven Levy's statements, proving that interest in hardware hacking is on the rise, a trend that had not been observed since the days of the Homebrew computer club. This resurgent interest comes hand in hand with the boom of the *Maker* movement and *open-source hardware*.

Exponential improvements in computing performance, in line with *Moore's Law*[19] have had tremendous impact in the declining general cost of electronic components. This fact, combined with wide availability of open schematics has led to extraordinary interest in electronics and the phenomenon been dubbed as the *Internet of things*, a network of interconnected physical, digital devices that "talk" to each other in a similar way as computers do.

At the heart of this interest is the *Arduino*, a credit card-sized microcontroller that serves as a logic unit for an endless a of devices, most of which are thought of and built inside hackerspaces. Arduino was developed in Ivrea, Italy, itself derived from Colombian artist and developer Hernando Barragán's *Wiring* project (Reas & Fry 2010).

A recent article on the subject by *The Economist* (2011) outlines some of the more interesting (or rather, quirkiest) Arduino-driven inventions:

> ...plants that send Twitter messages when they need watering, a harp made of lasers, an etch-a-sketch clock, a microphone that serves as a breathalyser, or a vest that displays your speed when riding a bike

[19]Moore's Law is a trend whereby computing power is commercially duplicated every two years. It is named after Gordon E. Moore, who first predicted it in 1965.

As the article points out, the "Arduino revolution" is a product of its low cost ($20 USD for a basic board) and a sizeable and increasing array of accessories (touch screens, microphones, sensors), made possible by the system's open schematics, which, rather than hindering its potential, has led to hundreds of thousands of units sold (Economist, The 2011) while also paving the way for the development of a number of clone boards, all of which share the same de-facto standards and work with the same basic programming language, called *Processing*.

Arduino is also at the heart of 3D printers: machines that produce physical objects out of digital models by means of extruding hot plastic through a nozzle in a controlled and systematic way. As a general rule, most (if not all) hackerspaces begin their life building a 3D printer, not only because it is a key project for the purposes of acquiring essential skills, but also because, once assembled, a 3D printer is a crucial replicator, allowing hackers to build parts for other projects in an easy, convenient and inexpensive way[20]. In briefly referring to 3D printers and hackerspaces, the article in *The Economist* says:

> Many [hackerspaces] are organised like artists collectives. At Noisebridge, a hacker space in San Francisco, even non-members can come and tinker —as long as they comply with the groups main rule: to be excellent to each other. "*The Internet is no substitute for a real community*," says Mitch Altman, a co-founder of Noisebridge. (emphasis added).

The quote provides a simple, yet enlightening perspective. In enthusiastically adopting open-source hardware and leveraging the benefits of online communications hackers and hackerspaces have come full circle as descendants of earlier collectives, re-discovering and embracing the benefits of co-presence for their own, unique purposes. In doing so, they have enabled themselves to work with physical objects, aided by dropping hardware costs, bringing to an end an era in which the ideal —indeed the only— way to hack, was through the authorship of aeriform software.

The same social circumstances that led to an explosion of countercultural movements in the decades after the post-war were decisive in shaping the emergence of the hacker subculture, one that was born inside the

[20]The implications behind the fascinating world of 3D printers are analysed in chapter 'making'

confines of the Massachusetts Institute of Technology but quickly found its way to the rest of the United States and elsewhere by virtue of the invention of the microprocessor. Although revolving around technologies, hackers were part of the same "salad bowl" environment that fostered the genesis of dozens of movements: hippies, free speech and civil rights activists, feminists and many others who, together, were seen as a force swaying away from social traditional values and established world-views, and whose main unifying characteristic was an explicit desire to distance themselves from those views and values, which they perceived as corrupted. Despite their shared origins and common ground, however, hackers followed a more pragmatic approach in their path to self-discovery, preserving what they saw as useful and making conscious efforts to change things by means of subtle and unexpected —but usually lawful— manipulation of the rules of the environments that concerned them. The hacker mythology and its ethos are based on the expansion of freedom of speech towards cultural manifestations and information with an emphasis on software —the language of computers.

For the hacker subculture, freedom of information became a primary ideal, as it was thought that only through it would personal freedom be fully achieved: *information shall set you free*. Furthermore, thirst for information, manifested in inherent curiosity has provided ideal circumstances for the subculture to flourish, both within the confines of networked publics and, increasingly, through physical co-presence, as a result of a number of things, including a rise in their numbers, dropping hardware costs and, somewhat ironically, the use of online tools, which, rather than promoting isolation, has allowed them to communicate and organise efficiently.

This chapter concludes the "lead-in" of this dissertation. The core, starting with chapter [4], ['making'], aims to analyse the consequences of these developments, in order to better understand hacker sociality, skills transmission and potential for innovation.

3 Research Methodology

3.1 Hacker Ethnography

As a result of my background, I have interacted with hackers (of the free and open source software kind) on numerous occasions and moved naturally amongst them. As such, I believe my position is ideal for adopting an ethnographic approach —one mostly consisting of fieldwork in the form of participant observation and complemented, at a narrower scale, by a reasonable number of qualitative interviews, as detailed below.

I see hackerspaces and the individuals who conform them both as a subcultural movement derived from the broader bohemian category and as communities of practice, sharing and fostering their skills and knowledge by virtue of their collective intellectual curiosity. In this context, I regard my choice of an ethnographic approach as suitable for a number of reasons.

First, it will allow me to empirically test my hypotheses by allowing me to gain first-hand exposure to hackers and hackerspaces. Empirically obtained data is, in my case, essential, given the relative scarcity of scholarly works on hackerspaces. Second, it will then enable me to contrast my observations against my chosen framework and sub-frameworks and test for any theoretical inconsistencies that might arise, in search for what Baszanger & Dodier (1997) call a process of "totalisation" —delineating their boundaries in accordance to the scope of my field. Third, ethnographic fieldwork will allow me to "explore the tissue of [hackers'] everyday life to reveal the processes and meanings which undergird social action" (Herbert 2000, p.551), that is, to gain an understanding of their social structure and in doing so, answering the puzzles formulated throughout this dissertation.

3.2 Three Cities, Three Technoscapes, Three Hackerspaces

The growing presence of hackerspaces across the world poses an interesting challenge with regards to my methodological approach, the first of which is achieving a reasonable degree of what Silverman (2000) calls *generalisability* with regards to my findings, particularly when analysing a limited number of sites and given the budgetary constraints of a PhD candidate in lone-researcher mode[21].

To address this issue, I will approach my fields with a globalised perspective, following Appadurai's (1996) concept of *scapes*, particularly, *technoscapes*: irregular landscapes defined by the "global and ... ever fluid configuration of technology", attempting to make sense of the causes and effects such technology exerts within local, yet increasingly connected com-

[21] See section 3.6 for more on the financing of this project and solutions to budget constraints.

munities. I intend to adopt a centre-periphery approach, thereby choosing three specific hackerspaces in three different cities of the world, from San Francisco in the United States (centre) to Melbourne to Bogotá, Colombia (periphery). This choice is deliberate and the product of careful thought combined with my personal circumstances. Figure 1 provides a graphical representation of my selection as it fits into the research design detailed in this section.

3.2.1 Half-way: *Connected Community* in Melbourne

I intend to undertake the greater part of my research in Melbourne, embarking in fieldwork at *Connected Community*, the city's local hackerspace. Connected Community is a maturing space, with about 15 fee-paying members, over 40 collaborators[22] and a recently attained incorporation as a non profit organisation[23].

Notwithstanding the fact that I am based in Melbourne, making it logistically convenient to adopt Connected Community as my main site, I see Connected Community as an ideal location for two main reasons. First, I regard it as being positioned half-way between the centre and the periphery of the hackerspaces technoscape, far enough from fully-developed technological foci, yet still within a developed nation with a relatively small but healthy IT landscape. As such, it will allow me to make cautious generalisations about the phenomenon, while also enabling me to corroborate and/or disprove most of my assumptions and to make the larger part of my observations long before embarking on costly travel overseas. Second —and most important— Connected Community is a community of practice in the making. Having recently formalised and incorporated but still being in its relative infancy, this hackerspace will provide me with a priceless opportunity to witness its evolution and growth, in terms of members, social relations and skills.

I intend to make Connected Community my primary field, performing the majority of my research with Melbourne-based hackers at their headquarters. This will allow me to have a strong frame of reference with which to make comparisons against technoscapes at the centre and periphery. Section 3.3 delves into the research strategy in more detail.

3.2.2 Centre: *Noisebridge* in San Francisco

Noisebridge in San Francisco is one of the most prominent hackerspaces —one that has served as a model for several others. Two main reasons make Noisebridge particularly noteworthy. First, it was one of the first original American spaces, founded by Mitch Altman, a well-known hacker

[22] See .
[23] See .

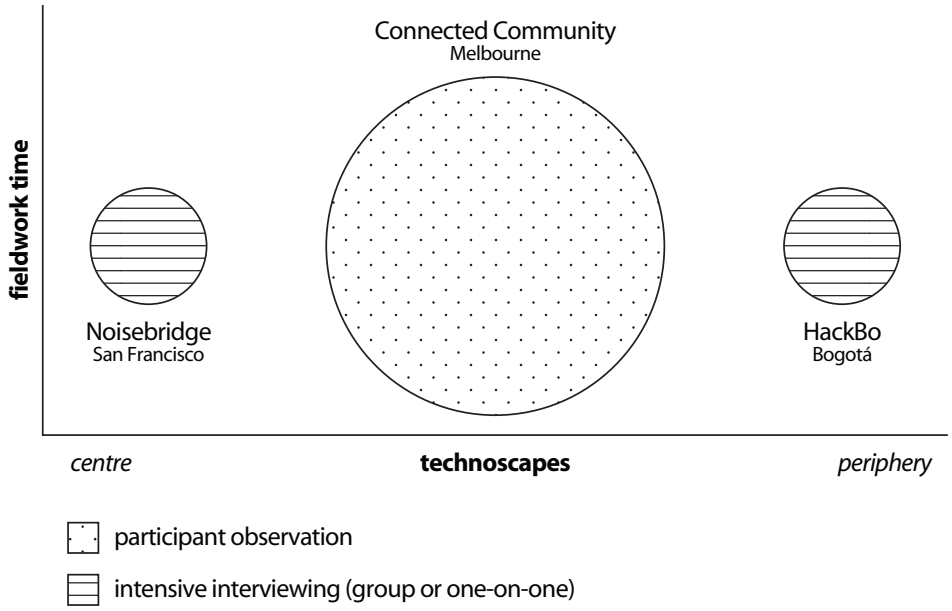

Figure 1: Synthesised methodological approach

who came up with the idea after his visit to the 2007 Chaos Communication Camp, a yearly hacker convention held in Germany[24]. A piece on *Wired* magazine details the genesis of Noisebridge, as well as American hackerspaces in general:

> While many movements begin in obscurity, hackers are unanimous about the birth of U.S. hacker spaces (sic): August, 2007 when U.S. hackers Bre Pettis, Nicholas Farr, Mitch Altman and others visited Germany on a geeky field trip called Hackers on a Plane. (Tweney 2009)

The second —and most important reason for Noisebridge's notoriety is its location. As mentioned in section 1, the origin of Silicon Valley as a central technological hub is closely tied to a group of early pioneers and the ever favourable influence of Stanford University and the U.S. Military (Lee *et al.* 2000). Today, and despite its well-known ups and downs, it is perhaps the most influential IT hub in the world, largely responsible for the technology-driven economic booms of the 1980s and 1990s in the United States (Bresnahan & Gambardella 2004).

In curious contrast to this image of hi-tech behemoth, the Bay area at large has historically presented itself as a Mecca for countercultural movements at least since the 1950s, having served as base for the artists of the

[24]Section 2 offers details on the conference's organisers: the Chaos Computer Club, a renowned hacker group.

so-called *San Francisco renaissance*, as well as becoming a centre for west coast beat poets, hippies, politically-aware students, radicals, dissidents, gays and a plethora of colourful characters.

Noisebridge's appeal thus lies in the fact that it is caught in the midst of the duality between the entrepreneurs and the bohemians: some of its members have long-standing careers in the Valley's tech industry, others have artistic or political backgrounds, while a special few seem to slide naturally between the two worlds. Altman himself is somewhat of a hippie and a pioneer of virtual reality technologies, having founded a company called 3ware[25]. Noisebridge's over 150 members range from professional programmers, to artists, activists and designers. It also has the dubious honour of counting Jacob Appelbaum (the most prominent American Wikileaks associate) as a founding member. Appelbaum has been the subject of several news reports lately, due to Wikileaks' spotlight, his relationship with Julian Assange (Rich 2010) and the continued harassment he has been subjected to by U.S. government officials (Mills 2010).

3.2.3 Periphery: *HackBo* in Bogotá

Some 6,000 kilometres south-east of San Francisco is HackBo, Bogotá's own hackerspace. HackBo was founded in 2010 after three failed attempts to organise what was, until then, a loosely-tied community of mostly free and open source software hackers stemming from the country's public universities (Arizmendi 2011). HackBo currently counts 15 fee-paying members and a larger number of associates[26], having now become a consolidated space, thanks in part to a strategic alliance with an already existing cultural centre, *El Eje*[27] (The Axis), with which it shares a common habitat —a house located in the city's university district. HackBo's members describe their space as an "open community lab" (Uribe 2011) where everybody is welcome to share their experiences and knowledge and to learn about computer languages and hardware hacking.

HackBo was modelled after Hacker Dojo, another iconic American space founded by Lee Felsenstein[28]. In terms of activities, it follows many of the same trends as other hackerspaces around the world: electronics tweaking, open source software and crafts, yet, for the purposes of my study, HackBo offers a very interesting opportunity.

Unlike the United States and Australia, whose budget for research and development is in the billions of dollars and represent relatively high per-

[25] See .

[26] See .

[27] See .

[28] Felsenstein is a long-standing and well-known hacker, former moderator of the Homebrew Computer Club. See Levy (1984) for more information.

centages of their GDP[29], Colombia occupies a humble fifty-second place, having invested about 600 million U.S. Dollars in 2007, only around .16% of its GDP (Unesco 2010, p.82). Yet, there are perceivable cues that suggest change. Juan Manuel Santos, the recently elected President released an ambitious four-year plan for IT infrastructure immediately after reaching his position. The plan calls for an aggressive strategy to widen broadband usage and coverage in the country with special emphasis in depressed and remote regions, while promoting incentives for skills development and IT related business activities, particularly software development (Molano 2011).

Despite this ambitious push, which also includes the institution of three new IT research centres, there is still a relative scarcity of formal research entities in the country, a fact that raises the question as to whether or not hackerspaces can fulfil that role with some degree of success, either by positioning themselves as informal but effective research centres or by providing much-needed knowledge and skills to future researchers.

Colombia's current stance with regards to ICT, combined with its unique cultural and social conditions, make HackBo attractive as a vehicle through which to study how environmental nuances influence learning and technological development inside hackerspaces.

3.3 Research Strategy

Ethnographic participant observation will be my primary research method, complemented by in-depth interviews at hackerspaces overseas. I intend to collect a substantial amount of data and to reach major preliminary conclusions before undertaking any research outside of Australia, the intention being to use interview data from overseas to test for representativeness and generalisability (as well as deviations) by contrasting it against the original, more comprehensive sample, hoping to verify and evaluate what should by then be a well-developed, yet early analysis.

I intend to spend a considerable amount of time amongst Melbourne hackers, assuming the role of a participant observer, regularly attending the Connected Community's weekly Tuesday meetings as well as some of the more informal weekend "hang-out" sessions. Tuesday meetings are of a formal nature and highly attended (thus ideal for performing Interaction Ritual Theory analysis), while the more spontaneous weekend meetups are somewhat more intimate and will hopefully provide insight into power relations, conflict and other intimate phenomena.

In attempting to work within the boundaries of my theoretical foundation, I have identified key elements on which to focus, hoping to find patterns and consistent behaviours that will subsequently lead to deep and

[29] United States: 395.8 Billion, 2.8% of GDP in 2010. Australia: 15.3 Billion, 1.8% of GDP in 2010 (Wadsworth 2010).

hopefully fruitful analysis. While my intention is to gather data for all chapters in a concurrent manner, I will focus my observations sequentially in the same order as my three core chapters so as to build upon them as the work progresses. Outlined below are these main focal elements.

3.3.1 Core 1: Applying Interaction Ritual Theory

- Identification of specific hacker rituals as well as their nature (formal, natural) and degree of success (successful, failed, empty, forced).
- Identification of ritual ingredients and outcomes in the context of hackerspaces — Collins (2004, p.41) describes well-delineated causes and consequences of IRT. I will attempt to spot such factors in rituals held in hackerspaces, placing added emphasis in co-presence and barriers (ingredients) and symbols and negotiated morality (outcomes).
- Identification of key situations leading to "symbolisation" and the establishment of sacred objects.

3.3.2 Core 2: Applying Legitimate Peripheral Participation

- Identification of a clear power structure in the context of LPP's examination of the duality between newcomers and old-timers and the prior analysis of IRT's sacred objects.
- Identification of instances of negotiated meaning and common concern. Similarly to Polanyi, Lave & Wenger argue that knowledge is partly negotiated within a group. Within hackerspaces, analysis of this common meaning could be especially fertile, particularly in shedding light on the processes of learning and participation.
- Identification of motivation factors leading to the transition from peripheral to full participation within hackerspaces.

3.3.3 Core 3: Applying Cognitive Change

- Identification of problem selection in the context of prior analysis of symbolisation (core 1) and negotiated meaning (core 2). Cognitive Change Theory places problem-solving at the centre of technological advance[30], thus the nature of problem selection becomes especially meaningful in understanding how technology flourishes in hackerspaces.

[30]It should be noted that the concept of problem-solving, according to the author, is indeed a broad one, involving not only "utilitarian" activities but also aesthetic and intellectual ones (Laudan 1984, p.84).

- Categorisation of types of problems solved by hackers within the CCT system.
- Identification of the effects of the "environment" as described by Laudan (1984, p.101) in relation to technological production in hackerspaces, considering prior analysis of settings and rituals. Also, identification of potential "niche-isation" in different hackerspaces and the determining factors in this process.

It is worth mentioning that I intend to conduct all my research overtly, with full disclosure to the community. I have already engaged some members of Connected Community at a personal level, yet all official data collection will begin only after gaining approval from the Monash University Human Research Ethics Committee (MUHREC). I should also note that I am already acquainted with the process of gaining ethics approval and performing research within the committee's guidelines as a result of having chosen similar methods for my Master's thesis. Section **??** specifies my timeline for gaining ethics approval and undertaking participant observation at Connected Community.

3.4 Data and Data Analysis

Fieldwork at Connected Community in Melbourne will be documented primarily with the aid of fieldnotes, following Schatzman & Strauss's (1973) note-taking method. Summarily, the procedure involves labelling notes into three categories: Observational (ON), Theoretical (TN) and Methodological (MN). At a later stage, the notes are further categorised into logical thematic packages and complemented by analytic memos that serve as more explicit and elaborated theoretical notes. As noted earlier, my observations will take place overtly so I expect to be able to take "jotted notes" (Lofland & Lofland 1995, p.90) on the spot, transforming them to "full fieldnotes" at a later time.

While fieldnotes seem to be the data-gathering method of choice for social scientists at large (Silverman 2000; Lofland & Lofland 1995; Schatzman & Strauss 1973), I share Peräkilä's (1997) concerns regarding their reliability. At best, fieldnotes provide a mediated account of events, filtered by the researcher's own points of view or interpretations. At worst, they can reflect erroneous observations and lead to mistaken conclusions. Thus, I will attempt to simultaneously collect raw data in the form of audio or video recordings to the extent to which such recordings are logistically, socially and ethically admissible.

For the purposes of interviewing, audio recordings alone will be the method of choice. Interviews conducted for my Master's thesis provided me with some methodological experience in conducting and logging ses-

sions. My method involves taking carefully annotated notes prior to transcribing. Much like the fieldnote model described above, the notes are categorised and, more importantly, accompanied by a detailed, time-coded guide by which one can easily refer back to the original data.

Moreover, I seek to analyse all my qualitative data using Miles & Huberman's (1984) method, by means of three concurrent flows of activity: *reduction*, whereby one selects, focuses and simplifies raw data, *display*, involving assembling information so that it allows for "conclusion drawing and action taking" (matrices, graphs, networks) and *conclusion/verification*, in which one connects causes and propositions in order to infer and determine. I realise that data coding can be an extremely laborious process, so my overall timeline for the completion of this project (see Section **??**) accounts for these steps.

3.5 Potential Woes

Realising that there is no such thing as a perfect methodological design, or a one-size-fits-all solution, I consider the task of identifying potential shortcomings with the proposed research design a mission-critical one. This section attempts to provide preliminary reflections on potential shortcomings. It also offers possible solutions and/or counter-arguments.

Familiarity with the setting. While prior contact with hackers and relatively good knowledge about their social etiquette and practices is almost certainly a good thing, it also carries with it the risk of making the researcher "feel too comfortable". Hammersley (1990), seems to agree by arguing that "when a setting is too familiar, the danger of misunderstanding it is especially great". It is thus important not to take anything for granted and to attempt to disregard previous facts or assumptions that are the result of prior experience. As such, making a conscious effort to enter the field without any biases or preconceptions is crucial.

Under this same category, one can find the risk of developing over-rapport with research subjects. Familiarity and shared values can stop a researcher from evaluating his or her settings critically. Establishing rapport is an ever-present recommendation in fieldwork guides, yet the risk of over-sympathising with members of the communities under study can result in lack of critical judgement. On the topic, Roberts (1994) asks: "how does one, whose self interests are foremost in beginning an examination of a social world, hope to remain objective enough to command a claim of validity from his audience?". I do not believe there is a straightforward answer to that question, yet I am convinced that active and deliberate steps must be taken in order to prevent the loss of a researcher's independence and capacity for critical inquiry.

Under-analysis of data. Having chosen to study multiple fields, I run the risk of either collecting too much or too little data for any one of them. I have considered this possibility and attempted to minimise it by selecting specific (and meaningful) events to assist to while performing participant observation in Melbourne. With that same frame of mind, I have decided to limit fieldwork for my other two sites so as to only seek to identify similarities and divergences from tendencies already observed in Melbourne. This will hopefully provide me with a reasonable volume of data —one that aids in reaching accurate findings without becoming overwhelming. Needless to say, this potential catch will also be considered when determining the number of interviews to be conducted at the two hackerspaces overseas.

Multiple methods Silverman warns about possible complications stemming from the use of multiple research methods: "multiple methods may tempt novice researchers to move to another dataset when they are having difficulties in analysing one set of material" (Silverman 2000, p.134). I share the author's concern, yet I view my methods as complementary. In essence, I will avoid turning to one set of data when the other does not fit. Instead, I will only use interview data to explicitly contrast existing findings that are the product of previous fieldwork in Melbourne.

By identifying potential problems with my methodology before they happen, I aim to minimise their impact and to plan out possible solutions or alternative methods if needed. I consider this section to be nothing more than a work in progress, in the sense that the above list will be extended, developed and revised as this work moves forward.

3.6 Some Thoughts on Financing and Logistics

This project is, by design, ambitious in nature. Not only is it broad in scope, but it also considers fields separated by great distances. As exciting as this sounds, its logistics can indeed become a cause for concern for a single PhD candidate with a moderate budget. Thus, securing proper financing has become an on-going priority.

I intend to apply for a Postgraduate Travel Grant to conduct fieldwork[31]. As mentioned in section 3.2, my choices of overseas hackerspaces have also been shaped by my personal circumstances. I am a Colombian citizen from Bogotá. I have been acquainted with various members of the hacker community in that city for a number of years and personally know at least one of the members of HackBo. This will reduce my barriers of entry to the site in terms of time and resources, while allowing me to cut my travel expenses by having a place to stay while I conduct my research. Moreover, due to the nature of international flight hubs, the simplest, most cost-effective way for

[31] See .

me to fly to Bogotá is by connecting flights at the Los Angeles Airport in California. As a result, the logistics of my research at Noisebridge will be greatly minimised, as my stay in San Francisco will be relatively simple to arrange.

In light of the fact that time spent overseas will be short, I cannot engage in the same type of long-term participant observation I intend to conduct in Melbourne. Consequently, I have opted to adopt intensive interviewing as my main research method at these locations. Much like Lofland & Lofland (1995), I do not view intensive interviewing as a substitute for participant observation. Rather, I see both methods as being complementary and appropriate for each of my circumstances, as I intend to build upon previous findings at these locations.

Naturally, much if not all of the preparatory work for these interviews will take place in Melbourne. I intend to contact members of both hackerspaces immediately after gaining ethics approval, well in advance of my trip. Having been a subscriber to both Noisebridge's and HackBo's public email lists since December 2010, I expect to be able to identify key members and to approach them prior to reaching my destinations.

References

Altman, M. (2011). Science on the spot: Open source creativity - hackerspaces. . Accessed 6 February, 2011.

Amabile, T. (1996). *Creativity in Context: Update to "The Social Psychology of Creativity."*. Westview Press, Boulder, CO.

Angel, D. (2009). *No Big Deal: How Wikipedia Administrators Help Shape and Influence the Project*. Master's thesis, National Centre for Australian Studies — Monash University.

Appadurai, A. (1996). *Modernity at Large: Cultural Dimensions of Globalisation*. University of Minnesota Press.

Arizmendi, D. (2011). Hackbo, un espacio para los seguidores de la tecnología en bogotá. . Accessed 15 February, 2011. Resource in Spanish.

Bahrami, H. & Evans, S. (2000). *Understanding Silicon Valley: the Anatomy of an Entrepreneurial Region*, chap. 8: Flexible Recycling and High-Technology Entrepreneurship, 166–186. Stanford University Press.

Baszanger, I. & Dodier, N. (1997). *Qualitative Research: Theory, Method and Practice*, chap. 2: Ethnography: Relating the Whole to the Part, 8–23. Sage Publications, London, UK.

Blackman, C. (1998). Convergence between telecommunications and other media. *Telecommunications Policy*, **22**, 163–170.

Bodzin, S. (2004). Inventor rejoices as tvs go dark. Wired Magazine . Accessed 12 January, 2011.

boyd, d. (2008). *Taken Out of Context: American Teen Sociality in Networked Publics*. Ph.D. thesis, University of California, Berkeley.

Bresnahan, T. & Gambardella, A. (2004). *Building high-tech Clusters: Silicon Valley and Beyond*, chap. 1: Introduction, 1–10. Cambridge University Press, Cambridge, UK.

Brontsema, R. (2004). A queer revolution: Reconceptualizing the debate over linguistic reclamation. *Colorado Research in Linguistics*, **17**, 1–17.

Bunker, J. (2011). Remade: The rebirth of the maker movement. . Accessed 15 February, 2011.

Castells, M. (2001). *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford University Press, Cambridge.

Collins, R. (2004). *Interaction Ritual Chains*. Alexander Street Press.

Connected Community (2011). Group projects. . Accessed 12 February, 2011.

Coupland, D. (1995). *Microserfs*. Flamingo, London.

Csikszentmihalyi, M. (1975). *Beyond Boredom and Anxiety*. Jossey-Bass.

Dahlberg, L. (2001a). Computer-mediated communication and the public sphere: A critical analysis. *Journal of Computer-Mediated Communication*, **7**, 0.

Dahlberg, L. (2001b). The internet and democratic discourse: Exploring the prospects of online deliberative forums extending the public sphere. *Information, Communication & Society*, **4**, 615–633.

Dahlgren, P. (2005). The internet, public spheres, and political communication: Dispersion and deliberation. *Political Communication*, **22**, 147–162.

Debian Project, The (1997). New computer operating system rides space shuttle. . Accessed 19 March, 2012.

Dougherty, D. (2010). From knock-offs to 'make-offs'. Forbes Magazine . Accessed 15 February, 2011.

Dowding, M. (2001). National information infrastructure development in canada and the u.s.: Redefining universal service and universal access in the age of techno-economic convergence. .

Economist, The (2011). More than just digital quilting. . Accessed 17 March, 2012.

Eder, K. (1990). The rise of counter-culture movements against modernity: Nature as a new field of class struggle. *Theory Culture Society*, **7**, 21–47.

Gibson, W. (1984). *Neuromancer*. Ace Books, New York.

Gimmler, A. (2001). Deliberative democracy, the public sphere and the internet. *Philosophy Social Criticism*, **27**, 21–39.

Ginn, C. (2011). The big i: 3d printing. CNN Newsroom Blog . Accessed 14 January, 2011.

Grenzfurthner, J. (2009). Hacking the spaces. . Accessed 19 March, 2012.

Hackerspaces.org (2011). What are hackerspaces? . Accessed 6 February, 2011.

Hafner, K. & Markoff, J. (1991). *Cyberpunk : outlaws and hackers on the computer frontier*. Simon & Schuster, New York.

Hammersley, M. (1990). *Reading Ethnographic Research: A Critical Guide*. Longman, New York, NY.

Harvey, B. (1986). Computer hacking and ethics. Tech. rep., ACM Panel on Hacking.

Heath, J. & Potter, A. (2005). *The Rebel Sell: Why the Culture can't be Jammed*. Crichester : Capstone.

Hebdige, D. (1987). *Subculture: The Meaning of Style*. Routledge, New York.

Herbert, S. (2000). For ethnography. *Progress in Human Geography*, **24**, 550–568.

Himanen, P. (2001). *The Hacker Ethic and the Spirit of the Information Age*. Random House, New York.

Howells, J. (2000). *Knowledge, Space, Economy*, chap. 4: Knowledge, Innovation and Location. Routledge, London.

Ito, M. (2008). *Networked Publics*. MIT Press.

Jackson, I. (1998). Why is software freedom useful, and what does it mean? In *System Administration and Networking 1998*.

Jackson, M. (2011). Android market share reaches 56 percent; rim's, microsoft's cut in half. . Accessed 19 March, 2012.

Johnson, J. (2009). Mitch altman completes his worldwide tour of hackerspaces (welcome home!). . Accessed 19 January, 2011.

Kalish, J. (2010). A space for diy people to do their business. . Accessed 25 March, 2011.

Kendall, L. (1999). Nerd nation: Images of nerds in us popular culture. *International Journal of Cultural Studies*, **2**, 260–283.

Kenney, M. (2000). *Understanding Silicon Valley: the Anatomy of an Entrepreneurial Region*, chap. 10: Institutions and Economies, 222–240. Stanford University Press.

Khan, B. Z. (2006). An economic history of copyright in europe and the united states. . Accessed 8 July, 2010.

Kinney, D. (1993). From nerds to normals: The recovery of identity among adolescents from middle school to high school. *Sociology of Education*, **66**, 21–40.

Kuznetsov, S. & Paulos, E. (2011). *From Social Butterfly to Engaged Citizen (MIT Press 2012)*, chap. 10. Rise of the Expert Amateur: DIY Projects, Communities, and Cultures. MIT Press, Cambridge, MA.

Lakhani, K. & Wolf, R. (2003). Why hackers do what they do: Understanding motivation and effort in free/open source software projects. *MIT Sloan Working Paper No. 4425-03*, **1**, 1–27.

Laudan, R. (1984). *The Nature of Technological Knowledge. Are Models of Scientific Change Relevant?*, chap. 5: Cognitive Change in Technology and Science, 83–104. D. Reidel, Dordrecht, Netherlands.

Lave, J. & Wenger, E. (1991). *Situated Learning: Legitimate Peripheral Participation*. Cambridge University Press, Cambridge, UK.

Lee, C., Miller, W., Hancock, M. & Rowen, H. (2000). *The Silicon Valley edge: a Habitat for Innovation and Entrepreneurship*, chap. 1: The Silicon Valley Habitat, 1–16. Stanford University Press, Stanford, CA.

Lee, D. & Mendelson, H. (2008). Divide and conquer: Competing with free technology under network effects. *Production and Operations Management*, **17**, 12–28.

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. Penguin Books.

Levy, S. (2010). Geek power: Steven levy revisits tech titans, hackers, idealists. . Accessed 8 June, 2010.

Lofland, J. & Lofland, L. (1995). *Analyzing Social Settings*. Wadsworth Publishing Company, Belmont, CA.

Marchant, O. (2003). *The Post Subcultures Reader*, chap. 6: Bridging the Micro-Macro Gap: Is there such a thing as a post-subcultural politics?, 83–97. Berg Publishers, New York, NY.

McGregor, C. (1975). What counter-culture? *Meanjin Quarterly*, **34**, 40–44.

Miles, M. & Huberman, A. (1984). *Qualitative Data Analysis: a Sourcebook of New Methods*. Sage Publications, London, UK.

Mills, E. (2010). Researcher detained at u.s. border, questioned about wikileaks. . Accessed 29 March, 2011.

Moilanen, J. (2010). Hackerspaces, members and involvement (survey study). . Accessed 12 February, 2011.

Molano, D. (2011). Plan vive digital colombia. Tech. rep., Colombian Ministry for IT.

Moore, T. (2007). *Australia's Bohemian Tradition*. Ph.D. thesis, University of Sydney.

Moreira, A., Mller, M., Gerhardt, G. & Ladner, A. (2009). E-society and e-democracy. In *eGovernment-Symposium 2009*.

Morgan, K. (2004). The exaggerated death of geography: Learning, proximity and territorial innovation systems. *Journal of Economic Geography*, **4**, 3–21.

Oinas, P. (2000). *Knowledge, sInnovation and Economic Growth*, chap. 4: Distance and learning: does proximity matter? Edward Elgar Publishing.

Open Source Initiative (2012). History of the osi. . Accessed 18 February, 2012.

Peräkilä, A. (1997). *Qualitative Research: Theory, Method and Practice*, chap. 13: Reliability and Validity in Research Based on Tapes and Transcripts, 201–220. Sage Publications, London, UK.

Pettis, B. (2011). *Hackerspaces: The Beginning*. Self-published.

Poster, M. (2001). *Reading Digital Culture*, chap. 26: Cyberdemocracy: The Internet and the Public Sphere, 259–271. Blackwell Publishing, Oxford.

Raymond, E. (1999). *The Cathedral and the Bazaar*, chapter 2: The Cathedral and the Bazaar, 19–64. O'Reilly & Associates, Inc., second ed.

Raymond, E. S. & Steele, G. (1993). *The new hacker's dictionary*. The MIT Press.

Reas, C. & Fry, B. (2010). *Getting started with Processing*. O'Reilly & Associates, Inc.

Rich, N. (2010). The most dangerous man in cyberspace. . Accessed 29 March, 2011.

Roberts, B. (1994). The challenge of over-rapport. *Bulletin of the Council for Research in Music Education*, **123**, 90–96.

Rodman, S. (2009). 'big bang theory' has burst into an old-school hit comedy. . Accessed 7 July, 2010.

Roszak, T. (1969). *The making of a counter culture : reflections on the technocratic society and its youthful opposition*. Doubleday & Company, Inc.

Schatzman, L. & Strauss, A. (1973). *Field Research*. Prentice Hall, Englewood Hills, NJ.

Silverman, D. (2000). *Doing Qualitative Research*. Sage Publications, London, UK.

Smith, N. (2006). It crowd writer looks to future. . Accessed 7 July, 2010.

Spates, J. (1976). Counterculture and dominant culture values: A cross-national analysis of the underground. *American Sociological Review*, **41**, 868–883.

Stallman, R. (1985). The gnu manifesto. *Dr. Dobb's Journal of Software Tools*, **10**, 30–36.

Stallman, R. (2002a). *Free software, free society : selected essays of Richard M. Stallman*. GNU Press, Free Software Foundation.

Stallman, R. (2002b). On hacking. . Accessed 1 October, 2011.

Stoll, C. (1989). *The cuckooś egg : tracking a spy through the maze of computer espionage*. Doubleday, New York.

Syvertsen, T. (2003). Challenges to public television in the era of convergence and commercialization. *Television & New Media*, **4**, 155–175.

Thomas, D. (2002). *Hacker culture*. University of Minnesota Press.

Thornton, S. (1996). *Club Cultures: Music, Media, and Subcultural Capital*. Wesleyan.

Tocci, J. (2007). The well-dressed geek: Media appropriation and subcultural style. In *MiT5 at the Massachusetts Institute of Technology*.

Tweney, D. (2009). Diy freaks flock to hacker spaces worldwide. . Accessed 3 June, 2010.

Unesco (2010). Unesco science report 2010. Tech. rep., Unesco.

Uribe, C. (2011). Interview given to caracol radio. . Accessed 26 January, 2011. Resource in Spanish.

Wadsworth, J. (2010). Battelle 2011 global r&d funding forecast. Tech. rep., Battelle Memorial Institute.

Wagner, R. (2003). Information wants to be free: Intellectual property and the mythologies of control. *Columbia Law Review*, **103**, 995–1034.

Wark, M. (2004). *A Hacker Manifesto*. Harvard University Press.