The Ethic of the Code

Values, Networks and Narrative among the Civic Hacking Community

by

Douglas Haywood

Thesis submitted to Goldsmiths, University of London for the Degree of Doctor of Philosophy

Department of Sociology

Goldsmiths, University of London

2016

This thesis is dedicated to my grandfather, the late Dr Stuart MacRae.

Declaration of Authorship

I, Douglas Haywood, declare that this thesis and the work presented in it are my own and that it has been generated by me as a result of my own original research. Where information is derived from other sources, I confirm that this has been indicated in the thesis.

DOUGLAS HAYWOOD.

Acknowledgement

Firstly, I want to thank my supervisor Dr Brian Alleyne for his advice and for guiding me through the process of writing this thesis, even at a distance. The lengthy process of completing a part-time PhD alongside a full-time job requires extreme patience and understanding on the part of both the student and supervisor.

I would like to express my gratitude to my research participants for taking the time to answer my endless questions and making me feel welcomed as a part of their community.

I would also like thank my employers for allowing me the time and flexibility to pursue my goals and ambitions.

I am extremely grateful to my parents, family, and my friends for all their emotional support over the last five years.

Most importantly, I want to thank Fi for keeping me going and keeping me grounded. This project has been a life ambition and would not have been possible without you. Here’s to the next chapter…

Abstract

Computer hacking has come to represent something negative within mainstream society and is typically associated with malicious or criminal acts. However, for those involved in hacking, this practice typically means something quite different and much more positive in nature. Recently, hacking has also gained increasing popular appeal with greater interest in the role of hackers in the history of technology. This portrayal, however, represents hacking in a binary way, portraying the activity as either 'good' or 'bad' rather than as the reality of a complex and heterogeneous set of practices and ethics. It is within this context that the Civic Hacking movement has emerged. Those involved in Civic Hacking apply these ethics on a global and local scale to create projects which aim to solve a range of social problems using technology and borrowing from the approaches and practices of hacking. These 'problems' can include crime; violence; humanitarian disasters such as tsunamis, famine or earthquake; improvements needed to local government in terms of the democratic process or infrastructure; providing access to healthcare, education or banking in remote areas; involving local communities in issues and a range of other challenges which require solutions. This research project explores hacking as a non-technologically specific social practice based around a collection of Hacker Ethics. Through research focusing on hacking events, I argue that Civic Hacking is indicative of the influence of the Hacker Ethic in wider areas of society. In particular, I explore how Civic Hacking is situated within the wider history of hacking; to what extent the technological artefacts produced by Civic Hacking are shaped by the ethics of these groups; whether Civic Hacking is indicative of a democratisation of technologies; and the types of communities which form around Civic Hacking.

Table of Contents

The Ethic of the Code 1
Declaration of Authorship 3
Acknowledgement 4
Abstract 5
Table of Contents 6
List of Figures 10
List of Tables 11
Chapter 1 12
Introduction 12
1.1 Background: Hacking for Good 12
1.2 Research Aims 16
1.3 Outline of the Thesis 17
Chapter 2 20
Conceptual Framework 20
2.1 Chapter Overview 20
2.2 Part One: Definitions of Hacking 23
2.2.1 Introduction 23
2.2.2 Hacking as a Non-Technological Social Practice: The Hacker Ethics 25
Hacking as a Non-Technological Social Practice 26
The Hacker Ethics 32
The Ideology and Pragmatism of Hacking - Free and Open Source Hacking 42
Hacking as a Gift Society 44
Pragmatic vs Ideological Views of Hacking 48
Hacking's Influence on the Wider World 56
2.2.3 The Criminalisation and Demonisation of Hacking 63
Hacking as a North Atlantic Construct 63
Folk Devils and Moral Panics of the Network Society 70
2.2.4 The Politicisation of Hacking: Hacktivism 74
Hacktivism and its Relationship with Hacking 74
The Symbolic Power of Hacking 85
2.2.5 Conclusions: Towards a Definition of the Hacker Ethics 87
What is a Civic Hacker? 88
2.3 Part Two: Hacking for Social Good 89
2.3.1 Introduction 89
2.3.2 Information and Network Societies 91
Defining Network and Information Societies 91
Network Societies 95
Critiques of Network Society Theories 97
Relevance to Civic Hacking 100
The Network Society and Hacking 103
The Digital Divide 109
The Pragmatism of the Hack: ICT4D 112
2.3.3 Rip, Copy, Burn: Innovation and Hacking 117
Read Only: No Such Thing as 'New'? 117
Technology is Created by Users - Communities of Practice 122

2.3.4 Conclusions 126
2.4 Chapter Conclusions: Building on Previous Research 128
Chapter 3 132
Research Methodology and Methods 132
3.1 Introduction 132
3.2 Research Strategy 133
3.2.1 Rationale for Using Multiple Methods and Methodologies 134
3.2.2 Where does Ethnography Begin and End? 136
3.3 Methodologies 140
3.3.1 Virtual Ethnography 140
3.3.2 Mobile Ethnology and Ethnomethods 143
3.3.3 Conference Studies 148
3.3.4 The Study of Technologies as Cultural Artefacts 150
3.3.5 Social Network Analysis 152
3.3.6 Analysis of Narrative 155
3.4 Research Methods Used For Each Chapter in the Thesis 160
3.4.1 Background 160
3.4.2 Chapter Four: Portraits of Hacking 161
Data Sample, Collection and Analysis 161
3.4.3 Chapter Five: Event Fieldwork 167
Data Sample Selection, Collection and Analysis 168
3.4.4 Chapter Six: Social Network Analysis 171
Data Sample Selection, Collection and Analysis 172
3.4.5 Chapter Seven: Narrative Analysis 176
Data Sample Selection, Collection and Analysis 178
3.5 Mixed-Method and Multi-Site Research 185
3.6 Limitations and Ethical Considerations 187
Chapter 4 192
Towards a Typology of Hacking for Good 192
4.1 Introduction 192
4.1.1 Research Aims 193
4.2 Research Findings 194
4.2.1 Portrait One: 'Ethical Hacking' and Civic Hacking 194
Discussion of Ethical Hacking 200
4.2.2 Portrait Two: ICT4D Activists 201
Discussion of ICT4D Activists 212
4.2.3 Portrait Three: Civic Hacking 212
4.3 Overall Discussion of Findings and Design of Subsequent Research 223
4.3.1 Theme 1: Different Types of Hacking for Good? 223
4.3.2 Theme 2: The Social Shaping of Technological Artefacts 228
4.3.3 Theme 3: The Democratisation of Technology? 231
4.3.4 Theme 4: Virtual Communities 233
4.4 Summary 234
Chapter 5 237
Analysis of the 'Random Hacks of Kindness' Civic Hacking Event 237
5.1 Introduction 237
5.1.1 Research Aims 237
5.2 Research Findings 238
5.2.1 The Formation of Groups and Problem Topics 238
5.2.2 The Civic Hacker Work Ethic 240

5.2.3 The 'Social Geek' 245
5.2.4 A Metaphor of Power Cables 249
Narrative Type #1: Narratives of Openness and Sharing 257
Narrative Type #2: Narratives of Technology 259
Narrative Type #3: Anti-Authoritarian Narratives 260
Narrative Type #4: Narratives Regarding the History of Technology 262
5.3 Discussion 263
5.3.1 The Hacker Ethics and Civic Hacking among the RHoK Event, Community and Technological Artefacts 263
5.3.2 Proliferation or Appropriation of Hacker Ethics? 268
5.4 Summary 271
Chapter 6 273
A Community of Ethics: Social Network Analysis of the #hack4good Twitter Network 273
6.1 Introduction 273
6.1.1 Research Aims 274
6.2 Research Findings 275
6.2.1 In-degree 276
6.2.2 Out-degree 281
6.2.3 Eigenvector Centrality 283
6.2.4 Betweenness Centrality 285
6.2.5 Closeness Centrality 286
6.2.6 Connected Component 288
6.2.7 Exploring the Ties between Actors 294
6.3 Discussion 297
6.3.1 Structure of the Group: Decentralisation and Semi-Autonomy 297
6.3.2 Types of Ties: Sharing, Support, and 'hobbyism' 301
6.3.3 Seeking Advice and Teaching: Where does influence lie? 306
6.3.4 A Community of Ethics 311
6.4 Summary 315
Chapter 7 319
Telling Stories of Good Hacks: Online Narratives of Civic Hacking 319
7.1. Introduction 319
7.1.1 Research Aims 319
7.2. Research Findings 320
7.2.1 Datasource #1: Hackforchange.org Blog 321
7.2.2 Datasource #2: Code for America Blog 324
7.2.3 Datasource #3: Guardian Online Article 326
7.2.4. Datasource #4: Huffington Post Online Article 329
7.2.5. Datasource #5: Opendemocracy.net Website 330
7.2.6. Datasource #6: Npr.org Online Article 332
7.2.7. Datasource #7: NASA Blog 333
7.2.8. Datasource #8: TED Talk Video (Catherine Bracy) 335
7.2.9. Datasource #9: Sunlight Foundation Online Video 338
7.2.10. Datasource #10: TED Talk Video (Jennifer Pahlka) 339
7.3 Discussion 342
7.3.1 Narrative Structures 342
7.3.2 Media Narratives 345
7.3.3 Discussion of Narrative Types 347
Narrative Type #1: History of Technology and the USA 348
Narrative Type #2: Civic Hacker Narratives as Ethnocentric 349

Narrative Type #3: Narratives of Government as Technology 350
7.4 Summary 351
Chapter 8 354
Conclusions 354
8.1 Introduction 354
8.2 Defining Civic Hacking 355
8.3 The Hacker Ethics 360
8.4 The Ethic of the Code 364
8.5 A Community of Ethics 368
8.6 What Stories do Civic Hackers Tell? 372
8.7 Hacking is Going Viral: The Proliferation of Hacker Ethics into Wider Society 376
8.8 Scope for Future Research 381
8.9 Hack the Planet - Final Remarks 383
Bibliography 385
Appendices 421
Appendix A – Narrative Themes Mapped Against the Hacker Ethics 421
Appendix B – Hacking Narrative Themes 422
Appendix C – Online Narrative Data Sources Mapped Against Themes 423
Appendix D – Consent Form 424

List of Figures

Figure 1 Wiktionary Result for Civic Hacker, Wiktionary *127*
Figure 2 Google Searches 'Civic Hacking' vs Google Searches 'hacking', Google Trends *128*
Figure 3 Initial Research Sample of Potential Informants *162*
Figure 4 Direction of Access to those Directly Involved in Civic Hacking *163*
Figure 5 Hierarchy of Narrative Themes. Reprinted from Attride-Stirling (2001) with permission. *181*
Figure 6 The Presentation of 'Problem Definitions' *239*
Figure 7 The Organiser Opens the Event *242*
Figure 8 The Subdivision of Groups *243*
Figure 9 Networked Online Interaction *247*
Figure 10 The Initial Phase of the Process *252*
Figure 11 #hack4good Actors with an In-degree of Greater Than Two *277*
Figure 13 Relationship Between #hack4good Actor and Other Community Members *279*
Figure 14 Influence Derived from Perceived Technical Expertise and Advice *280*
Figure 15 Kudos Within the #hack4good Network *282*
Figure 16 A Retweeted Posting Within the #hack4good Network *284*
Figure 17 A Tweet Promoting the Work of Others *287*
Figure 19 Volume of Tweets per Day Relating to #hack4good *295*
Figure 20 A 'Peak Day' #hack4good Tweet *296*
Figure 21 Tweets Relating to a Key Member, @frathgeber *308*
Figure 22 Civic Hacking Narrative Themes *343*

List of Tables

Table 1 RHoK Southampton Conference participants ________ *168*
Table 2 Online Narrative Sources ________ *179*
Table 3 Classification of highly-connected #hack4good members ________ *289*
Table 4 Geographical Distribution of highly-connected #hack4good members ________ *290*
Table 5. Secondary Themes for Motivation ________ *292*
Table 6. Secondary Themes for Purpose ________ *293*
Table 7. Data Sources Used in Civic Hacking Narrative Analysis ________ *320*

Chapter 1

Introduction

1.1 Background: Hacking for Good

Computer hacking has come to represent something negative within mainstream society. It is typically associated with malicious or criminal acts carried out by deviants to access computer systems in order to break them or steal information. There is certainly a sense in which this type of deviant activity is part of hacking's history. This thesis seeks to develop these previous framings of hacking and to develop a more pragmatic theoretical perspective. For those involved hacking, it often means something quite different and much more positive in nature. For many hackers, hacking is typified by a number of features which are often hard to define and includes a set of ethics and cultural practices.

The term 'hacking' is usually applied to the modification of technology, software or hardware, and is used to refer to the use of clever workarounds to make technology do something different from the original intention of its designer. It is also inherently linked to a set of ethics, referred to as the Hacker Ethic (Levy, 1984; Kelty, 2008; Jordan, 2008), which forms an important conceptual basis for this dissertation. These ethics emphasises collaboration and openness and a strong emphasis towards decentralisation, anti-authoritarianism and rule breaking. Moreover, hacking typically has a social aspect to it, often apparently at odds with our mainstream perception of it as the work of loners or social isolates. Hacking is about working together, meeting like-minded people and community. It is also closely associated with being an inventor, exploration and innovation, joy and 'hobbyism' (Himanen, 2001; Coleman, 2013). Hackers often do not view their activity as working but express passion through the practical hands-on involvement. It is often a central feature of their lives and not viewed by them as 'work'. Hacking has also become a political act, a philosophical form of critique and a business model.

More recently, popular interest in this positive and wider interpretation of hacking has expanded into popular consciousness and can be seen in a range of places. The history of computing and the role of 'good' hackers have been explored through film and literature with figures such as Steve Jobs, Mark Zuckerberg and Alan Turing receiving attention. There has also been an increased interest in more historical innovation from Leonardo Da Vinci to Victorian scientists such as Charles Babbage and Ada Lovelace. For a society in which computer networks have come to influence almost every aspect of life, there is a growing argument that we owe much of our daily lives to hacking and to hackers. This too, however, is quite a binary view of hacking and is not reflective of its true nature. Hacking, according to hackers at least, is neither good nor bad but simply a way of approaching the world which can be applied to a variety of more pragmatic motivations.

Hacking as a set of practices is now no longer simply related to computers or technology and, as a concept, it is now applied to a range of different activities.

We now talk about ‘life hacking’, hacking academia and music hack days. So too, the culture of hacking is also applied to things beyond computers; corporate conferences and websites have borrowed from and adopted its customs, imagery and language in an attempt to gain some form of legitimacy by association.

Hacking can therefore be viewed as a very complex practice and not easy to define. It is within this context that, more recently, the Civic Hacking movement has emerged in the past ten years. Hacking has always had a strong emphasis towards improving society. The original Hacker Ethic stated that computers could and should benefit society. This thesis argues that those involved in Civic Hacking apply this Hacker Ethic on both a global and local scale to create projects which aim to solve a range of social problems using technology and borrowing from hacking approaches and practices. These ‘problems’ can include crime; violence; humanitarian disasters such as tsunamis, famine or earthquakes; improvements needed to local government in terms of the democratic process or infrastructure, enabling healthcare, education or banking in remote areas; and involving local communities in issues and a range of other challenges which require solutions. Civic Hackers tend to approach these problems as a group project which, often, take the form of events called ‘hackathons’. During the event, teams select a challenge and then work together to solve the given problem, with a prize awarded to the ‘winning’ team. Civic Hackers also collaborate globally using online resources such as social media to share ideas. Civic Hacking tends to involve use of open-source computer programming or hardware building to create tools aimed at addressing these problems. The end product might be a web application, mobile application or a physical piece of technology.

This thesis explores the idea that Civic Hacking can be seen in the context of a wider societal change and builds upon theories developed by Christopher Kelty (2008). This change has taken place partly as a result of technological innovations such as mobile technologies, increased network connectivity and social technologies which have democratised the ability to develop certain hardware or software applications and made it easier and cheaper to coordinate activity globally. It has also been socially driven by a move towards the democratisation of information and an emphasis upon decentralisation, distribution and 'open-source' approaches to various aspects of life. Of particular relevance here are theories of network societies (Lovink, 2016; Wark, 2004; Castells, 2000; Fuchs, 2014). This influence of hacking can be seen in a range of spaces, and specific examples, including the rise of 'Web 2.0'; social media; the Arab Spring uprisings; the Occupy movement; the Clean Web movement; crowd sourcing; Wikipedia; the open data movement; CrossFit; 'maker' events; couch surfing; Freecycle; peer to peer music download; and crowd funding. This thesis seeks to explore the ways in which these disparate activities all express the Hacker Ethics. The central argument of this thesis is that these Hacker Ethics, and indeed hacking as a practice, was just an early example of these societal changes. Although it may also have influenced some of these social changes, hacking can also be seen as one example of this wider social change.

1.2 Research Aims

My motivation and rationale for choosing this subject for my PhD research originates with an interest in hacking in its more traditional definitions, particularly in relation to hacktivism. In the course of my initial research, however, I become aware that a small number of groups and events were associating themselves with the term hacking in a much more positive manner. This is a new form of hacking culture, the study of which will allow me to contribute to prior research in the social study of hacking. By increasing understanding these groups, I will be able to contextualise wider hacking practice and answer questions which would challenge some of these previous binary definitions of hacking.

From a research point of view, almost no studies have been carried out into the humanitarian applications of hacking previously and certainly no-one has explored Civic Hacking in an empirical manner. I also identify a significant research gap in relation to the study of hacking taking place outside Northern Europe and North America which I aim to address. On the other hand, there is a wealth of literature to draw upon which will assist me, particularly in relation to the Hacker Ethics and Network Societies.

Based on my conceptual framework, I identify the following research questions through which I hope to make a contribution to the existing body of work and which form the basis for my project;

1. What are the different types of groups involved in hacking for social good and how are they situated within the wider history of hacking as a culture and practice?
2. In what ways are the technological artefacts produced by Civic Hackers shaped by the ethics of these groups and wider social factors?
3. To what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?
4. To what extent are Civic Hackers indicative of the proliferation of the Hacker Ethic into wider areas of society?
5. What types of communities are formed by Civic Hacker groups?

1.3 Outline of the Thesis

This thesis is divided into a literature review, methodology, four empirical data chapters and a discussion and conclusions chapter.

The literature review is divided into two sections which each provide an analysis of relevant work conducted in this area to which this thesis makes a contribution. The first contains a definition of hacking as a non-technologically specific set of social practices by examining its evolution over time, the various forms it has taken and ways it has been represented. A primary focus of this section is upon an analysis of the Hacker Ethics concluding with the definition of hacking which I use in carrying out my research. The second section situates Civic Hacking within existing literature including theories of network societies, innovation and humanitarianism.

The methodology chapter provides a background to the research strategies and methodologies I employ in my project and a discussion of how I apply these methods within each data chapter. These methods include interviews and participant observation, informed by Ethnographic techniques, Social Network Analysis and Narrative Analysis.

The first empirical chapter presents my initial fieldwork carried out into Civic Hacking which I use to define the boundaries of my research project and the focus of my study by producing a typology of those involved in hacking for social good, based upon ‘portraits’, which I use going forward. This also allows me to address my research question regarding the different types of groups involved in hacking for social good.

The second empirical chapter describes the fieldwork which I carried out at a Civic Hacking event, Random Hacks of Kindness, held in Southampton during 2012. This chapter addresses my research questions regarding the ways in which technological artefacts produced by Civic Hackers are shaped by their ethics through interpretation of participant observations and interviews, both online and offline, focusing upon the technological artefacts produced at this event and the narratives told.

In the third empirical chapter I present the findings from Social Network Analysis on a Twitter hashtag relating to a particular Civic Hacking event called Hack4good. By examining the nature of this network and its ties and the motivations of those involved, this chapter addresses my research question regarding what kind of community Civic Hackers comprise.

The final empirical chapter presents research carried out online into the narrative themes and devices produced in relation to Civic Hacking, both by Civic Hackers themselves and by those outside this group. By doing so, I address my research question regarding the extent to which Civic Hackers focus on the democratisation of technology and whether Civic Hacking indicates a proliferation of the Hacker Ethics into wider areas of society.

Finally, this thesis concludes with a discussion of the main findings from my research, their significance and contribution in terms of the existing literature and the extent to which they enable me to answer my research questions.

Chapter 2

Conceptual Framework

2.1 Chapter Overview

In order to situate my own research contribution within the context of previous work into hacking, it is essential to provide a critical analysis of existing theoretical concepts and demonstrate its relevance to my own thesis. It is also important to explore the historiography of hacking and how my particular stance on this has informed my own research.

In the first section of this chapter, therefore, I will explore and contrast the work of various authors who have studied hacking from a social perspective. A primary starting position of my research was that hacking should not be defined within a binary and reductionist framing device and I shall contrast this against the theory which has portrayed the activity in this way and present a conceptual framework from which I approached Civic Hacking. I will propose that neither hackers nor hacking should not be labelled in terms of 'good and bad', 'criminal and non-criminal'. Instead, I argue that hacking should be viewed as a complex and heterogeneous set of non-technologically specific social practices based upon ethics including exploration, collaboration and modification and also associated with ideas related to liberalism, democracy and information freedom. Such ethics can be applied to a range of technologically and non-technologically focused groups. These ideas formed the basis for my key arguments that the Hacker Ethics are a fundamental part of the Civic Hacking community and beyond which are built upon in later empirical chapters, particularly in relation to the common values which form this community. As I shall discuss, some of these views are contested by those who take a more pragmatic view of hacking.

In Section Two, I shall explore theory which, I argue, presents ethnocentric, reductionist and technologically determinist definitions of hacking. This literature has positioned hackers as ‘outlaws on a digital frontier’ who conform to popular stereotypes of being male loners, ‘geeks’ and even criminals residing in the industrial cities of North America and Northern Europe. I will argue that such definitions have originated from the societies out of which hacking emerged but that they provide too narrow a definition of the activity. This provided a way to position my research thesis on Civic Hacking as a positive and diverse set of practices against the wider body of literature into hacking as a relatively stereotyped criminal activity.

In Section Three, I shall discuss a range of theories which cover the political aspects of hacking. By doing this I will both provide an overview of previous work and also provide an analysis which supported my definition of what I mean by the identifier ‘hacker’ and the practice of ‘hacking’ within my own research project. This will lay the groundwork for my own research into Civic Hackers as a group and demonstrate the academic context into which it contributed.

In Section Four, I will provide an overview of theories of information and network societies, highlighting some of their weaknesses and alternative stances, but also showing their relevance to the sociology of hacking and to this research project specifically. This will focus on the way in which theories of network societies may explain the unequal distribution of Information and Communications Technology (ICT) within and between societies, the significance of this inequality and how this went some way to explaining the activities of Civic Hackers described in later empirical chapters.

In Section Five, I will discuss the link between ICT4D (Information Communication Technology for Development) and theories of innovation, specifically lead user innovation and the parallels between this and the Hacker Ethic described previously which are explored through field research among the Civic Hacking community. I will also discuss the relationship between Civic Hacking and international policy.

Finally, in Section Six, I will explore literature which argues that this kind of technological innovation is inherently collaborative in nature, another key feature of hackers and the Civic Hacking communities upon which my research focused.

2.2 Part One: Definitions of Hacking

2.2.1 Introduction

What is 'hacking'? This question has been the subject of a great deal of sociological debate in recent years. Much of this theorising, as I shall demonstrate in this chapter, has been based upon popular media constructions and not evidenced by empirical research. In the first half of this chapter, I will provide a critical analysis of this literature and argue that there is an epistemological need to reframe definitions of hacking to reflect the complex groups in which it takes place, rather than reducing it to binary subject types referred to as hackers.

I will also suggest a need to look beyond ethnocentric definitions of hacking as a cultural practice which is grounded in the technocracies of the North Atlantic. I will evidence the fact that, central to the misconception within the literature on hacking, has been a 'folklore' of technology, perpetuated by the media and embedded in popular culture, which presents the hacker as an outlaw of cyberspace. While such imagery may have considerable rhetorical appeal, it provides little in the way of understanding regarding the contested nature of the term 'hacking'.

I will address this issue and provide a balanced definition of hacking which formed the basis of my research into Civic Hackers; that is, those who hack technology for ‘social good’ (Haywood, 2013).

It is important to acknowledge here that definitions are inherently subjective and so any attempt to define diverse groups such as hackers may give the impression of homogeneity of membership. In addition, I would argue that there is a risk of oversimplification involved in attempting to compare groups operating both within the North Atlantic and in developing world regions since all of those groups are arguably part of a globalised network society of IT professionals and influenced to some extent by western media. I will therefore not focus upon normative classifications of hackers but rather aim to provide a useful understanding of the variety and complexity of this subject and what I see as issues with some of the literature in this area. However, I felt that some form of evidence-based typology of hackers was required to bound my own research, and to specify the groups upon which that research would focus.

Historiography of Hacking

It is worth providing a brief overview of the historiography involved in the study of hacking. A comprehensive review of the study of hacking presents a gap within the existing body of literature which has yet to be addressed but would be worthy of future work. Where the historiography is relevant to contextualise core arguments and debates within this thesis, I have highlighted this within the sections that follow. Many of the early studies of hacking emerged from popular writing by journalists, novelists and bloggers such as Steven Levy (1984) and

Bruce Sterling (1992]). These were heavily informed by popular notions of hacking and, to some extent, still influence a utopian/dystopian dichotomy of hackers. Other work took the form of first-hand hacker accounts, such as those by Richard Stallman (2002), Eric Raymond (2000a), Dr. K (2004), The Mentor (1986) and Julian Assange (2012), and continued more recently by Anonymous (2013). These were often attempts to apply anthropological, political, economic and philosophical theory, admirably, but ultimately rather crudely. Only relatively later, was hacking picked up as a distinct topic by academic researchers. The starting point for these studies was often technological and papers emerged from IT departments, written from a technical perspective. Criminology was also an obvious focus and there were numerous attempts to apply traditional theory of crime, law and politics to this new technology-based activity. More recently, those in the fields of science and technology studies, and sociology, have applied their disciplines to the study of hacking, and increasingly with a focus from anthropologists using Ethnographic and emerging online methods, which have been influential.

2.2.2 Hacking as a Non-Technological Social Practice: The Hacker Ethics

This section defines hacking not as a subject type or personality trait, 'the hacker', but rather as a shifting set of social practices through which are expressed a set of ethics. As I shall show, these practices are not necessarily tied to computer technology and may not even be a modern phenomenon. Some important aspects of these Hacker Ethics will be considered which formed the basis of my research. My approach will be to trace hacking historically as a social practice in its various forms.

Hacking as a Non-Technological Social Practice

The story of hacking does not begin with the invention of the computer. It is possible to trace the history of technological inventions from the telegraph onwards and identify a parallel practice whereby technologies were modified by individuals to do something which they were not intended to do when first conceived (Winston, 1998). Although one should be careful not to take an evolutionary view of technology which views it as moving towards 'progress', the "talented tinkerers" (Webster, 2006; Bell, 1973) involved in these early modifications can be viewed as forerunners of a particular *approach* towards technology. I would argue that this approach can also be seen in the emergence of computer hacking.

Hacking often involves the re-appropriation of technology and the manipulation of it from its original purpose. Hackers hack to resist being technologically determined, and to contest and reform technologies so there are new determinations, to enact the sociality of technology (Jordan, 2008, p.14). In practical terms, the complex variety of computer hacking might involve the clandestine penetration of computer systems for theft or political goals; computer intrusion for commercial testing; the open hacking of Linux and Mozilla. In the literature, it has also been interpreted as a radical political philosophy, a pragmatist solution and a subculture, with a high degree of overlap between them (Alleyne, 2016).

For the early hackers at Massachusetts Institute of Technology (MIT), however, hacking was not confined to computer systems. They hacked campus vending machines and model railways. They broke into off-limit parts of the university and 'hacked' the official curriculum. Meetings became a kind of social hacking in which they 'hacked' their relationships (Levy, 1984).

As hacking is not confined to technology, it goes beyond computing to create new things in a wider sense (Jordan, 2008; Wark, 2004) and is about understanding, mediating (and exploiting) human relationships (Thomas, 2001). It includes a range of activities from modification of phone lines (Taylor, 1999) to carpentry (Himanen, 2001). Bruce Sterling points towards this concept of hacking as a practice which is not confined to technology when he states,

> *"...if Alexander Graham Bell had gone along with the rules of the Western Union telegraph company, there would have been no telephones. If Jobs and Wozniak had believed that IBM was the be all and end-all, there would have been no personal computers. If Benjamin Franklin and Thomas Jefferson had tried to 'work within the system', there would have been no United States. (Sterling, 1992, p.60)."*

These examples demonstrate the notion of hacking as a practice of re-appropriating both technological and non-technological processes. I would argue that this is vital to any attempt at exploring what a hacker is since it does not rely upon technologically determinist stances which have been widely discredited for being asocial (MacKenzie and Wajcman, 1999). I therefore adopted this approach within my own research into Civic Hacking.

Sterling belongs to a particular narrative in the study of hacking, one which has tended to be heavily US-focused, and somewhat narrow in its analysis. Inspection of these studies reveals some common themes, such as hackers being portrayed as rule breaking mavericks and references to the history of technology and liberalism. These views are indicative of a strand of work on hacking which emerged from science fiction, tech journalism and online blogging, before the subject of hacking was picked up in a serious way by academic writers. They can also be seen in more recent non-academic work such as 'Dreaming in Code' (Rosenberg, 2008) and 'The Soul of a New Machine' (Kidder, 2011). Often such accounts emerged from the hacking community itself, and have tended to emphasise a utopian or dystopian dichotomy within hacking, which will be explored in this chapter.

The portrayal of hacking as a practice which can exist in other areas as well as in computing is supported by some first-hand accounts. The wider motivations for hacking can be applied to a variety of counter-cultural groups from urban explorers (Dodge and Kitchen, 2006) to graffiti artists, electronic musicians and other art forms, in that they galvanise around the pushing of boundaries through exploration; artistic, societal, legal, spatial and technological. For this reason, it is worth considering whether hacking, as a set of practices, has in fact proliferated or migrated beyond technologically-specific practices, such as modifying code or network intrusion, and into wider fields such as space, art and academia.

One interesting example of the spread of hacking is the phenomenon of urban exploration, often referred to as 'place hacking 'or 'space hacking' (Garrett, 2011; 2012). This is an activity in which the participant explores inaccessible, abandoned and often 'off limits' buildings. It is worth noting that, as with computer hacking, MIT students have a tradition of urban exploration through roof and tunnel hacking, a practice closely linked to college pranks (Bender, 2011). This practice could be considered alongside computer hacking as enacting ideas regarding freedom of access (physical as well as informational), scepticism of authority and official rules, sharing and openness, and a sense of enjoyment in demonstrating their skill. A more technology-related form of hacking, and one closely related to Civic Hacking, can be found in the open data movement. This takes a number of different forms, including use of government data, collaborating on academic projects, or scientific research, but it always involves the use of freely available data to create technological solutions (Open Knowledge International 2017). Again, I would argue, this practice has much in common with the motivations of hacking.

While some of the practices associated with hacking were technology-specific, they were often never restricted to computer systems. Therefore, rather than viewing hacking as proliferating from a technological starting point, it might instead be more appropriate to consider computer hacking as one example of a wider set of practices. In other words, it may not be the case that computer hacking proliferated into other areas of society, but rather that computer hacking is one example of a wider societal change.

Increasingly, the term hacking is used to describe not only subculture activities but is also used in relation to the activities of typically mainstream groups. Use of the phrase 'to hack' has become commonplace when describing situations when the speaker or writer wishes to imply collaboration, openness or an unconventional nature. For example, a basic web search reveals the expressions 'Hacking Academia', 'Music Hack Day' and even 'Hacking Human Resources'. The use of the Hackathon format by mainstream event organisers, including within corporations, is also a good example of this adoption of hacking's particular approach to both "collapsing and recreating social/technological distinction outside the production of software or the manipulation of computers and networks." (Jordan, 2008, p.70).

Hacking, therefore, is not a purely technological activity but also a philosophical construct, although technology may be the instigator or the culmination of this philosophy. So, a particular piece of open-source software might result from an emphasis among a hacking community regarding collaboration and democracy, and could be regarded as the material outcome of these viewpoints.

I would argue, however, that the concept of hacking can also be used to support a relatively romanticised notion and it is therefore easy to see why it was picked up so readily by academic authors, as well as popular media, who have often portrayed hackers as historical heirs, the culmination of a long line of persecuted innovators. What these theories fail to do is explain just what it is that hackers have in common with these other innovators. They fail to address the question of what defines a hacker as a hacker and not, say, an inventor, a scientist or an IT professional. They also suggest a direct link between quite different historical groups, the Victorian technologists and modern computer hackers, separated by a great deal of time and social context. Attempting to define hackers as 'innovators' alone is just too vague and unbounded, and hacking risks becoming anything if we are not careful (Jordan, 2008).

If we consider the above-mentioned practice of urban exploration and the open data movement, they have something in common in that they are all involved in 'acting out' a set of ethics which bear close similarities to those related to computer hacking. In terms of a comparative definition of hacking, I believe that practices such as these should therefore be considered as a type of hacking since they are motivated by similar approaches. These practices are reflective of a wider shift towards informational democracy, as I will discuss in Part Two of this chapter.

But do the above examples, urban exploration or open data, *really* constitute hacking? I would argue that they may be examples where the lexicon and culture of hacking has been appropriated in order to gain legitimacy in the eyes of a society which increasingly demonstrates an interest in hackers and the history of technological innovation. These examples are important since they take a non-technologically determinist stance. They suggest that hacking is not restricted to computers, therefore computer hacking may be one example of a wider ethic which will be explored later. This has implications for my own thesis since Civic Hacking could be seen as another example of this since many Civic Hacking activities are also non-technological. By exploring Civic Hacking within my own PhD research, I intended to gain an empirical understanding of whether we should consider some of the groups described above as 'hackers', in what sense and whether they are indicative of a social shift in which wider groups are adopting these practices.

The Hacker Ethics

If hacking is not to be viewed as a purely technological act, what might be a better way of understanding this practice? The Hacker Ethics present a useful notion in understanding why the practices of hacking feature in areas beyond computing, and one which has informed my own research (Levy, 1984; Himanen, 2001). Rather than viewing hacking as an activity which is the result of technology, this approach interprets hacking as the construct and performance of a set of ethics, ethics which go beyond technology into wider aspects of society (Kelty, 2008).

Since discussions of Hacker Ethics build upon existing work on ethics and technology, at this point it is also worth briefly considering the wider body of work on ethics more generally and particularly in relation to technology design. Discussions of ethics and technology is not new, having been debated from ancient Greece to the industrial revolution (Luppicini, 2008). In fact, it is widely accepted that as the influence of technology on society grows, the ethical issues increase (Moore, 1985). More recently, however, the notion of 'technoethics' has been developed, a field which specifically considers the ethical implications of technology and the responsibilities of those involved in its production and use (Bunge, 1977). This approach places emphasis on the duty of the technologist and argues that one cannot separate their moral responsibility as a person from their invention. Technologists are subject to a range of conflicting demands including the desires for profit or innovation, however, they are relatively unconstrained by external codes set out by governing bodies (Galvan, 2003). 'Technoethics' has been developed in recent years to promote and encourage this ethical approach to technology design, one in which the practitioner should control the way their design acts upon the world, rather than remain a morally ambivalent bystander. There is a choice, says Findeli (1994), and an attitude when it comes to designing a piece of technology. One can choose a "moral way" rather than a technological way. Rather than blindly approaching as a set of technological solutions and needs, it is essential to consider that these solutions to particular spheres may in fact create problems for others. It is certainly possible to see a link between this approach towards technological design and the ethics of hacking. As I shall explore later, ethics are a key feature of the communities formed by Civic Hackers. As technology becomes a more ingrained feature of our lives the distinction between technically related ethics and other kinds of ethics becomes less (Johnson, 1985). Therefore, Hacker Ethics could also be viewed as simply ethics, less specific to the particular technology of hacking.

This aligns with my research interest on Civic Hacking and my inference that the ethics of hacking could be seen in wider areas of society beyond computing.

The study of hacking has developed considerably in recent years, therefore it is important to explore the different ways in which the ethics of hacking have been problematised by different authors since they were first proposed as a concept. Steven Levy (1984) provides us with an early and influential discussion of hacker culture, and it is from his description of the MIT computing labs of the 1960s that much of the popular study of hacking as a construct emerged, including the original notion of a Hacker Ethic. Levy explains that 'hack' as a term associated with computing may have emerged from MIT college 'lingo' used to describe an elaborate college prank. As Levy says "to qualify as a hack, the feat must be imbued with innovation, style, and technical virtuosity" (Levy, 1984, p.23).

Levy summarises these ethics as the following;

- Sharing
- Openness
- Decentralisation
- Free access to computers
- World Improvement

He also describes the following aspects of the Hacker Ethic which were "silently agreed upon" by these early hackers;

- Access to computers –and anything which might teach you something about the way the world works – should be unlimited and total;
- All information should be free;
- Mistrust authority – promote decentralisation;
- Hackers should be judged by their hacking, not bogus criteria such as degree, age, race or position;
- You can create art and beauty on a computer;
- Computers can change your life for the better.

However, I would argue that Levy's use of the term 'ethic' in the literature is rather simplistic in that it implies that hackers only have one shared ethic, when, in fact, there are a number of different and less well defined ethics involved (Coleman, 2013). Levy's descriptor somewhat clouds the complex reality of hacking which in reality comprises a wide range of participants, activities and motivations. It might be better, I would argue, to refer instead to Hacker Ethics, as a plural, since this covers the range of approaches identified in the literature (Jordan, 2008; Levy, 1984; Himanen, 2001; Kelty, 2008; Coleman and Golub, 2008). While Levy's account describes a time when the ethics of hackers were unspoken and undebated, Coleman and Golub (2008) suggests that they quickly became a self-aware and critical group, with large numbers of hacker manifestos being written down. Therefore, while Levy's work is influential, things have certainly moved on, and rather than comprising a unified set of values, the Hacker Ethics are now interpreted as "more of a mosaic of interconnected but at times divergent ethical principles" and therefore should not be treated as a single code (Coleman, 2013: p18-19). Chadwick (2006) also considers that the idea of a single community of hackers with a shared common culture is not reality. Levy is quite technologically determinist in his approach as he suggests that emerging computer technologies were the primary factor in shaping hackers as a group (1984). It is worth noting that Levy also represents the tradition of popular journalistic writing on hacking which, while useful, is often rather simplistic in its portrayals.

There are, however, a number of other researchers who have subsequently sought to position the Hacker Ethics as being related to an approach towards the world rather than a set of defined rules. Pekka Himanen (2001; 2009), for example, takes a different approach from Levy in attempting to articulate a 'hacker work ethic', which is heavily influenced by the writing of Manual Castells. He focuses on the attitudes of hackers towards their 'work'. According to Himanen, hackers are defined by qualities such as playfulness, caring, exploration, passion, entertainment, interest, joy and enthusiasm, which casts the Hacker Ethic in opposition to Max Weber's influential 'Protestant Work Ethic'. Weber (2001) argued that a shift occurred in values with regards to division of work and leisure time when Capitalism emerged in Northern Europe during the 1800s, the earning of money as a primary motivation and the rejection of working for works sake. Weber attributed this emergence to what he called the 'Protestant Work Ethic'. Himanen describes the Hacker Ethic, in contrast, as "turning Sunday into another Friday". That is, the centralisation of work among hackers means that work becomes an end in itself and there is less separation between 'work time' and 'leisure time'. Rather they become one and the same thing. Drawing upon first hand testimonies by a range of hackers, he argues that hackers are motivated by “passion”, “joy” and “happiness” of work which is not found within the Protestant Ethic. Himanen goes as far as to argue that this Hacker Ethic is spreading from hackers into wider society, influencing the ways in which wider society operates. Himanen also aligns hacking with the Aristotelian concept of ‘virtue ethics’ which focuses upon the character of the individual rather than the moral outcome of their decisions. This places less emphasis upon external laws or the results of a person’s ethical choices and more on what is considered virtuous when deciding what is ethical. I would argue however, that such notions are culturally variable rather than universally applicable (1999). It might be argued that Himanen’s Hacker Ethic is based upon a set of rigid and subjective virtues with little consideration of how they might vary within a different context. For example, those within different geographical or social contexts might well approach hacking in a different way from those described by Himanen. This was something I was keen to explore further through my own research project.

Like Himanen, McKenzie Wark is also one of a series of researchers who have attempted to interpret hacking and free software in terms of traditional grand theory and macro theories of network societies. Wark (2004) differs from Himanen, however, in that he views hackers as a Marxist “revolutionary class” of the network society. He positions hackers as engaged in a struggle against the ruling class, in contrast to Himanen’s view of hackers as the positive, business-minded cornerstone of the network society, and he accuses Himanen of aiding the ruling class by obfuscating the exploitations of the network society.

Much of the research into hacking takes a particular stance, one which is both positive and somewhat idealistic about the purpose and potential of hacking (Stallman, 2002; Coleman and Blumler, 2009; Shulman, 2005). It is interesting to consider that this contrasts with the significant media and public focus on hacking as a criminal or deviant act, as described later, although no more accurate. The Hacker Ethics might be compared to the "the hard work of freedom" (Coleman, 2013: p210), freedom not just based on the right to free speech but also unalienated labour, the right to work and produce. While there is some evidence that the "fun" of hacking motivates hackers rather than earning a living (Torvalds and Diamond, 2011) and that hackers are "only weakly motivated by conventional rewards such as social approval or money" (Jargon File, 2007), we should not see this 'pure' pleasure of work, free from politics, focused on the practice of hacking for its own sake, however, as somehow more authentic as opposed to liberalism as an ideological veneer (Coleman, 2013: p15).

Sherry Turkle generally takes a more dystopian view of the impact of technology on society, however, even Turkle could also be seen as buying into this more idealistic notion of hacking (2005). When studying the hackers at MIT in the early 1980s, she argued that they created "a mode of production different from the standard, a mode of production built on a passionate involvement…". This "hacker style work" involved loyalty only to the project not to hierarchy, which has been highly influential on the development of computing since much of the technology involved has been built by open source communities using this approach. This approach to work is also described by Kidder (2011) in 'The Soul of a New Machine', where the author explored the idea that hackers are not motivated by “ego and money”. It is worth noting, however, that both Turkle (2007) and Coleman (2013) also describe the *humour* of hacking so we should not consider it only an intellectually serious pursuit. Since its early days at MIT, hacking has always possessed a comedic streak.

Much of the literature on hacking cited above, however, provides little in the way of critical analysis as to whether hacking has an inherent ethic of hard work or why this might be the case. There is no counter view or attempt to balance this discussion of work ethics against an empirical reality which is presumably less binary (Kelty, 2008) and which I intended to explore through my research. Nor any acknowledgment that a particular narrative may be at play within this literature when positioning hackers as genuinely harder working or more passionate than other groups, a narrative which positions hacking as somewhat idealistic. In contrast with the view of hacking as being defined by a work ethic, it is worth nothing that there is also a perception that various forms of online protest and activism are somehow ‘lazy’ or require less effort, so-called slacktivism (Morozov, 2009; Franklin, 2014). These arguments will be explored in more detail later (Section 2.2.4 on hacktivism).

The enthusiastic notions of ethic in relation to technology described above are not a recent phenomenon. As early as 1995, Barbrook and Cameron produced a scathing critique of what they saw as the hypocritical nature of the information age. In ‘The Californian Ideology’ (1995), they argued that a “hybrid orthodoxy” has been created for the information society, based upon a fusion between the “free-wheeling spirit of the hippies and the entrepreneurial zeal of the yuppies”.

While this orthodoxy referenced Jeffersonian liberalism, the authors argued that it was been corrupted by entrepreneurial individualism and was, in fact, largely facilitated by state funding. Instead of openly rebelling against the system, this “virtual class”, comprising of skilled high-tech entrepreneurs, accepted the notion that individual freedom can only be achieved by working within the free market and began to drift towards the right. This allowed them to enjoy the cultural freedom and wealth created by this system while avoiding the fact that it is not equally distributed and based upon profound contradiction. The deprived only participate in the information society by providing cheap labour, a type of slavery. Members of the virtual class meanwhile “can play at being cyberpunks without having to interact with their impoverished neighbours”. This has corrupted the idea (albeit technologically determinist) that technology has the potential to emancipate from monopolies and instead has increased social polarisation, segregation, oppression and dominance. Similarly, Paul Edwards provides us with a more dystopian view of the development of computing in The Closed World (1996). Edwards describes how the social and cultural context within which computing emerged during the Cold War, led to the shaping of these technologies as political and military tools.

From these perspectives, it could be argued that notions of the Hacker Ethics need re-examining more critically against both empirical data and also a wider, more complex reality in which hacking has been shaped by a variety of contrasting influences beyond hackers. Some of the dominant stances within the literature on hacking appear quite utopian (Turner, 2006). There is a strand of thinking which runs through the study of hacking since its early years which portrays them as a somehow purely ethical or ideological group. It seems unlikely, however, that this should be any more factual than the portrayal of them as deviants or villains which I will describe later. It seems that there is a need to adopt a more realistic approach to the study of hacking which acknowledges that this is simply a set of socially shaped practices which can be applied within various different contexts. In Cypherpunks (Assange et al, 2012), the authors convey the idea of 'pure' hacking, the 'original' hackers before they were corrupted by corporations such as Google and Facebook. They argue that these hackers have a responsibility to help citizens through their hacking, to change the world, to empower people, to stand up against governments to take back power, to topple dictators and to correct false facts by politicians (Assange et al, 2012, pp.67-71). It is important to acknowledge that these authors are likely to have a particular bias and to adopt similar caution with their writing as one might with, for example, Richard Stallman. So, while the idea of Hacker Ethics are formative to my own research, it is important not to allow these idealistic or romanticised notions of hacking to dominate.

So what framing device might be of more use to understanding hacking within my own research project? An alternative approach might be not to label or classify hackers but rather explore further the ways in which those involved in hacking themselves self-identify. Although the study of self-affiliation as a concept is a significant topic in contemporary social science (Barnard, 2000), it is underused within the literature on hacking. It might be argued that this is because first-hand accounts of hacking more often tend to be journalistic accounts of criminal hacking and Ethnographic encounters can be difficult to facilitate (Alleyne, 2016; Glenny, 2011). In reality, there is a body of literature to demonstrate that identity generally is relatively fluid or plural (Sokefeld, 1999) and that the imposition of classifications can have a performative effect (Bowker and Star, 2000; Rabinow, 1984).

The Ideology and Pragmatism of Hacking - Free and Open Source Hacking

Another aspect which can be used to explore hacking is a relationship between hacking and notions of informational freedom and equal access to technology (Soderberg, 2007). This also had relevance to my study of Civic Hackers since this was a central point in their views and activities. Computer hackers have always placed a great deal of emphasis upon liberalist philosophy and an emphasis on intellectual property rights and concepts of free speech (Coleman and Golub, 2008; 2004). I would suggest, however, that this may be culturally variable and the philosophy which informs hackers in the US may differ from parts of Europe or other regions of the world, although this is an under researched area (Alberts and Oldenziel, 2014). It would also argue that such liberalist philosophies do not consist of a defined or coherent group of ideas but rather as an often conflicting and constantly shifting set of philosophies, (Coleman and Golub, 2008). It is important to establish that these views are not a singular set of fixed ideas but rather something ephemeral and constantly shifting. This is significant when contrasted against the literature which seeks to categorise hackers as a singular and homogeneous group, as I shall demonstrate later.

Defining what ideals makes someone a hacker is a popular topic of dialogue among hackers themselves (Mizrach, 2009) with a high degree of online and 'real world' debate taking place, something which I was keen to explore through my own study of Civic Hacker narratives. In fact, the degree of self-awareness of such debates among hackers has led some authors to suggest that hacking has itself become a practice around which social critique can take place (Goode, 2015).

The relationship between notions of freedom and hacking can be witnessed throughout many activities including the politics of open source software, peer-to-peer file sharing and denial of service. As I will demonstrate later, hackers have often been portrayed in the literature as nihilistic criminals who lack any kind of morals (Alleyne, 2016; O'Neil, 2006). This has produced an image of hackers which is too simplistic in nature and which may obscure the cultural significance of this group. This binary situates hackers as, on the one hand criminal, and on the other, as "heroes of the computer revolution" (Levy, 1984). A more powerful device would involve treating hackers as a heterogeneous set of individuals, a view which informs my own research approach.

In some ways, I would argue, the liberalism associated with hacking is indicative of the fact that hacking has always had the potential to be somewhat political. By this I mean that if we accept that the historical origins of hacking were informed by a sense of moral right and wrong regarding access to information, then the act of hacking is likely to become, under particular circumstances, a political act (Coleman and Golub, 2008). So, it is not surprising that the most recent manifestations of hacking, described later, involve the marriage of technology and overtly activist activities. For example, hacks against organisations which are seen to oppose peer-to-peer file sharing, which I shall discuss in more detail in my discussion of 'hacktivism' at Section Four.

This liberalism has been strongly linked to Free and Open-Source (FOSS) software hacking. Within about thirty years of the original MIT hackers, the FOSS hacking movement had grown into a self-aware collection of communities which formed around particular software products such as Linux. Open source software is computer software which is licensed so that anyone can use, copy and change its code and FOSS hackers are involved in modifying this code. Many definitions of hacking come from 'cracking' which differs in its values from the open source community (Jordan, 2008, p.10) so it is certainly worth focusing attention on these communities in order to construct a more rounded typology of hacking.

Hacking as a Gift Society

In order to address the question of *why* hackers volunteer large amounts of their time and resources for these open source projects, we might draw upon the concept of a 'gift society' (Raymond, 2000b; Soderberg, 2007). The idea of '*the gift*' has been an important sociological and anthropological concept from early Ethnographic texts (Mauss, 1954; Malinowski, 2014). A gift is based upon some promise of future reciprocal return, whether material or symbolic (Wiener, 1988). For hackers, researchers have found that motivations included the pleasure of taking part, sharing of links or the increased reputation within that community gained through contribution (Kleinknecht, 2003; Kelty, 2008). In internet communities generally, both Kollock (1999) and Rheingold (1993) describe virtual 'communities' of relative strangers in which this 'gift' will be repaid by some member of the wider group, not necessarily the direct individual who was initially the recipient. The 'cultural capital' (Bourdieu, 1991) which emanates from such symbolic exchanges can be viewed as important in forming and strengthening the ties within these communities, however weak those ties might be.

It is possible therefore to explore hacking in the light of this corpus of literature, as virtual groups or communities (Nycyk, 2010) who form not just around technologies but which share similar ideologies regarding informational liberalism and in turn shape those technologies accordingly. These studies often have basis in sociology and anthropology and make use of online techniques like virtual Ethnography, social network analysis, hyperlink analysis, blending of traditional and emergent techniques to try and understand what draws communities together online. A particular focus for my research was on what brought these Civic Hacker communities together to form interaction between diverse people who have in common a "mania" for machines and software (Jordan and Taylor, 1998). However, it was important not to assume that hacking or technology were the primary motivation behind this since Jordan cautions that "Hacking needs to be defined by a series of commonly enacted interactions or material practices which both create and wrap around hacking techniques….The hack (and crack) remain the central material practices but a range of other factors need to be recognised as a basis for a community, without which individual hacks would remain just that…" (2008 pp.66-70).

On the other hand, defining online communities can be complicated and, as with other 'cyber-communities' (Kozinets, 2010; Webb, 2001), there is little in the way of empirical research to demonstrate a wider hacking community, unified by shared values or other commonalities. Instead, it is more useful to consider these groups as 'weak' (Granovetter, 1973) networks of networks, in some ways reflective of the internet itself (Castells, 2001) or as a 'community of interests' (Seymour-Smith, 1986, p.46). Kleinknecht (2003, p.113) found that those involved in hacking described their groups as 'communities of knowledge' in which sharing is emphasised, although he also found that gaining access to this knowledge required the hacker to abide by certain informal rules.

Barbrook also describes this concept in 'The Hi-Tech Gift Economy' (2005) and argues that, rather than being an inherent compromise between free market economy and anarcho-communism, the same piece of information can exist online as both commodity and gift. While in a traditional Gift Society, gifts are given on the basis that they will be returned in the future, online this is less likely since the giver may never meet that person again. However, the assumption is made that they will be reimbursed at some point in the future by someone within that community, not necessarily the individual in question (Kollock, 1999). Rheingold (1993) also described 'virtual communities' on the Usenet internet forum in which the gift is a central notion. In some ways building upon concepts originally proposed in Benedict Anderson's 'Imagined Communities' (Anderson, 2006; Ziegler, 2002), the concept of virtual communities has been expanded over the years to encompass 'Communities of Interest', 'Communities of Knowledge' and 'Communities of Practice'. In terms of overall concept, a virtual or imagined community seems relevant to hacking communities. It is a community in which members have often never met in person and transcend physical boundaries (Smith and Kollock, 2001). It is also a group of individuals who are drawn together by a common set of shared interests. In particular, the concept of Communities of Interest seemed relevant to my own research since hackers are likely to have some shared interests in common.

The gift as '*présentation totales'* (Mauss, 1954), a symbolic embodiment of the values of that community. Henri and Pudelko (2003) describe the various typologies of virtual communities in terms of three social contexts; the goals of the community, the methods of initial creation, and the evolution of its goals and methods. For Dan McQuillan (2012), rather than focusing on the type of horizontal or decentralised networks which hackers may comprise, we should instead explore their "circulations, their tempos and their transmutations…what Kathleen Stewart describes as an atmosphere".

Of course, in reality a community is often a combination of different models – it may be part 'Community of Interest' (Seymour-Smith, 1986) and part 'Community of Practice' (Lueg, 2001). It is important to consider where the emphasis lies within that group; what is their core purpose. I would contend that hackers are in fact more closely aligned to what Moon (1993) calls a 'Moral Community',

> *"A society in which social interactions and relationships are governed by principles that are freely accepted by the parties to the relationship." (Moon, 1993, p.14)*

Some caution is required when attempting to apply these social science theories to hacking in a relatively simplistic manner. On the other hand, these approaches to the hacking do provide useful models with which to engage in empirical studies. There is a value to exploring what it is that hackers have in common, and what aspects bring them together. They can also be particularly useful due to the complex informational networks within which these groups exist.

Pragmatic vs Ideological Views of Hacking

A particular view of hacking has been highly influenced by another hacker turned writer, Eric Raymond. In his study 'The Cathedral and the Bazaar' (1999), Raymond explores the practicalities of this philosophy which encompasses any software whereby the code is open to modify and free to obtain. Proponents of open-source such as Raymond promote both the technical and ideological aspects of this system, what he describes as a "bazaar" in which many programmers around the world work to modify and debug software. This is contrasted against the "cathedral building" of traditional corporate software which might be viewed as quite individualistic in nature and based upon the idea of owned property rights. On the other hand, open source communities are relatively selective about their membership which restricts the availability of expertise (Weber, 2004) which therefore goes against Raymond's view that resources are plentiful within an open source setting.

This approach provides us with a useful vision of hacking, and one which is more pragmatic and realistic than crackers or free software activists. However, this still creates something of an artificial contrast between hackers who 'play by the system' and those who do not. It also relies upon relatively outdated anthropological modes which may be accurate, but are not subject to empirical scrutiny, an issue I aim to address through my own research.

Despite proposing a community based upon morals and ethics, it is also worth analysing the argument that this does not consider how hackers can subsist in practical terms from their activities. Geert Lovink (2016) suggests that many 'free culture' proponents ignore how artists are meant to make a living in the information age. He argues that corporations have grown rich on the "rip and burn" slogan but that many of the above authors do not examine the issue of paying for cultural production. He criticises free software proponents such as Yochai Benkler (2011) for failing to address who benefits financially from the 'wealth of networks'. Similarly, although hackers may see work and play as the same thing, they must also subsist somehow (Soderberg, 2007). There is a contradiction in stating that short-term freelance work is exploitation whilst also praising the freedom of individual creative workers. Indeed, even Lawrence Lessig (2001) has celebrated the rise of creative amateurs while also pointing out that the blurring of work and play also leads to exploitation. Companies such as

Huffington and Facebook cash in fortunes on the back of volunteered time, monetising open data while it is rare for revenues to be distributed among those who produce the content. Free culture projects such as Wikipedia can be effective but often offer no practical model for sustaining creative labour.

If Eric Raymond represented the pragmatic, cost-efficient, pro-business approach of the 1990s Dot Com boom, then a more idealistic branch of Free and Open Source hacking was advocated by Richard Stallman (2002). Stallman, also an example of a first-hand hacker account, developed the Free Software Foundation during the 1980s, heavily influenced by libertarian philosophy and an ethic that 'information should be free' (Moody, 2002). Eric Raymond differed significantly from Stallman in that he saw open source as a good business model and sought to work *alongside* corporate IT to a greater extent, while Stallman held strong ideologies which distanced him from mainstream IT, engaging instead with anti-copyright ('*copyleft*') activism and the creation of the GNU General Public License (GPL) as an alternative to mainstream copyright law (Kelty, 2008). Levy (1984, p.314) refers to Stallman as the 'last of the true hackers' in that he fits more closely with the original Hacker Ethic while arguing that other hackers 'gave up on' these ethics to work for mainstream companies. This alleged split in the hacker movement between those who politicised hacking and those who took at more pragmatic approach ultimately led to the appropriation of the FOSS movement by corporations and, Soderberg argues, this practical approach by some hackers may explain their success (Soderberg, 2007). All of these accounts fit the narrative of a dichotomy within hacking in which some hackers worked 'within the system' and changed it while others fought against it. None of these arguments, meanwhile, consider the impact of wider societal changes upon hacking and the possibility that the technology of hacking may not in fact be the determining factor at all. Instead, I would argue that computer hacking is indicative of wider changes in society which I shall discuss later.

Corporations such as Apple, IBM and Microsoft have at least some roots in this Hacker Ethic of free information (Goode, 2015). The founders of Apple, Jobs and Wozniak, began their careers distributing 'blue boxes' (Chandler, 1996, p.231) which allowed free phone calls to be made by hacking dial tones ('*phreaking*') and Bill Gates started his career in the same 'Homebrew Computer Club' as Stallman, Wozniak and other hackers (Isaacson, 2014). As I shall discuss below, the division between what is considered 'legitimate' IT innovation and what is considered 'hacking' is often less than clear cut, and frequently subject to the influence and interpretation of media and popular culture. I would argue that this makes any definition of hackers which is based upon their criminality relatively problematic.

This debate between Raymond and Stallman has been much discussed, however, I would argue that its relevance to contemporary studies of hacking is somewhat limited. There is no rationale for why hacking as a practice need be either ideological or practical and why, in fact, it cannot be both. I would argue that we should take a more realistic and practical approach to the study of hacking, one in which it is neither good nor bad, practical nor idealistic, but instead focus on the complex realities of these practices and their relevance to society. This approach has implications for my own research and forms a core argument since the groups involved in Civic Hacking have as a core purpose a desire to address social problems and have often been framed in contrast to 'bad hackers' by the media.

A more pragmatic approach may be to infer that, rather than disappearing, these hackers instead carried the Hacker Ethics with them into what became the mainstream IT industry. Kelty (2008), for example, presents a different notion of the Hacker Ethic to Levy, exploring the more pragmatic approach to open source hacking through a small open source software company in the US which aimed to provide services to the health care system. He argues that this organisation engaged with a spirit of breaking rules, science and progress, innovation, scepticism and critique for the good of society not just individual gain (Kelty, 2008, pp.81-85). Kelty links this spirit to that of Enlightenment philosophy involved with progress and also cost saving pragmatism in the public sphere (2008, pp.64-65). Although Levy (1984) also covers the idea that hacking should be in the public interest, he does not place it as firmly at the centre of his Hacker Ethic. It is significant that Kelty does not engage in repeating well-known stories about the 1998 schism between the business minded open source faction around Eric Raymond and the religious free software fighters, led by Richard Stallman (Lovink, 2017). Instead, openness becomes also a means to achieve something, a way of working, rather than an end goal in itself.

Again, it is worth noting that, to date, the open source movement has tended to be confined to mainly post-capitalist network societies involving a high proportion of North Atlantic-based males (Gozukele, 2006). Kelty's argument is indicative of a social movement, founded in the libertarian politics and political philosophy of Northern Europe and North America. According to the author, the open source movement provides a means of conceptualising 'openness' grounded in participation, democracy, sharing and collaboration which could well be applied to more recent ICT developments including wikis and peer-to-peer music downloads. Kelty's idea of Enlightenment, however, is another example of the North Atlantic dominance in hacker literature and Kelty fails to consider how the philosophies in countries outside this region might have influenced the politics of hackers in them.

Historically, Open Source projects, and hacking generally, were largely confined to those societies which had access to technologies whether through money or knowledge. This has meant that those involved were largely confined to the middle classes, based in North America or Europe and were educated males, an image that has come to shape the popular image of the hacker as well as hackers' own dominant narratives. Since those involved in hacking have not been those who 'needed' to gain access to technology or save money by hacking networks or modifying code, it does not seem likely that these were their motivations.

Recent literature, however, suggests that the '*pragmatism*' of hacking may be increasing as it is seen as a practical approach to saving costs and increasing access to information or ICT (Gitau and Donner, 2010). This can be seen in a range of issues from the adoption of FOSS by South American governments (Chan, 2004; Fernandez-Ardevol and Ros, 2009) to international development

(FrontlineSMS, 2010; Walton and Donner, 2011) to hardware hacking innovation in Africa (Ekine, 2010; Castells, et al 2007; Hersman, 2015; Fardon, R. et al, 1999). Sun et al (2015) provide a study of DIY 'making' among elderly electronic hackers in China in which they argue that this practice is deeply tied to the participants' relationship with their culturally constructed imaginings of class and citizenship. It is interesting to note that such studies reveal the ethnocentric nature of most portrayals of hackers.

I would suggest that this is indicative of the fact that open-source hacking projects are starting to move into areas of the world beyond the North Atlantic and to individuals outside the hackers of popular narrative. There has until recently, however, been little literature on this area and further empirical research would be required to establish this, to explore to what extent it is due to the *pragmatism* or *politics* of open source and, if so, demonstrate how this differs from previous interpretations.

This distinction of pragmatic hacking might seem to suggest that the other types of hacking represent 'hacking for the sake of hacking' while the examples of hacking in developing regions are of 'hacking for need', and that the two concepts are quite separate. In reality, however, the picture is more complex. As I will discuss later, many of those involved in forms of what might be described as pragmatic 'hacking' such as ICT4D projects and Civic Hacking originate from wealthy and educated backgrounds. Often those involved in this pragmatic hacking are not themselves in 'need' but rather trying to develop solutions on behalf of those without the resources to do so. On the other hand, as access to training or cheap technology increases, a growing number of those hackers involved in humanitarian work no longer come from these backgrounds. Within my own research, I was keen to explore this among those involved in hardware hacking and innovation within developing regions and, in particular, the Civic Hacking movement.

In addition, there is a question regarding whether anyone really *needs* to engage in hacking. This need could be seen as a relative concept. The needs of these Civic Hackers in wealthy societies are relative to their circumstances and differ from those in total poverty – both digital and economic. Civic Hacking could be seen as a luxury, a 'nice to have', but is also pragmatic as it can be about saving money or giving access to those without – this can be more or less of a need depending on the particular project. For example, a Civic Hacking project aimed at improving parking in Boston is, arguably, relatively less significant than one aimed at reducing disease or extreme violence. However, as evidenced by government initiatives, access to affordable technology is increasingly seen as a 'need', in some ways it is as necessary as education or electricity. It is also worth considering the emergence of hacktivism outside Europe and North America in this debate. If access to internet and technologies is considered a need in this way, would the activity of groups involved in organising safe internet access in the Middle East ('Arab Spring') and China be grouped under the same category of 'hacking for need'? In such cases, the need may not be economic but rather political or cultural.

Hacking's Influence on the Wider World

A key debate which I have identified and which informed my own research thesis comes from contrasting the work of Kelty and Coleman, interestingly both US-based social anthropologists involved in the study of hacking. These authors both represent a particular approach to the study of hacking which has emerged from the social sciences with a particular emphasis upon applying Ethnographic techniques and contemporary anthropological epistemology to hackers.

Kelty has argued that open source hackers did not produce an ethic but rather that *hacking* itself is the practical response to a previously existing historical problem. He describes that problem as regarding legitimate means for the production of knowledge (Kelty, 2008, p.306). By this, Kelty is referring to the challenge of democratising information through activities such as open data projects and 'crowd sourcing' (Shirky, 2008). In other words, these hackers were concerned with dispersing control of information into wider areas of society who did not traditionally have this kind of access. According to Kelty, this philosophy was not simply the result of technologies such as computers or the internet but was also facilitated due to the opportunities provided by easier access to data. As I shall discuss later, however, despite the promises of informational democratisation offered by open source technology, there remains a debate over the extent to which this has really occurred or whether technology merely increases the divides and inequalities already present in societies.

For Kelty, software such as UNIX does not form part of a separate 'Gift Economy' situated outside the commercial market but instead he argues that markets have been shaped by and in response to open source philosophy (Kelty, 2008, pp. 307-308). Kelty suggests that Richard Stallman failed to recognise open source as a pragmatic market itself, as Eric Raymond did, but rather focused on it being a human right or philosophy regarding the freedom of information (Kelty, 2008, p308). This is significant since this employs a non-technologically determinist stance towards hacking, instead viewing it as a social construction and part of a wider cultural trend. Kelty also refuses to engage in the kind of binary debates which have often defined studies of hacking, on the one hand utopian and the other deviant.

However, if we are to accept Kelty's claim that a Hacker Ethic has been instrumental in shaping wider societal norms, then he fails to address why they have been cast in opposition to this society. This is the kind of binary distinction which, I would argue, has helped create a myth of hackers as a subculture versus mainstream society. It might be argued that the FOSS model is being co-opted and commodified by big business in the same way as sub-cultures or street-art and that resistance must take the form of subversion from within the system rather than confrontation (Shy, 2001).

There is a distinction to be made, however, between Kelty's interpretation of hacking as a product of the world and Coleman's view of hacking as influencing the world around it. Kelty's approach takes a pragmatic approach, with hacking an integral part of a wider world, while Coleman presents hacking as more idealistic, with hackers existing somewhat within the ‘bubble’ of a distinct ‘world view’. The former, a more realistic angle on hackers as needing to be neither wholly pragmatic nor ideological. This debate will form an important starting point for my own research into Civic Hacking as it relates to wider social movements. In ‘Coding Freedom: The Ethics and Aesthetics of Hacking’ (2013), Gabriella Coleman conducted Ethnographic research among open source hackers and concludes that this movement which initially focused around a technical craft to ensure software freedom has helped catalyse broader political and economic transformations. This view differs from that of Kelty in that Coleman argues that hacking’s role in transforming other arenas of life is “not primarily rooted in the power of language or the discursive articulation of broad political vision” but is instead a politics of critique which provides a practical, living counterexample to mainstream corporate IT development (Coleman, 2013, p.185). In other words, it offers a “practical revolution” which is based upon proof of concept that economic incentives are unnecessary to secure creative output (Coleman, 2013, p185). So rather than viewing hacking as being shaped by wider social trends, Coleman positions hackers as the key influencers in these social changes. While this view may not be wholly without a basis in reality, it is certainly limited in its acknowledgement that the ethic of free software and wider, pragmatic, influence of mainstream IT need not be mutually exclusive. This also carries the risk of straying into technological determinism if one views hacking as being a technologically defined act.

Various groups were inspired to extend the legal logic of free software into other domains of artistic, academic, journalistic and economic production.

> *"…as the idea of free software spread into other domains of social life, it gained significant social visibility and notoriety. Through the legibility and use of free software by multiple publics, its status has shifted dramatically. What was once an odd, exceptional, and subcultural practice has acquired a more authoritative position….has been legitimated and brought from the subcultural background into the political foreground." (Coleman, 2013, p.186)*

This has given hackers a strong position from which to critique the assumptions which dominate mainstream intellectual property law since hackers can counter the view that economic incentives are necessary to induce labour and secure creativity - not only through rhetoric but through living proof in the form of high quality software which powers much of the internet.

Coleman describes 'translation' into three different spheres beyond the purely technological including capitalist technology companies such as IBM, anti-corporate activists in the counter-globalisation movement and a movement to create an intellectual *commons* as part of a larger liberal critique of neoliberal capitalism (Coleman, 2013, p.186). She argues that through a process of 'social translation' involving the gradual enrolment of social actors to "recruit various allies to extend a network of meanings, objects and institutions", open source hackers have transformed other domains of social, political, and legal life" and that "the effects of doing so have spilled far beyond this realm of technoscience to transform the politics of intellectual property law more generally" (Coleman, 2013, p.189).

In the words of Anonymous themselves,

> *"You may have heard of us as just hackers but we have been involved with occupy movements, anti-cut protests and anti-war demonstrations." (Anonymous, 2013)*

Despite the attempts of Microsoft in the early 2000's to demonize open source as a "cancerous form of communism", a range of groups embraced this approach, "allowing the ideas and practices associated with free software to travel far beyond the technological field….since it was endowed with semiotic surplus and elasticity" (Coleman, 2013, p.189).

> *"The meaning of free software is further specified, although also transformed, as different types of actors - journalists, educators, scientists, artists, lawyers and businesspeople - have taken the idea or objects of free software to justify new practices. To put it in slightly different terms, FOSS acts as an icon as well as a transposable set of schemes that are tactically adopted by others to justify divergent political and economic examples of FOSS's wider adoption, each of which has also shifted the ways that many FOSS developers conceptualise and engage in FOSS production." (*Coleman, 2013, *p.191)*

This 'translation' of hacking into other fields is certainly worth considering. A core aim of my own research project will be to explore this concept through empirical data. I would caution that placing hackers firmly at the centre of this translation, as determining actors in it, risks failing to consider a potential alternative. That hacking itself is the 'translation' of a wider societal movement. Still, Coleman does provide some powerful case studies to support her claims.

For example, the ways in which IBM began to link its name with the growing popularity in Linux open source software to adopt, repackage and sell Linux, thus extending its reach beyond the open source community. This process of appropriation could well be applied to other aspects of open source as I will demonstrate by exploring Civic Hacking through my research. Coleman also examines Independent Media Centre (IMC) activists, a loose collection of global activists who produce and distribute local media via the internet and their desire for an "open-source society" (Coleman, 2013, p.195). As with IBM, the adoption of open source by these groups has led to the extension of its network into the spheres of activism and academics.

> *"Just as some developers work full-time, blurring their volunteer pastime with their day job, other developers have entered the world of anti-corporate political activism through the spread…into these channels (or vice versa)."*
> *(*Coleman, 2013, *p.195)*

Finally, Coleman explores the movement to create a knowledge 'commons' of publicly accessible resources, taking hacker ideals "from the confines of the hacker lab out to the field" (2013, p.198). This has made the arguments of open code non-technical and relevant to mainstream practitioners in law, government and academia to the extent that they are now no longer considered radical among many of these groups. This argument was one which I was keen to explore further through looking at Civic Hacking groups and exploring how they might form part of this wider societal appropriation of hacker ideals and ethics.

However, there is still a dichotomy between this notion of hacking as an influential and positive practice and many of the more popular portrayals within existing literature. If hackers, like the Protestant reformers, rejected revolt and insisted on changing a system from within, why is the enduring image of the hacker, at least in popular culture, one of subculture, deviance and criminality (BBC, 17 Dec. 2010)? As Taylor points out,

> *"The acceptable bounds within which technological curiosity could be explored became an area of contestation for those seeking to maintain what was perceived to be the original Hacker Ethic" (Taylor, 2001, p.1).*

If the folklore of hacking began on such high moral ground, how is it that it has come to represent a 'dark side' of network societies? There is a subculture associated with hacker technologies and hacking as a subculture is the dominant popular image of this group, tending to be associated with dystopian, anarchistic and deviant imagery (Lin and Beer, 2005; Raymond, 1999; Alleyne, 2016). Again, however, the idea of a hacker subculture is a relatively undefined terminology and seeks to group a wide range of differing agendas under a single label. My own experience of speaking with those involved in the above activities and the work of others (Coleman and Golub, 2008), suggests that they often self-identify much more closely than that, associating themselves, for example, with a particular and specific '*flavour*' of Linux or the 'Nairobi IT scene'. I would argue that outwardly imposed differentiations between '*crackers'* (criminals who break into networks) and hackers may be useful to hackers *only* when explaining to 'outsiders' what they are not. It is this contradiction between deviance and ethics which will be the focus of the next section.

2.2.3 The Criminalisation and Demonisation of Hacking

Hacking as a North Atlantic Construct

As several of the authors discussed above have already indicated, it is possible to view hacking as a construct largely of North Atlantic societies, and specifically the USA. Therefore, it has been argued that the practices of hacking are embedded with particular symbolism, signs and coded imagery. Hacking emerged from a set of approaches, often referred to as a Hacker Ethic, which are argued to be reflective of the politics of libertarianism and information sharing as noted above. But the idea of hacking as a deviant activity is also closely linked to this US-centric construct. Therefore it is useful to explore the body of literature which has focused on the relationship between the culture of North America and hacking as a deviant act. This conceptual framework has been important to my research since it contrasts with the globalised and arguably more positive nature of Civic Hacking.

It should be acknowledged that, often, literature on deviant hacking emphasises 'the hacker' as an individual type (Alleyne, 2015), exhibiting particular traits, rather than hacking as a social practice. They also tend to emphasise hackers as lone actors and provide limited discussion of the communities they form (Glough, 1993).

In Narrative Networks (2015), Alleyne provides us with three popular hacker narratives which were of relevance to my own study;

1. The Cyberpunk; closely aligned to the science-fiction genre; set against a post-industrial dystopia and involving themes of cynicism, individualism and anarchism.
2. The Hacker turned dot.com millionaire hero; individuals such as Mark Zuckerberg and Steve Jobs who used their hacker skills to make their fortunes and attain celebrity status. However, I would argue here that this narrative can also be extended historically to include the demonization/heroism of other technological innovators such as Alan Turing and Leonardo Da Vinci.
3. Finally, there is the 'corporate dupe' personified in the Dilbert cartoons; the geek technologist, frustrated within the confines of corporate capitalist software industry.

Some of this literature also suggests that the portrayal of hacking was influenced by distinctly North American constructions of space and place, frontiers and the characters which inhabit such landscapes. It might be argued that such imagery has both contributed to and is reflective of a popular narrative of hacking as a criminal or deviant act.

There is a theme within much literature on hacking which argues that the idea of a frontier landscape has been an essential part of American consciousness and that this has been transferred into cyberspace (Cooper, 2000). The internet has been described as a kind of landscape on the "electronic frontier" of cyberspace and the encroachment of new technology into what was idealised as a pristine landscape has always been viewed by some with suspicion, with parallels to early American descriptions of railroad locomotives as a "devilish Iron Horse" (Healy, 1996, pp.58-66). This is a line of thinking which has been much discussed within the study of technology and society (Marx, 1989; 2010) and is intended to provide some potential insight into the public fear surrounding hacking. If the threat of both technology generally, and frontier landscapes specifically, is ingrained within North American society, then these authors suggest that this may go some way to explaining the fear associated with the symbolism of computer hacking as an encroachment upon a 'pristine' cyberspace, the frontier with its lawlessness, free from the rules of 'civilised' society. Comparisons have been made between North American literary antiheroes such as Huckleberry Finn negotiating a frontier in a similar manner to those whom one finds within cyberspace; individuals who are both "loners" yet connected to a network of fellow travellers (Healy, 1996, p.57). It has been suggested that this recurring American literary antihero has found its most recent incarnation in the popular image of the hacker. The portrayal of cyberspace as a lawless landscape occupied by criminals and rebels is reflective of its US-centric origins and intrinsic to its construction as a deviant act. The folklore of the American ‘wild west’ permeates many definitions of hackers, most obviously in the labelling of criminal and ethical hackers as ‘Black Hats’ and ‘White Hats’ respectively, drawn from the symbolism of the cowboy film genre (Alleyne, 2016). As Sterling describes,

> *"...there is an element of American culture that has always strongly rebelled against these symbols; rebelled against all large industrial computers and all phone companies. A certain anarchical tinge deep in the American soul delights in causing confusion and pain to all bureaucracies, including technological ones. There is sometimes malice and vandalism in this attitude, but it is a deep and cherished part of the American national character. The outlaw, the rebel, the rugged individual, the pioneer, the sturdy Jeffersonian yeoman, the private citizen resisting interference in his pursuit of happiness - these are figures that all Americans recognise, and that many will strongly applaud and defend." (Sterling, 1992, p.57)*

Continuing this theme, Sterling notes that "these electronic frontier-dwellers resemble groups of nineteenth-century pioneers ..." (Sterling, 1992, p.168). In a similar way to the transformation of some of these frontier pioneers into outlaws and criminals in American mythology, these hacker groups have also been framed as outlaw figures by the media, politicians and other elements of mainstream society.

Discussions of the changing definition and image of hackers highlights both this comparison with American frontier mythology and the associated criminalisation. The history of hacker culture reveals something of this 'wild west' imagery, for example, the media publicity following the arrest of hacker Kevin Mitnick in 1995 as portraying him as a sort of cowboy antihero with the subsequent chases, duals and 'sheriff' of the FBI agents in tow (Mitnick, 2012; Shimomura and Markoff 1996). Cyberspace is constructed as a frontier which is rife with Americanism and ideas of liberty, a similar situation has emerged in cyberspace to that of 19th century North America in which laws were created in the east of the country, under conditions which were completely alien to the west, forcing individuals to break such laws in order to 'get by' (Chandler, 1996, p.235). This might include informal property laws in 'land grabs' or a more relaxed attitude towards firearms or prostitution. Similarly, this argument often presents hackers as those who did not necessarily intend to break laws but did so involuntarily as they found centralised mainstream laws and social norms changing around them. This concept identifies within American culture, a certain degree of quiet respect, even admiration, for such rebels and this "outlaw innovation" (Flowers, 2008).

Such admiration, however, may be at odds with the portrayal of hackers by much of the media and government. The literature cited above does not make clear why these heroic figures came to be both admired and feared, and fails to fully question how it is that hackers could be both simultaneously criminalised and revered. As ICT and the internet became more important to society, global security, and indeed financial markets, the hacker and hacking became more of a source of concern to those in power.

In some ways, this idea of cyberspace could be aligned with the narratives of Levy or Stallman who saw the internet as something 'pure' and presented somewhat idealistic notions of hackers as heroic individuals motivated by an altruistic desire to do good, who were only corrupted by big business or the government, by a new type of hacker who 'sold out'. But I would argue that this notion is itself a myth, no less embedded in reality or with basis in empirical research than more utopian constructs of hacking. This contributes only to a dualistic version of hacking and does little to help our understanding of the complex practices involved.

Again, it is worth reinforcing the idea that the above literature represents a relatively ethnocentric view of hackers and that there is very little literature focusing on hacking in non-American or European nations. It is possible that these world views may be different for hackers outside these societies, however, this is yet to be explored. So, while it is possible, as those above have, to argue that hacking is the product of North Atlantic society and thus has particular traits, I would argue that this is very difficult to quantify without a proper exploration of hackers in other societies (Alleyne, 2016; Kloet, 2002; Nelson, 1996). This framing of hackers by certain theorists provided me with an important conceptual context against which to contrast my own, more pragmatic, position.

It is worth noting that there is a clear masculine bias within these frontier images (Adam, 2003, p133). Hacking narratives have tended to be dominated by masculine, as well as Western, frontier metaphors with feminine narratives lacking (Adam, 1998; 2001; 2003; Taylor, 1999; Miller, 1995; Brail, 1996). This should not be surprising since the IT industry generally tends to be overrepresented by males (Henwood, 1993; Adam, 2003; Cudd, 2001; Kramer and Kramarae, 1997;). In fact, inequalities may be exaggerated in an online setting (Herring, 1996; Kember, 2003). Even among portrayals of female hackers which do exist, they tend to focus on the sexualised stereotypes of the film Hackers (1996) or Lisbeth Salander in The Girl with the Dragon Tattoo (Larsson, 2008). This conflicts with the 'openness' of the Hacker Ethic presented by the authors above. This raises the question of whether hacking is really open to all or just to particular groups. Certainly, accounts of hacking tend to be dominated by white, middle-class males and there is little in the way of alternative voices being heard through the literature. There is some evidence, however, of female hackers emerging with their own voices (Adam, 2003) although often these have been overlooked by mainstream academia so we must look to blogs and media reporting (Sollfrank, 2002; 1999; Segan, 2000a; 2000b). The Civic Hacking movement does seem to place some more overt emphasis on the inclusion of different backgrounds and has some relation to movements aimed at encouraging women to code (Girls Who Code, 2017).

Folk Devils and Moral Panics of the Network Society

Some of the above attempts to explain hacking as a deviant act owe something to Stanley Cohen's seminal text on social reaction to deviance, 'Folk Devils and Moral Panic' (Cohen, 1972) so this is worth considering briefly. Cohen argues that popular consciousness, driven strongly by the media and agents of control such as the police, constructs "such types as heroes and villains and fools" (Cohen, 1972, p.11) with which to label those who are seen as deviant, those who challenge social norms (Becker, 1963). Just as the author makes reference to youth subcultures such as 'Teddy Boys', 'Mods' and 'Rockers' of the 1950s and 60s whom he claims were demonised by the rest of society, some researchers have argued that this has relevance for the construction of the hacker which might be described as a 'folk devil' of the network society due to their criminalisation by mainstream society. The association of various forms of new technology with moral panic is well documented (Raynes-Goldie, 2010).

Although Cohen was writing before the emergence of computer hackers, his interpretation means that the public reaction to one off events such as the Kevin Mitnick case could be seen as a process of rumour, mass hysteria, sensitisation and the reinterpretation of events real or otherwise. In fact, the wider creation and appropriation of countercultural groups by the media has been the subject of much sociological debate in recent years (Cova, 2007; Frank, 1997; Heath and Potter, 2006). It has therefore been relatively straightforward for various authors to apply this work to hacking. On the face of it, this theoretical position also goes some way to explaining the intense reaction to hackers in that they are perceived in the media as being affluent and educated youths, who behave in a way not expected. Society expects youths from backgrounds of social deprivation to behave in certain ways to conform to 'norms of hooliganism'. The seemingly disproportionate social response to groups such as students, 'hippies', 'beatniks' and hackers, however, comes from the fact that they challenge the norms to which educated and relatively affluent members of society are expected to adhere (Cohen, 1972, p.197).

This concept of moral panics has been developed by other authors exploring hacking (Meikle, 2002, p.166). Such terms are highly emotive and, I would argue, are representative of a line of thinking in this work which contributes to an artificial polarisation between 'good' and 'bad' hackers. This should be contrasted against authors described previously such as Coleman (2013) and Kelty (2008) who seek instead to focus upon the complex nature of hacker communities and their actual relationship with wider society and who provide a much more rounded framework from which to position my own research. This particular view of hacking is useful, however, in reflecting the fact that the meaning of the term 'hacker' has changed from its original usage, captured by the Hacker Ethics described above. Many hackers resist these negative definitions (Sterling, 1992 p.57), self-identifying more with the 'talented tinkerers' described in my earlier sections, an idea which I aim to address through my own fieldwork. This can be seen in self-depictions of Hacker Ethics, political aspects of hacking, their engagement with police, business or charity and calls for recognition of the 'hackers' in the history of technology. There is, in fact, some evidence to suggest that hackers are becoming viewed in a more positive, or at least more realistic, perspective through wider public interest in the history of hacking and its contributions to society (Rheingold, 1993; Mizrach, 2009).

I would question, however, whether some of these more positive portrayals are any more realistic or a reaction to this popularised image of the deviant hacker since the 1980s. Part of my research aim was to counterbalance these portrayals of hackers with a more pragmatic and empirically based interpretation.

As the literature cited above demonstrates, much of the previous research into hackers was grounded in criminological explanations of adolescent delinquency and masculinity (Yar, 2005, p.387). Based on the small number of interviews carried out first hand with hackers, however, it is apparent that the ways in which these individuals self-define is often quite different from these public constructions (Turgeman-Goldschmit, 2008). Instead there is far more emphasis on ethical concepts, on the belief that their intelligence and technical knowledge distinguishes them from the rest of society (Heckert, 1989), or on hackers as agents of social change (Ben-Yehuda, 1990). As evidenced in the first section of this literature review, a binary division between good and bad has been constructed which needs to be addressed through empirical research. To redress the inequality in this research conducted so far, it could be based upon the recognition that hackers are a much more complex and heterogeneous group than has been previously theorised (Coleman and Golub, 2008). This will be a core focus for my own research project.

It is also worth noting that what is illegal hacking (often termed ‘cracking’) in one place and time may not be considered criminal in another and so is highly subjective (Fafinski, 2009). The Computer Misuse Act in the UK, for example, is new and evolving. What is legitimate, even entrepreneurial now, may be illegal in the UK in ten years' time or in another legal framework such as The People's Republic of China. The same may also be true of what is considered ethical or moral within a particular time and place. Twenty years ago, it is likely that world governments could not have conceived of hacktivist groups such as Anonymous and Lulzsec which carry out politicised or ideological hacks (Coleman, 2014). Now they adapt laws and regulation in order to classify and prosecute these acts, whether as mere childish pranks or terrorism. The act of hacking as criminal intrusion is to some extent dependent upon fluid regional legal and ethical systems. This might be what Meikle is referring to when he states that;

> *"The original sense of 'hacker' and the open-system Hacker Ethic just didn't fit with the consolidation of information technology at the centre of the 'new economy'. And the marginalisation and demonization of the Hacker Ethic, in which information famously 'wants to be free', was a necessary step in consolidating a worldview in which information would prefer to be paid for." (Meikle, 2002, p.167)*

Although it may be true that hackers are criminalised within particular contexts, I would argue that the use of contrasts between criminal and non-criminal, 'good' and 'bad', when interpreting hacking and hackers does not hold up to its application within globalised and highly complex societies. This is partly because it focuses too much on external representations of hackers rather than the diverse variety of ways in which they self-identify. By drawing upon first-hand accounts by hackers, my research project aimed to provide a more realistic view of this activity rather than one based upon these dichotomies.

Although hacking, with its link to libertarian ethics, always had the potential to become a political act, it was only with this contest between the ethics of hacking and government/corporate control that, during the 1990s, led to the conscious politicisation of the hacker and the emergence of 'hacktivism'. This type of hacking is worth exploring in more detail since it bears relevance to my study of Civic Hacking, an activity with close ties to hacktivism, and is the subject of the next section.

2.2.4 The Politicisation of Hacking: Hacktivism

Hacktivism and its Relationship with Hacking

Having explored the ways in which hacking has been presented as either idealised or dystopian, it is worth also considering how it has been framed more recently as a politically motivated practice (Samuel, 2001). It has been argued that hacking has always been 'tinted' with the narrative of resistance and contest (We Are Legion, 2013). From the MIT hobbyists to the ethics of open source software, hacking has involved a desire to explore systems which has often put hackers at odds with established power structures. Hacking has therefore had the *potential* to be a political act under certain circumstances. The frequently subtle politics of cracking and FOSS makes no distinction between social and technological but makes use of the determinism between the two in creating and breaking objects. Hacktivism takes this determinism and applies it to the 'everyday' politics of human rights or anti-capitalism rather than "the politics that dominate discussion in the backrooms of IT support" (Jordan, 2008, pp.70-71). In a society dominated by technology and information, the ability to control such technologies has led to a conflict between state control and individual freedom (Himanen, 2001). It is often within these politicised debates that Civic Hackers attempt to make interventions.

Again, we find that the North American influenced ideals of liberty and democracy mentioned above may have played a role in shaping the nature of this struggle or at least its portrayal, however, there was a point at which individuals finally went beyond this relatively passive libertarianism and emerged as self-aware activists. It is not surprising then that this emergence of political subversion coincided with the 'hacker crackdown' during the 1990s since it was also the point at which computing and the internet obtained both a symbolic and technical position of importance in western societies. Jordan (2004) suggests that hacktivism emerged at a point when the subculture of hacking was being both pushed aside by the mass adoption of corporate computing and also vilified through negative portrayals by the mainstream media. An early signal of the conscious blending of hacking and political activism came in 1989 with an anti-nuclear motivated hack of the Goddard Space Flight Centre network, one of the first examples of activist motivated hacking (Thomas, 2001, p.2).

The word ‘hacktivism’ may have been coined by a hacker (Mathaba, 2011), but as with other hacker definitions it is typically an imposed rather than self-applied label, a construct largely of the media (Coleman, 2009). Defining what it means and whom it covers is as complex as it is for the wider practices of hacking (Jordan, 2001). The term carries with it a weight of implications - homogeneity, a dualism between good and bad (as discussed in the section on criminalisation), a distinction between previous hackers and hacktivists – many of them unhelpful. It might be argued that overtly political hackers such as Julian Assange have something in common with the non-directly political individuals like Kevin Mitnick as ‘folk devils’ during the 21st century in that they have been portrayed by wider society in terms of binary and reductionist ‘folk devil’ characters. The ethos of Anonymous as a movement is characterised by a range of contrasting tensions between nihilism and idealism, dystopianism and utopianism, egotism and collectivism (Olsen, 2013) and between *“the negative freedoms of libertarianism and collectivist goals of equality and justice”* (Goode, 2015). Therefore, it is important not to characterise such movements in too simplistic and unified terms. This was an important consideration for me when approaching Civic Hacking as a research subject.

As early as 1990, the Electronic Frontier Foundation expressed an arguably idealistic enthusiasm for the politics of the internet with what they felt was a, debatably, decentralised and democratic model. This was based upon supposedly North American, ‘Jeffersonian’ ideals of liberty, diversity and community, free from governmental control, and judgement by contribution rather than by race or gender (Jordan and Taylor, 2004, p.133). The politics of hacking has often been anchored to a *"mythical, prelapsarian America, an idealised community…"* (Meikle, 2002, p.34) and this culturally specific brand of politics inherent in hacking may go some way to explaining the fear associated with hackers (Vegh, 2002; 2005).

> *"Fear of hackers goes well beyond the fear of merely criminal activity. Subversion and manipulation of the phone system is an act with disturbing political overtones. In America, computers and telephones are potent symbols of organised authority and the technocratic business elite." (Sterling, 1992, p.167)*

While this relationship between North American politics and the criminalisation of hackers is well rehearsed within the literature, Brian Alleyne (2016) suggests that hacktivists informed by alternative social and political narratives are largely lacking.

Individual freedom, however, is not necessarily focused on democratisation or benefiting wider society. David Golumbia (2013), attempts to group a number of different individuals as what he terms "cyberlibertarians". This includes diverse figures such as Julian Assange, Tim O'Reilly, Mark Zuckerberg, Clay Shirky and Lawrence Lessig. What connects these individuals, he argues, is that despite their different backgrounds and positions, they possess a shared, overarching focus on individual freedom.

This view should be contrasted against the mythologizing of hacktivists which is typical of a particular view in the study of hacking which portrays hacktivists as "freedom fighters" (Still, 2005). I would argue, however, that this representation of hacktivism does not acknowledge the fact that it often takes a set of beliefs which would traditionally be seen as politically leftist in nature and appropriates them for use by the capitalist right wing. In other words, they began as a cry for informational freedom by citizens and became used to insist that governments do not intervene or overly regulate the capital of cyberspace (Borsook, 2000). Many of these *technolibertarian* hackers fight against anything that prevents individual from accessing whatever information they want (Jordan & Taylor, 2004, p.134). Thus, there is an apparent contradiction between the anti-corporatism which often typifies hacking and the involvement of some hackers in the technology industry in which companies like Facebook and Google promote the Hacker Ethic and even hold internal 'hackathons' (Mezrich, 2009; Mikkonen et al, 2007). Golumbia argues that hackers are in a sense neoliberalists;

> *"There is no concern with equal rights, democracy…there is concern only with the ability of corporations and individuals to make as much money as possible." (*Golumbia, 2013, *p.22)*

Interestingly, however, Civic Hackers tend to define themselves by a focus on developing society as a whole rather than seeking individual benefit. One might also argue against this portrayal of hacktivists as informational 'freedom fighters', however, on the basis that they often disrupt access to information. The techniques employed in hacktivism are often aimed at disruption rather than creation. This is another aspect in which they differ from the Civic Hackers who will form the focus of my research. On the other hand, Otto Von Busch and Karl Palmas (2006) provide an interesting definition of hacktivism. They argue that, just as hacking is about building new things as opposed to destroying them ('cracking'), so hacktivism should also be defined as a constructive act. They argue that what is often described as hacktivism, denial or service, defacement or online jamming, could be described as 'cracktivism'. Dan McQuillan (2012) equates the motivations of Anonymous and Lulzsec as having more in common with the robust commitment to free speech and struggle against tyranny expressed by the antinomians of 1600s England than "geek liberalism, or even libertarianism".

It is also worth considering whether Hacktivism should be considered 'hacking' in the traditional sense of modifying or creating code (Caltagirone, [no date]). After all, it can encompass a range of techniques and, interestingly, participants do not necessarily need a high level of IT skill to carry out acts. The Low Orbit Ion Cannon (LOIC) Distributed Denial of Service (DDoS) software utilised by supporters of the Anonymous group (BBC, 28 Jan. 2011c), for example, are as user friendly as, say, Facebook or Microsoft Office. This does, on the face of it, present somewhat of a contradiction to the perception of hackers as technologically accomplished individuals discussed in Section 2.2.2. If hacktivists are not distinguished by their 'technological virtuosity' then what do they have in common with hackers? This question is of relevance to my own research since Civic Hacking does not always involve technical hacking and can often encompass a much wider set of practices, as discussed in the previous sections.

Despite this apparent contradiction, however, hacktivism should be seen as *closer* to the original Hacker Ethic of information freedom promoted by Civic Hackers. Open and free access tend to be important ideals to hacktivists so groups such as the EDT have more in common with the original MIT hackers than the 'cybercriminals' of popular culture, due to their views on the democracy of cyberspace (Wray, 1998, p.3). In 'Underground' by Suelette Dreyfus and Julian Assange (2011), the authors argue that the origins of WikiLeaks are in the earliest dentitions of a hacker, one which did not imply any illegal activity but rather finding clever technical solutions and 'thinking from outside the box. In this case, they suggest, the creative application of secure and anonymous online publication to solve the "hard problem of getting governments and corporations to tell the truth." Tim Jordan describes a similar form of hacktivism which focuses on protecting and extending the availability of information on the Internet through anonymising tools (2008, p.73), what Julian Assange calls "Cypherpunks" (2012). This may be linked to an earlier form of 'cyber activism' involving the creation of rogue websites and online chat groups to target corporations (Hill, 1998) while, with the rise of social media, this type of activity has become even more accessible and powerful, involving the use of tools to enable secure and private information access through "digitally correct hacktivism" (Jordan, 2002, p.128) or the use of anonymous software such as Tor as a form of activism (Lovink, 2016 p190).

Additionally, the relative ease of access afforded by online forms of activism which do not require technically sophisticated hacks allows a greater number of individuals who could not otherwise protest to participate in mass social action.

> *"Ten years ago it would have been infeasible for tens of thousands of individuals with no physical connection or central leadership to conceive, announce and implement a massive act of civil disobedience against a significant Western power, crippling a portion of its online infrastructure in the process." (Anonymous, 2013)*

It is worth remembering, however, that new technology is not the only determining factor in these types of movements and should certainly not be a starting point for discussions (Jordan, 2009). In addition, this increased access to technology can also drive both positive and negative effects. After all, while the increased global democratisation of protest indeed presents opportunities (Illia, 2002), it arguably takes less individual courage (in parts of the world free from excessive state oppression at least) to press a button on an automated piece of software than it does to face shields and water cannons (Jordan & Taylor, 2004, p80; Thomas, 2005, p.6; Meikle, 2002, p.143). On the other hand, in certain regions of the world, the implications of online protest can be severe, albeit slightly less immediate.

In recent years, there has been criticism of some forms of online protest as 'slacktivism', suggesting that they are somehow 'lazy' or, at the least, inferior in the eyes of those who assume that online is less genuine than offline activity.

Geert Lovink, for example, claims that "strong organisational forms, rooted in real life....will eventually overrule weak online commitments (Lovink, 2011, p160). On the other hand, there are successful and less successful forms of both online and offline activism, hence so-called 'clicktivism' should not always be dismissed simply for being accessible (Franklin, 2014). Henrik Christensen (2011) argues that while there is good reason to be sceptical of the sincerity of some internet campaigns, particularly Facebook groups, critiques of online 'slacktivism' are overstated since many examples of real world activism also do not require great effort or risk.

The media attention surrounding WikiLeaks (BBC, 2011a) is a key example of where hacking ends and hacktivism begins. Although the activity would not be described as computer hacking in the sense of modifying code, WikiLeaks does share a common root in the Hacker Ethics of free information and decentralisation and its founder, Julian Assange, emerged from the hacker underground of the 1980s. Geert Lovink (2011) describes WikiLeaks as being involved in "information hacks" which assists human rights groups who are struggling to get their message across by playing by the rules and seeking legitimacy from dominant institutions. Instead, WikiLeaks were able to gain legitimacy through a spectacle of popular media, tapping into public dissatisfaction with mainstream politics. In this sense, the activities of WikiLeaks certainly fit a definition of hacking as a contesting of control over information by a dominant group. Gabriella Coleman (2015) concludes her most recent study of hacktivism with a depiction of surveillance in the digital age, a situation in which she argues that governments and corporations find it all too easy to capture data on the users of technology. In this, she explicitly links hacktivism to a struggle for technological democratisation through figures such as Edward Snowden and a host of activists, lawyers and journalists. Coleman describes how *"never before have so many 'geeks' and hackers wielded their keyboards for the sake of political expression, dissent, and direct action"* (Coleman, 2013, p.382). She also depicts a new age in which citizens are, in the wake of the Snowden revelations, more aware of this mass surveillance and are increasingly turning towards technologies such as encryption, anonymisation and other privacy features to build a surveillance free internet. Civic hackers make some contribution in this debate since they are both inclusive of those who are not highly technical and also aim to allow easier access to ICT - this was something I intended to explore through my research.

The ethical debate over hacktivism is based around a central principle – is denying others freedom of information ever justified? Do the ends of denial of service justify the means? After all, it could be argued that "the virtual sit-in conflicted with the Hacker Ethic" in that it often denies others their rights to freedom of information (Jordan, 2002, p91; Still, 2005). Meikle describes Hacktivists as individuals "who hold that bandwidth is above human rights" (Meikle, 2002, p.151). The DDoS of a pro-ETA news website hosted by IGC was viewed as censorship by even hard-line hacktivist proponents and led to an outcry by advocates of internet freedom (Sauter, 2014).

Part of this argument was that the anonymous nature of many such acts, in addition to the fact that they can be carried out by individuals rather than groups, means that they lack democratic legitimacy (Jordan, 2008, p.71). The power of hacktivism does not require mass participation (Wray, 1998, p.7) and this was the case with the EDT, however, the LOIC used by Anonymous did galvanise thousands of individuals from around the world. In addition, denial of access of information could have potential knock on effects on other users, in extreme cases other human rights groups or even emergency services (Thomas, 2001, p.2). Oxblood Ruffin of the *Cult of the Dead Cow* hacktivist group went as far as to claim that this form of activism violates the First Amendment (Ruffin, 2000).

But some claim that such acts are justified under certain circumstances. This argument rests on the difference between ‘consequentialism’, the ends justifying the means, and ‘deontological’ ethical theory (Caltagirone, [no date], p.4) which argues that if everyone acted in such a way it would be detrimental to social order. Most arguments against hacktivism are based on this idea. However, cases such as the use of hacktivism in Indonesia to publicise genocide in East Timor when no other avenues of protest or expression where available, do present strong ethical dilemmas. For Civic Hacking, access to information is key. These debates are therefore useful in contextualising my own research field.

Closely linked to this idea, is the argument that hacktivism is focused on *method* rather than cause because the emphasis tends to be weighted towards the techniques used and often the causes being protested are lost (Samuel, 2004). Unusually, Samuel was able to gain access to primary interview data with hacktivists which evidence this view (Samuel, 2004, pp.6-10). Samuel found that the hacktivists she spoke to spent a great deal of time debating the ethics and efficacy of particular activities, for example DDoS. She suggests that, for her participants, the method and activity used defines whether someone is considered a hacktivist or not to a greater extent than the actual outcome. Therefore, according to her findings, the questions of whether DDoS (i.e. the prevention of information flows) is ethical or otherwise is what defines hacktivism more than any particular context. In this way, hacktivism differs from Civic Hacking. While Civic Hacking may be political, it is above all pragmatic, an idea which I intended to focus data gathering on. These groups were focused much more on the practical outcome of their activities rather than any kind of symbolic theatre produced through gestural methods.

The Symbolic Power of Hacking

The *performance* of hacking, however, was an essential part of its symbolic power from the early days at MIT (Bender, 2011). As mentioned previously, hacking was not confined to computer systems but was also about the exploration and modification of social systems and official regulations. This symbolic power has translated into hacktivism as a powerful tool of political protest (Thomas, 2005). The Electronic Disturbance Theatre (1996) coined the term electronic civil disobedience and have been successful in drawing attention to the Zapatista movement in Mexico through a range of hacks against the Mexican government, blending code with performance art (Coleman, 2013, p136).

Such '*culture jamming*', the subversion of legitimate websites through a kind of 'virtual graffiti' has also been used against corporations including Nike (Jordan and Taylor, 2004, p85) and more recently Amazon. It is apparent from much of this activism that it is more of a symbolic act than a real attempt to crash a computer network. Hacktivism is a performance which is intended to create a public spectacle and a drama (Still, 2005, pp.149-152). Although on the face of it, this might appear at odds with the practical 'tinkering' of hacking, when considered in the context of the philosophical development of hacking and its symbolic importance, I would argue that this kind of performance begins to make more sense. Anonymous began as a collection of pranksters ('trolls') who carried out trouble making purely for the fun of it ('lulz') but have since become a serious political movement and also received the label of 'criminal' in the eyes of the state (Coleman, 2013, p.393). However, she also suggests that this serious political activism would be less powerful, certainly less high profile, were it not for this associated theatre. For hacktivist groups, it may be argued that the media hype is more significant than the actual effectiveness or end result of their activities. Much of this focus relates to the new methods being used more than the actual cause (Meikle, 2002, p.155), the "antics and desire for spectacle and spoofing" and their use of online absurd comedy and often playful real-world protest (Goode, 2015). As discussed, this should be contrasted against the practical pragmatism of Civic Hacking.

2.2.5 Conclusions: Towards a Definition of the Hacker Ethics

So, what then is hacking? The literature discussed above suggests a need to reframe hacking, and indeed hackers, from the popular image which has been constructed as a media driven 'folk devil' of the Network Society, to a more rounded and complex reality, based upon more accurate first-hand accounts. Hacking in fact represents a complex and heterogeneous set of practices which often evade definition. Gaps within the literature suggest that there is a need for research in this area, guided by an approach which provides a sufficiently complex definition of hackers and hacking.

However, a theme which emerges from the literature, and on which the original Hacker Ethic was built, is the idea of manipulating technologies, thus re-appropriating them to achieve a task for which they were not intended. This, I would argue, should be combined with the following core 'ethics' as a way of identifying and exploring those who may be involved in hacking;

- Collaboration
- Fun of hacking
- Community
- Practical Involvement
- Inclusivity

This list forms a definition of Hacker Ethics which shall form the basis of my own research and will be explored further in the following chapter. Hacking has often been motivated by a combination of curiosity, desire for financial gain and increasingly political activism. A much-overlooked motivation, however, has been those who 'hack' technologies out of a more pragmatic desire to solve social or development problems. Such hackers also differ from these ethnocentric constructions in that they are frequently based outside North Atlantic societies and form a globalised network which is often focused on the world's least developed countries.

What is a Civic Hacker?

Based on the preceding discussion, I therefore propose a broad definition of hacking as a (sometimes non-technological) activity in which technologies are manipulated to achieve a task for which they were not originally intended. A hacker can be said to be one who engages in this act of hacking but also as someone who relates to the set of Hacker Ethics described above. There are a variety of motivations for this activity, however, my focus will be on those who hack for social good (as described in Section 2.3.2), those who I will term Civic Hackers. Through empirical data on Civic Hackers, I will develop the argument that, as discussed above, these Hacker Ethics are proliferating to other areas of wider society.

2.3 Part Two: Hacking for Social Good

2.3.1 Introduction

Having explored the key debates within the study of hacking and provided a definition of Civic Hacking from which to frame my own research, it is now important to further position Civic Hacking within a wider social context. Theories of 'Network Societies' provide us with a useful way of conceptualising the world in which we live because they allow us to understand how information networks have shaped, and are shaped by society. By making use of this approach, I shall explore theories which argue that hacking as a social practice came to occupy an important position due to the hackers' ability to manipulate, through ICT, a core currency of this society; information. If we accept this importance of information, inequalities in information and ICT access become even more relevant. The unequal distribution of information and ICT has been referred to as the Digital Divide (Korupp and Szydlik, 2005; Gurstein, 2003; Luyt, 2004) and, as will be discussed below, may be a somewhat problematic notion. It does, however, contain some points of relevance to the study of Civic Hacking since these groups are aimed at addressing inequality through technology.

More specifically, ICT4D and similar movements which combine technology and development seek to address these inequalities by attempting to make ICT more appropriate to people living in developing countries (Toyama and Dias, 2008). This section will explore the literature which suggests a relationship in terms of practices and approaches between these ICT4D groups and a new type of hacking, Civic Hacking, which is motivated by humanitarianism. Based on the literature, I began to infer that some ICT4D groups are in fact involved in hacking, not just because they modify code, and technology but also because they display aspects of the Hacker Ethics. These groups often work with the lead users of technology to create collaborative, appropriate and local solutions to global problems. In this way too, they have something in common with those involved in other types of hacking.

By the end of this section, I will provide a greater understanding of some of the theories upon which my research was built as well as demonstrate that there was a gap within existing research into this humanitarian motive for hacking which I intended to address through my own study of Civic Hackers.

2.3.2 Information and Network Societies

Defining Network and Information Societies

Before exploring how theories of the network society relate to hacking, and in particular Civic Hacking, it is first important to explain the background to these theories and provide some context. In recent times, information has become a key denominator for describing the world in which we live (Lash, 2002). The idea of a discernible 'Information Society', one in which information is the central feature, has been around since at least the 1960s (Machlup, 1962; Porat, 1978) although there has been little in the way of a single consensus on just what it means, thus leaving the impression of quite a vague notion (Webster, 2006; May, 2002; Feather, 2008).

Defining what is meant by the information society means answering a fundamental question: how does this 'new' society differ from what has gone before? In other words, is that society 'new' and, if so, in what way? Various authors have attempted to answer this question by approaching it from the point of view of several different changes in society.

Technological changes appear at first glance to be the most obvious indicator of an 'information society'. On the face of it, the massive increase in devices such as PCs, televisions or mobile phones are significant in the creation of a new type of society and this has also been portrayed as a clear progression from agricultural revolution to industrial revolution to an information revolution (Poster, 1990). However, most commentaries are vague in their definitions of technology, failing to provide any real-world or measurable examples from which such a societal change can be measured. In these views, ICT is both everywhere and nowhere, making our ability to judge its significance almost impossible. This stance is also technologically determinist since it presents technology as the prime social dynamic, thus oversimplifying the changes which have occurred.

Changes in economic relationships with information, the increasing importance of information to economic stability and growth within society, are also described as central features within much of the literature. Again, this relationship appears straightforward on the face of it; as a society moves towards being increasingly reliant upon information for its economic success, one might theorise that it has become an 'information society'. Several authors have, for example, demonstrated statistically that the increase in informational business has been significant to the economy of the United States (Machlup, 1962; Porat, 1978; Dizard, 1981). However, this is also less than straightforward. Much of this quantification has been interpreted in a biased manner, with judgements regarding categories being used to assign values which tend towards the economies of information, oversimplifying the complex factors involved. Activities which would not necessarily be considered 'informational' by many people, for example, building libraries or R&D departments of manufacturing firms are divided out from their interrelated non-informational areas in an "arbitrary" manner and then cited as examples of an increase in business based upon information.

Changes in occupational patterns will be discussed in a later section of this chapter in relation to hacking specifically, however, this is worth introducing at this point since it is an important area of interest for sociologists studying information societies. The inference of various authors is that an information society can be judged by the dominance of occupations centred upon information (Bell, 1973; Drucker, 1968). Thus, a decline in manual manufacturing work and an increase in white-collar or service sector jobs (evidenced statistically) is viewed as indicative of this change. This view emphasises the influential significance of information itself, rather than specific technologies. Within an information society, the dominant occupational attributes are *"'thinking smart'…being 'inventive' and having the capacity to develop and exploit networks" (*Leadbeater, 1999*).* Ideas, knowledge, skills, talent and creativity become more important than physical effort. Castells (2000) also argues that the economy is driven by "people whose major characteristic is the capacity to manipulate information". Again, however, the ways in which statistics regarding such occupations are categorised (informational and manual) are based upon particular judgements which often mask the complexities involved and the blurred boundaries between them. It might be more useful to instead point towards a more qualitative measure in which qualified professionals, albeit statistically small, came to dominate occupational types rather than 'non-experts' e.g. landed gentry (Perkin, 1989) or in which a 'new class' of employee 'composed of intellectuals and technical intelligentsia emerged' (Gouldner, 1979). Interestingly, from this point of view, those involved in hacking could almost be described as 'non-experts' since, as I have discussed, it is an activity associated with 'hobbyism' and leisure time rather than the domain of qualified professionals.

Spatial changes are also frequently cited as signifying information societies (Castells, 2000; Webster, 2006). These changes emphasise the relationship between information, time and geographical location and the changes to these which have occurred as a result of increased informational networks. Locations are increasingly connected through as electricity, internet or money transfer and people are increasingly connected in different manners and to varying degrees as a result of this change, allowing almost-instantaneous communication with anyone at any place and time. But at what point these spatial changes can be defined as an information or network society in terms of volume or velocity. After all, information exchanges through telegram, telephone or even postal services pre-date ICT networks (Webster, 2006, p.18).

Finally, a set of cultural changes have been described which might be said to take place within an information society (Poster, 1990; Dyson, 1997; Turkle, 1997). Contemporary culture is more 'information-laden' than at previous times and so symbols for receiving messages about ourselves are of increasing importance. On the other hand, due to the saturation of these symbols, they may have become meaningless and are losing their meaning and power as the amount and complexity of this information increases. Toffler (1980) describes a sense of cultural dislocation and uneasiness which results from this increased information and speed of communication. While we all may accept that these cultural changes are experientially true, they are difficult to quantify and therefore provide a difficult framework from which to define an information society.

One might argue that none of the above frameworks are capable of accurately defining the information society and that attempting to define this by the quantity of information is misguided. The *character* of information must be such as to have transformed our lives (Webster, 2006). It is not enough just to consider information in itself but we must instead examine the *meaning* of that information; its significance to our lives. Information needs to be about something and so cannot be measured in isolation purely in terms of its economic value, volume or speed of travel through space and time. By approaching information qualitatively in terms of its complex range of significance, meaning and value results in a quite different conclusion than for those who attempt to quantify its increasing scale. While it is relatively straightforward to show that the amount of information has increased, this often says nothing about the impact this has had upon society. On the other hand, those who explore the changing significance of it tend to be left with the, common-sense, conclusion that information has changed and defines the society in which we live in one way or another.

Network Societies

The study of this increasing significance of information has also, more recently, been developed to form the term 'Network Society'. While similar to theories of Information Societies theories of Network Societies seek to not only position information as their defining feature, but emphasise the ways in which social structures are organised around information *networks*, specifically those using electronic technologies (May, 2002). This view differs from the Information Society since it argues that societies have always been signified to some extent by information and this does little to distinguish contemporary life. It instead argues that the key difference between past and present society is in the importance of global networks which connect various aspects of life. On the other hand, certain aspects of society have remained consistent, namely what Castells refers to as 'informational capitalism', the relationships associated with a capitalist economy which are continuous, albeit in a more globalised and fluid state (Castells, 2000). Within this globalised flow of information networks, Castells describes winners and losers, those who have access to quality information and those who do not. Since my research project was concerned with the ways in which Civic Hackers intervene within these networks to address inequality, this body of literature seemed significant and worth exploring further.

Network societies are typified by an increased number of links between groups and individuals without personal contact and are simultaneously global and local, dependent upon digital communication. Within such societies, technologies such as mobile telephones, internet and social media can be viewed as a "new lifeline" alongside traditional networks of roads, electricity cables and water pipes. This may result in "amplification" of imbalances so that, while technology allows for better distribution of knowledge, it may also serve to intensify existing social inequalities (Warschauer, 2002).

> *"A modern type of society with an infrastructure of social and media networks that characterises its mode of organisation at every level: individual, group/organisational and societal. Increasingly, these networks link every unit or part of this society (individuals and organisations). In western societies, the individual*

> *linked by networks is becoming the basic unit of the network society. In eastern societies, this might still be the group (family, community, work team) linked by networks." (Van Dijk, 2006, p.23)*

Critiques of Network Society Theories

Theories of Network Societies have been subject to some level of critique and there are a number of contrasting approaches to this construct. A primary criticism of Network Society theories is that they suggest a total break with what has gone before. There is an argument, however, that existing forms in society are perpetuated in a network society and some basis to reject the notion that an information revolution has somehow 'changed everything' (Webster, 2006; May, 2002; Hamelink, 1986). In fact, 'informationisation' can be seen as an outcome and expression of established forms as opposed to a novel society (Webster, 2006). Rather than increasing levels of democratization, it could be argued that existing economic structures not only remain within the Network Society but are, in fact, often exaggerated (Schiller 2000; Dean et al, 2006).

As with the concept of an Information Society more generally, theories of Network Societies can be relatively undefined, often constituting a number of different approaches and frameworks. It may be that part of the attraction of such theories, and the reason for their adoption by the mainstream media when discussing technology, is the ease with which they can be appropriated by those outside the social science debates in which they originated. In particular, Castells has been the subject of much critique in this respect. Webster (2006, p.115), for example, comments on the terseness of some of Castell's commentary and argues that this is "grounds for suspecting the novelty of the substantive phenomena on which it is based". On the other hand, it could be argued that Castells has successfully portrayed the society in which we live to the extent that it is recognisable.

Like Castells, Yokai Benkler has also taken a more optimistic view of the changes resulting from information networks. He argues that there has indeed been a revolution brought about by networked information which has had deep and structural repercussions for contemporary society. In particular, they have allowed individuals the freedom to take a more active role than previously possible in society and allowing for increased democratic participation to achieve improvements and development (Benkler, 2006). Cooperation and collaboration have been increasing due to the revolutionizing effect of the internet and gives examples such as Wikipedia and open source and shows that mainstream organisations are adopting this approach (Benkler, 2011). This line of thinking has something in common with the 'Californian Ideology' embraced by many within the hacking community and which has been subject of much critique as described in the previous section.

Yet the views of Castells and Benkler should not be taken at face value. While it might be comforting to view information networks as somehow inherently democratic, these networks are dominated to some extent by corporations and are increasingly under the control of big industry and government. It was therefore important for my research to contrast this reality against the libertarian ideology of grass roots activists and hackers who present networks as a 'pure' thing which should not be subject to regulation. The internet is no longer subject to the "freewheeling ethic" of deregulation but is now a site of conflict involving state intervention and big business (Lovink, 2003). It cannot exist in a vacuum but is subject to constant influence by the world around it. While the internet may present the image being democratic, even the apparent free speech provided by blogs and social media, often takes place within an "echo chamber" without actually carrying any genuine political power (Lovink, 2011). This was relevant to my research since Civic Hacking was predicated on this democratizing power of ICT while on the other hand contrasted against the state and corporate dominance of both development work and the activism in which these groups engaged. Lovink in particular is sceptical of Web 2.0 in its emphasis on amateurs, participation, collectivism and community. He argues that just because these applications appear to be 'free' does not necessarily mean that corporations are not making profit indirectly from them (Lovink, 2008).

Information has both changed society and, in other ways, it remains the same. While the notion of an information society should not be rejected altogether, since aspects of it are useful, it should be more critically assessed than the analysis provided by Castells. Christian Fuchs makes use of Marxist theory to describe our society as a capitalist system in which information is just one important aspect. In his view, information societies are often used by dominant interests in order to advance neoliberal policies. Fuchs argues that contemporary society is an information society in terms of its forces of production and capitalist in its relations of production. These concepts should not be seen as separate but rather interconnected, both a new society and one that has not changed in other ways (Fuchs, 2014). Fuchs rejects the view that the internet is participatory as put forward by Castells, that it is somehow democratic and instead argues that it is exploitative in nature (Fuchs, 2011).

Relevance to Civic Hacking

Despite these critiques, however, theories of Network Societies do have implications for the sociology of hacking and for my own research project. If we accept the argument that information and the networks which control information are central foundations of our society, then I would argue that the hacker occupies a position of great efficacy since they possess the power to manipulate these information networks through ICT. These theories therefore provided me with a useful theoretical starting position from which to approach Civic Hacking.

I was drawn to theories of network societies as a means of interpreting Civic Hacking as part of a set of social movements which have emerged in recent years and providing some explanation for their commonalities. Various social movements which have emerged within the past ten years including Occupy Wall Street and the Arab uprisings which can be interpreted within the context of the power relationships which take place within a globalised network society. Technologies of the internet, and in particular social media, have provided the ‘disempowered actors’ within such society the means to challenge embedded power structures such as financial institutions and political regimes.

> *"In our society, which I have conceptualised as a network society, power is multidimensional and is organised around networks programmed in each domain of human activity according to the interests and values of empowered actors. Networks of power exercise their power by influencing the human mind predominantly (but not solely) through multimedia networks of mass communication. Thus, communication networks are decisive sources of power-making. If power is exercised by programming and switching networks, then counter power, the deliberate attempt to change power relationships, is enacted by reprogramming networks around alternative interests and values, and/or disrupting the dominant switches which switching networks of resistance and social change." (Castells, 2012, pp.7-9)*

The catalyst for this resistance comes when citizens make use of networks of communication to share their feelings of suffering, anger, outrage and, ultimately, hope. These social movements carve out new public spaces, both on the internet and through the occupation of urban spaces, in order to create free communities which are often symbolically meaningful in their manipulation of the spaces of dominant elites. Coleman (2015) also argues that those involved in the hacktivism of Anonymous are motivated by hope, where applied to *"censorship in Tunisia…North American rape culture…political and economic injustices in Zuccotti Park and Tahir Square"* (Coleman, 2013, p.395).

Network Society theories also provide an understanding of the ways in which information is distributed globally and help interpret concepts such as the Digital Divide. The term digital divide emerged from an argument that lack of

ICT among certain parts of society, whether globally or nationally, has resulted in deep inequalities in the extent of participation in key areas of life. An expression of this perceived inequality of information has been the ICT4D movement who seek to address this imbalance through increasing access to appropriate technology. There are other terms for this field and it comprises a range of varying methods and ideologies. For example, Geekcorps is a non-profit organisation which supplies technical expertise to developing countries to work on improving infrastructure. Ushihidi, on the other hand, is a Kenyan based free and open source software company which develops 'crowdsourcing' tools to allow people to gather and analyse data such as election results, crime statistics and disease, and has proved particularly useful in parts of the developing world.

I was interested in whether certain groups and individuals working within this area bear a relationship to Civic Hacking in that they embody some of the Hacker Ethics described in Section One and through my research I identified some clear links between both groups. ICT4D groups will also be explored through the literature on innovation and collaborative invention and I aimed to explore the ways in which these groups exhibit elements of the Hacker Ethic described previously.

It is worth noting that ICT4D tends to be used to describe organisations and charities, who work in this area rather than local innovators such as hardware hackers (Hersman, 2015) who attempt to solve technical problems in developing countries. This might include the numerous attempts by individuals to 'hack' mobile phones to hold more than one SIM card or 'tether' mobile phones to act as internet connections. However, I was partly concerned with the relationship link between hardware hacking and ICT4D which meant that it was useful to consider them together.

The Network Society and Hacking

1) Changes in Informational Work

As described above, one way which it has been argued that Network Societies differ from previous forms is in terms of changes in informational *work*, in other words an increased focus on professions relating to the management of information. This change is represented by, among other things, a “new class” of IT professionals, albeit in relatively small numbers, who have a significant impact upon society, sometimes in humanitarian and socially conscious ways (Bell, 1973, p.220; Webster, 2006, p.8-32).

A decentralisation of society has brought with it a move *away* from the situation in which a relatively few multinational organisations or nation states control information and instead towards individual innovators (Castells, 2000) who develop local and appropriate ICT. I would argue that the ‘hackers’ involved in the ICT4D movement, these Civic Hackers, represent an example of this trend in that they tend to move control over ICT away from states and corporations and into the hands of end users.

There is an increase in creativity and personal drive which typifies the network society, what Castells calls the ‘spirit of informationalism’ (Castells, 2000; Webster, 2006, p.105). This idea can be extended to suggest that a Hacker

Ethic is evident today, being a combination of adventure and lawlessness in which the motivated work for the "*hell of it*" (Himanen, 2001; Webster, 2006, p.105). As described in the previous sections, I was concerned with whether this Hacker Ethic is spreading to wider areas of society and so these concepts were of relevance.

2) *Information is not evenly distributed*

My previous analysis of hacker literature also revealed a relationship to concepts of equal access to information. Theories of Network Societies also provide some insight into the ways in which information (and indeed information technology) is distributed across society which has important implications for the study of hackers, particularly those motivated by a desire to solve social or humanitarian issues.

Access to information has a greater symbolic efficacy than the actual content of the information in question and full participation in a network can be viewed as a prerequisite of participation in wider society (Castells, 2000; Webster, 2006, p.106). This idea is closely related to the concept that information should be free and available to all, a central argument to the Hacker Ethic described in my previous chapter and therefore provided an important analytical device.

On the other hand, while access to ICT is indeed important, those accessing technologies also require the skills and knowledge to use its language, code and logic. This may explain why the focus of much ICT4D work has been on education and the production of locally meaningful artefacts. Both Castells and Himanen, I would argue, also fail to provide sufficient evidence that the symbolic importance of access to networks of information is of greater importance than the content of that network, and there is a lack of first hand research to test this position.

The *commercialisation* of information has decreased its access by 'poorer' groups, leading to a struggle between the public and the private appropriation of such technology (Schiller, 1996; 2000; Webster, 2006, pp.125-160). Emphasis on the goal of success in the market has driven scientific and technical knowledge away from pursuit of knowledge for its own sake and improving public services (Dickson, 1984; Webster, 2006, p.138). This can be seen in a range of contemporary areas from academia to public media in which financial pressures are forcing the emphasis towards profit focused strategies. I was keen to explore the ways in which hacking might provide a potential antidote to this in that the ethics of free access to information and the channelling of this information towards social improvement have been heavily rooted in hacker culture from the beginning. This information inequality of network societies has forced certain groups more than others to the fringes of informational capitalism (Webster, 2006, p.111). Castells comments that this has *"…pushed nations such as Zaire and Uganda to the margins of the global network society, condemning them to eke out existence by the 'political economy of begging'.…"* (Webster, 2006, p.114).

It is incorrect, however, to argue that such marginalisation is a *cause* of poverty, a technologically determinist argument. While lack of ICT certainly amplifies its effects, I chose instead to frame it as a symptom of other inequalities in terms of education and economic wealth within my own research project.

3) *ICT as a social construct of the North Atlantic*

Another way in which I chose to approach Civic Hacking was by considering the cultural bias inherent in technological artefacts. Informational inequality can have a significant impact upon developing nations outside Europe and North America. A requisite of giving voice to poorer nations' attempts to overcome poverty is to challenge "information imperialism" (Schiller, 1996). Currently, the world's information environment overwhelmingly emanates from the Western nations, especially the United States. There is a media dependency on the west which reinforces this cultural imperialism, an informational means of sustaining Western dominance. This argument was powerful enough to influence UNESCO policy (Webster, 2006) and much of the ICT4D movement has also been focused on this idea of developing culturally appropriate solutions (Ekine, 2010; Heeks, 2008). This also has a clear relationship with hackers who modify technology to make it more appropriate and thus formed an important jumping off point for my research.

The social construction of technology has been largely dominated by the West and often 'imposed' upon developing countries, resulting in both positive and negative appropriation (Miller, 2011, pp.160-161; Prahalad, 2006; Chambers, 1997). As discussed in the previous section, hacking has been heavily influenced and shaped by the politics, culture and philosophy of western societies. This produces some interesting questions regarding how technologies such as the PC, TV or the mobile phone, for example, would look had they been developed in, say, sub-Saharan Africa. A broad spectrum of scholars has argued that technologies are socially shaped as the artefacts of particular cultures, and that these cultures have tended to be dominated by groups, often comprised largely of males or from western nations (MacKenzie and Wajcman, 1999; Barker and Downing, 1980; McCormick and Sanders, 1982; Dyer, 1997; Frost and Sullivan, 2003, cited in, Castells et al, 2007).

Whether for pragmatic or cultural reasons, many areas of the world have modified technologies such as mobile phones and software to make them more locally appropriate (Castells et al, 2007; Ekine, 2010; Frost and Sullivan, 2003, cited in, Castells et al, 2007; O'Neill, 2003) through what might be described as a form of 'hacking', as defined in the previous chapter. I would suggest that many of those involved in ICT4D projects might also be described as hacking since they often make use of hardware and software hacks and express the Hacker Ethics described previously. There is, however, little in the current literature which explores this idea so it represents a significant research gap. This idea will be discussed in greater depth later in this section and formed an important theme within my research.

There is a paradox represented by the conflict between the communal openness of the Hacker Ethic and the *"cult of the individual"* at the heart of libertarianism (Jesiek, 2003, p.10) which I have already touched upon in the previous section. This draws on a definition of 'Libertarian', based on European rather than North American philosophy, which provides us with a solution. In this construction, libertarianism is about defending the wider freedoms of the individual in society as opposed to a North American distrust of centralised authority and expectation that individuals will look out for themselves.

> *" ....In Europe, it refers to a culture or ideology based on the uncompromising defense of individual freedom as the*

> *supreme value — often against the government, but sometimes with the help of the governments, as in the protection of privacy ....” (Castells, 2001, p.33)*

As discussed earlier, European philosophy has been incorporated into the Hacker Ethic, shaping the ways in which the technologies hackers produce are constructed, taking the form of a greater democratisation of technology and the use of technology for social good. This argument contradicts much of the previous literature into hacking which, as I have shown, frames it as a largely North American construct and often focuses on this mistrust of authority and government. An exploration of the relationship between hacking and mainstream business (Himanen, 2001; Kelty, 2008) or corporate sponsored *charity (*Random Hacks of Kindness, 2010), however, suggests that this approach may hold some weight. Here, however, we must return to an important omission. Within this argument there is no mention of what influences might shape the behaviour of hackers outside of North America or Europe, for example by South East Asian or South American cultures and how their technological outputs might be shaped by these different experiences. In common with other scholars, Jesiek frames hacker technologies as artefacts of economically wealthier, and therefore arguably more globally dominant, European and North American cultures. It is unclear whether it is cultural bias in the literature which is constructing this representation or is the result of a genuine inequality between regions, however, I would argue that there is a need for further research into how technology is being constructed and modified outside the more economically dominant societies of the North Atlantic. This theoretical framing was useful in terms of approaching Civic Hackers who aimed to address these types of inequalities while themselves often originating within these 'dominant' global cultures.

So, as we have seen, theories of Network Societies suggest that information and ICT is central to industrialised society, that these commodities are not evenly distributed globally and that these technologies tend to be a construct of Western societies which are imposed upon developing countries. But what is the relevance of this to hackers? The idea of democratising technology is closely tied to the original Hacker Ethic of information equality and freedom which I have already described. This, I would argue, is a key feature of the ICT4D movement and groups I would refer to as Civic Hackers so would prove useful to my research. But first, I shall discuss the unequal nature of access to information in more depth.

The Digital Divide

Having considered the importance of informational networks to contemporary society and the relationship to hacking, I will next explore theoretical concepts relating to inequality of information access as this relates to my research project. "*Half of humanity has not yet made a phone call*," Thabo Mbeki claimed in 1996 during a speech at the Information Society and Development Conference (Shirky, 2002). Although the empirical accuracy of this statistic is questionable, it does reveal something of the growing importance of the inequality of access to ICT and its role in political policy making.

There can be little question that inequality of sorts in terms of access to technology exists both between groups and individuals within society and among societies globally. What this divide is, on the other hand, is somewhat less clear. The term ‘global digital divide’ has also come to be of increasing importance to signify the lack of ICT access *between* so-called economically ‘developed’ nations and ‘developing nations’ - although this terminology can, in itself, be problematic (Chambers, 1997; Willis, 2005).

There is a range of empirical data which shows that not only is internet access increasing in the developed world but that global inequality of access to the internet is a distinct problem (Pick and Sarkar, 2015). Only 15% of the world’s population accounts for 88% of internet usage (Rahman, 2009) and this kind of inequality is likely to have a negative impact on those within a network society since technology allows for a better distribution of knowledge. The complexity and cost of the internet, however, may serve to intensify existing social inequalities, or even create large groups of “*misfits*”; people who do not find a place within a network society (Van Dijk, 2006, p.3).

On the other hand, one must be wary at this stage of straying into technological determinism. It would be false to suggest that, if the developing world had the same level of internet access as, for example, New York, its social and economic problems would be solved. After all, I would argue, it is not lack of technology causing poverty but rather poverty itself which results in a lack of technology.

It could be argued that ICT has become a ‘*dominant language’* (Bourdieu, 1991) of network societies. Those who possess control and skill over this 'language' might have power in other aspects of life while those who do not are excluded (Hindman, 2009). This inequality can be amplified through "*The Matthew Effect*" (Merton, 1968) or in other words, 'the rich get richer'.

Addressing this imbalance is partly about *access* to ICT in terms of skills, culture, motivation or materials (The Economist, 2012). Being an influential member of a contemporary network society requires the skills, motivation and opportunity to interpret a wide range of signs and symbols. The ability to make such interpretations gives some members of that society symbolic power or indeed material power while for those who cannot, or choose not to form such interpretations, it excludes them from this power. Such groups and places may become "mechanisms of reproduction of social devaluation" (Castells, 1999, p.33). The inequalities highlighted by network societies can also affect certain groups more than others.

> *"…there are growing segments of semi employed, in and out of the labour market, creating a potential danger for some individuals, particularly among minority youth, to join the ranks of the criminal…"* (Castells, 1999, p.33).

On the other hand, Castells does not explain what causes certain groups to be affected more than others nor fully provide examples of such cases. Theoretical understandings which imply that lack of ICT causes social problems have been much criticised (Winston, 1998; Bornstein and Davis, 2010), particularly among ICT4D practitioners since they are seen as a form of 'technological determinism' which implies that lack of ICT is a *cause* rather than a *result* of deprivation.

Critiques have also increasingly focused upon what is known as the 'second-level digital divide', an emphasis upon inequalities in *production* of digital materials not just in access to them (Korupp and Szydlik, 2005; Attewell, 2001; Natriello, 2001). So, for example, the fact that a majority of internet blogging or software development still derives from a small number of companies and individuals, although a greater proportion of people have access to those products.

Despite criticism regarding the term Digital Divide, however, the argument that information is not equally distributed both globally and within societies can be evidenced (Castells, 2001; Pick and Sarkar, 2015; Korupp and Szydlik, 2005; Attewell, 2001; Natriello, 2001). Theories of Network Societies may help explain this due to the fact that information systems have become a primary way of organising society and therefore lack of access to ICT can increase some of the wider social problems experienced by certain groups (Van Dijk, 2006; Bornstein and Davis, 2010). My study was concerned with the ways in which Civic Hackers approached development challenges through technology so these theoretical underpinnings proved useful.

The Pragmatism of the Hack: ICT4D

Given the challenges of information access discussed above, the ways in which groups have attempted to address these issues has relevance to my own research since Civic Hackers are involved in these types of interventions. In this next section, I shall offer examples of ICT4D projects and other uses of IT to address social issues which I argue represent a type of hacking and which relates closely to my research on Civic Hacking. It should be noted that examples of such 'hacks' are very limited, especially first-hand data, which is part of what my own research aims to address. What research has been carried out in this area has tended to focus heavily upon mobile phone technologies since, due to demand and access in certain parts of the world, mobile phones are where much of this work has been carried out (Ekine, 2010; Castells, 2001; Donner, 2007).

There is a strong sense in which Civic Hackers engage in part of a wider global debate regarding ICT and development. Since 2003, the United Nations (UN) has facilitated a World Summit on the Information Society (WSIS) which aimed to bring together various organisations to set a policy agenda which promotes a more inclusive information society (World Summit on the Information Society, 2017). This has brought together traditional policy makers with 'non expert' multinational corporations and grassroots NGO activists in a multi-stakeholder participatory model. While this bottom up approach to international policy making was initially met with enthusiasm from activists, it has ultimately presented challenges for these groups (Franklin, 2007). The need to address wider issues, work within existing UN styles and deal with organisations who had differing ideologies increasingly led to dissatisfaction. The private sector has become the main sponsor of the ICT4D movement among mainstream governments. This presents a conflict of interests in the eyes of grassroots activists who do not approve of the UN embracing this partnership. These corporations are often seen as using this ICT policy agenda to their advantage to exploit new markets (Tarrow, 2005; Smith, 2005; Boas, 2004; DeMars, 2005). In fact, attempts to address development and poverty through

ICT under the advice of organisations who may not best understand local realities set the conditions and social justice may not be at the forefront of their agendas. On the other hand, multi-stakeholder platforms (such as the UN) have demonstrated that partnerships between UN agencies and private sector can marginalize grassroots activist groups (Gurumurthy, 2003). Within this space, Civic Hackers can be seen as making interventions in this traditional global policy making by providing a platform for local voices and driving this bottom up, community led agenda.

At a local level, there are examples of these ICT interventions influencing both international policy and also private sector innovation (Zainudeen et al, 2006). In many parts of the developing world, a phenomenon often referred to as '*beeping*' (also regionally known as '*flashing*', "*menancing*", "*fishing*" or "*boom call*ing") in which mobile phone users leave a 'missed call' on the recipient's phone in order to communicate, is prevalent (Donner, 2009a; Castells *et al*, 2007, pp.59-66). This practice has become extremely popular in developing countries due to its cost saving benefits and could, I would suggest, be viewed as a kind of hack, although it is important to note that there is no overt use of the term 'hacking' to describe such activity. Based on my previous analysis of hacking, however, there are similarities in that it modifies and manipulates existing technologies, without any kind of official authorization, making them more appropriate to the user's needs. Interestingly, the motivations for this kind of 'hacking' seem to be pragmatic, a way of cost saving and overcoming limitations, rather than typifying the ideology or criminality of other hacks (Alleyne, 2016). 'Beeping' may be informed by pre-existing cultural traits among users such as the expectation that the "rich guy" should pay (Goliama, 2011), providing us with more evidence for the cultural shaping of technologies.

There are a number of M4D (*'Mobile for Development'*) examples in which innovative applications for cheap mobile internet and internet banking can be seen to represent examples of pragmatic hacks since they are involved in the modification of existing technologies. On the other hand, many of those who adopt these technologies are driven by a desire to check football or cricket scores as much as by more practical considerations (Porter et al, 2012). As with other technologies, distribution is not globally equal and much work is directed at addressing this imbalance,

> *"...encouraging higher rates of adoption has become a priority, one factor/lever which could contribute to socioeconomic development." (Donner, 2009a, p.95)*

Donner also argues that often the development of technologies to solve these issues is driven by user development in which individuals modify their own devices. This pattern of modification and adoption is typical of hacker technologies.

There is a strong demand for cheaper mobile technologies in many parts of the world (Porter et al, 2012; Castells *et al*, 2007, p.61; Yee, 1999) and the modification of cell phones to be used as mobile payphones shared among communities or sharing SIM cards between one cell phone (Burrell, 2010) represent common trends. Again, I would argue that such unauthorized modification of technology present potential examples of a kind of pragmatic hack based on my previous definition.

Occasionally, such pragmatism is adopted by mobile phone companies and humanitarians who base designs on this ‘bottom up’ development and grassroots innovation (McKemey et al, 2003) either to generate profit or address inequalities. This type of user driven innovation will be discussed in more depth in the next section.

Finally, it is worth noting that as well as these practical and technologically determinist motives, there can also be cultural reasons why technology is used in different ways, reflecting the culturally constructed nature of devices. For example, family structure and belief systems may contribute to the shaping of mobile device modification and usage, making them expressions of the society in which they emerge. An example of this would be the mobile phone which was designed to suit the requirements of wealthy, individual users rather than be shared among families and communities. The development of technologies in North Atlantic societies may take a very different form from those which are better suited to those in developing countries. This desire to produce technologies which are applicable to their surroundings might be one reason why ICT4D projects often place great emphasis upon local and appropriate, user-led design. This type of innovation in order to make technology more accessible has a clear relationship to Civic Hacking and therefore is important in providing theoretical context for my own research.

2.3.3 Rip, Copy, Burn: Innovation and Hacking

As I have shown in previous sections, hacking often involves the appropriation and blending of existing technologies. This can be used to address inequality. Software entrepreneurship among the urban poor is less likely than among graduates (Amsden and Clark, 1999, p.213). It might be argued that hackers engage in a kind of software entrepreneurship by innovating with new technologies. Although still a statistical minority, hackers from low income backgrounds may challenge this notion by demonstrating that hacking may increase the opportunities for those without formal education to participate in software innovation and this can be a way of bridging such divides.

This section explores the relationship between hacking and theories of user innovation, suggesting that a key part of the Civic Hacking movement is collaboration and a desire to produce more appropriate responses and avoid the '*cultural imperialism*' discussed above. This demonstrates how my research is situated within and contributes to an existing body of literature on innovation.

Read Only: No Such Thing as 'New'?

I have suggested that hacking can involve taking a previously existing technology and modifying it to achieve a different purpose; in some cases, to solve humanitarian or social issues. The idea of appropriation of existing technologies to suit specific user needs has been discussed in relation to the study of innovation (Haddon, 1992) and any innovation relies upon borrowing from what has gone before (Richardson and Boyd, 2004). There are parallels here with modification through hacking which my study aimed to explore.

The most significant inequality is not a result of *access* to a piece of technology, but the ability to understand and write the language of that technology. As Lessig states, "*most of us in today's world are observers, passive recipients, consumers, rather than modifiers*" (Lessig, 2004, pp.36-37).

On the other hand, new knowledge and practice can emerge from those who are excluded from mainstream economy (Tuomi, 2003). Zachary (2004) provides interviews with hackers in Ghana which supports this argument that innovation can be driven by the exclusion from legitimate forms of IT which can result from poverty,

> *"Sohne thinks that African computer people are compelled to be creative and resourceful. They must live by their wits — and pluck whatever they can from the discarded high–tech materials that turn up in Accra's digital dung heap.... To Guido Sohne, the "hacker" as a social type is a driven programmer who persists even in the face of daily humiliations and in the absence of a decent educational system. To Sohne, the hacker is a new kind of African nationalist who draws on free resources (available chiefly from the World Wide Web) to harness the global forces that might transform his circumstances. In taking advantage of the Web and low–cost computers, Sohne envisions a future where at least some Africans*

> *transcending the downward spiral engulfing much of Africa and — against the odds and as an equal partner — joining a global community built around innovation, knowledge–sharing and pragmatism…"* (Zachary, 2004, pp.30-32)

Zachary compares these individuals to the "*hero-engineers*" of the industrial revolution (Zachary, 2004, pp.30-32) although I would suggest that a cautious approach should be taken with regard to such statements. It would be easy to see in these pragmatic hackers, something of the 'pure' Hacker Ethic of 1960s MIT (Bender, 2011) but I would argue this would be to engage in evolutionism and a kind of romanticism which has historically been attributed to those viewed as the '*other*' (Barnard, 2000).

However, the kind of 'lead user innovation' (Gatignon et al, 2015) which emerges from pragmatism has much in common with hackers and often creators of innovative technology understand the futility of keeping innovations secret since they will eventually be discovered by others (Von Hippel, 2005). Similar to hacking, it is therefore often considered more beneficial to freely reveal and then gain the personal reputation and input of collaborative 'tinkering'. In fact, often the earlier one "reveals", the better for the product (Raymond, 1999). This element of the Hacker Ethic which I have described can be seen in many open-source projects, most famously Linux. My own research aims to show that this ethic is often also a key feature of ICT4D hacks since they often involve open source innovation.

Empirical studies from the West suggest that user development and modification is widespread (Shah, 1999). Examples from the developing world, however, are fewer and more anecdotal. 'Lead users' are those who experience challenges before the rest of the marketplace, and as these challenges are likely to become common problems, solutions need to be found. The more a user meets this definition, the more beneficial their innovation tends to be (Von Hippel, 2005).

There is a weight of evidence to suggest that technology is biased towards certain dominant groups, be it through gender, culture or language (Li and Kirkup, 2002; MacKenzie and Wajcman, 1999; Barker and Downing, 1980; McCormick and Sanders, 1982; Dyer, 1997; Frost and Sullivan, 2003, cited in, Castells et al, 2007) and that those who are excluded from those dominant groups may innovate by modifying these technologies in order to make them more appropriate (Johnson, 1997; Zdenek, 1999; Feenberg, 1999).

Users tend to innovate when products do not meet their needs (Von Hippel, 2005; Castells et al, 2007). This has been very much the case in developing countries since, as mentioned previously, many dominant technologies emerged from North Atlantic societies and may not be suited to these countries. As Jesiek notes, many of these technologies are open to adaptation through innovation,

> *"...we may take for granted the form and function of telephones, bicycles, and perhaps even computers, but the ongoing evolution of these and other objects remains at*

> *least nominally — and in some cases substantially — open to alternate pathways of development."* (Jesiek, 2003, p.5)

The following story provides an example of such a situation, and one in which this innovation led to mainstream adoption of new practices,

> *"Much to the chagrin of the Icelandic population, Microsoft announced that it would not offer an Icelandic language version of its Windows 98 operating system....In response to this roadblock, enterprising hackers looked to the open source world for alternatives. KDE, one of the more common desktop environments for the open source Linux operating system, was soon developed into an Icelandic flavour. And while subsequent releases of Microsoft's operating systems — including a Windows 2000 multi-lingual edition and all versions of Windows XP — offered an Icelandic language option, it might not have happened without the pleading of Icelanders and the active search for alternatives. In this case, the open source model of software development facilitated a rapid reaction to specific social values and goals, namely the preservation of native culture via the Icelandic language, while the closed commercial developer lagged behind."* (Jesiek, 2003, p.6)

However, user innovation can be cost saving (Von Hippel, 2005) which has implications for hackers in developing countries and the ICT4D projects which work with these 'lead users' to develop solutions. My project aimed to explore this idea by researching Civic Hackers who were involved in a type of innovation to produce more appropriate technologies.

Technology is Created by Users - Communities of Practice

Collaboration is another key feature of the Hacker Ethic which I have described and represents a globalisation of collective action which can be seen from Wikipedia to the Linux development community (Paulus and Nijstad, 2003) and within the Civic Hackers who I intended to base my own research around. Collaboration is also important to innovation. In fact, one interesting feature of hacktivism, as noted earlier, is that despite the fact that these groups often do not actually 'hack', by breaking or modifying computer networks, they still express an aspect of the Hacker Ethics due, in part, to their collaborative nature. Despite the fact that popular accounts of innovation, as with hackers, tend to focus on the *lone* 'hero inventor', many innovations have been collaborative (Tapscott and Williams, 2006; Surowiecki, 2004), driven by those using the technologies. In fact, this kind of group driven user innovation creates an argument for a heroic *user* rather than a heroic inventor (Antorini, 2005, cited in, Von Hippel, 2007, p.23). So, the motives for hacking can benefit both the group as a whole or the individual. The Linux hacker community, for example, has been described as an "*innovation economy*" and in that it is interested in itself as a group although interestingly not the greater good of society (Tuomi, 2003, p.209). Civic hackers, on the other hand, may challenge this view since they are primarily aimed at benefiting wider society.

There is a relationship here to the idea of technology as a socially constructed artefact which is partly a creation of its users rather than as an objective product. The use of a technology assigns its meaning and without this meaning, technology is just physical matter (Williams and Edge, 1996). It is important to note that innovations should be viewed in terms of their meaningful appropriate role in society (Silverstone and Morely, 1990). Innovation is about creating new meanings and new social practices as well as producing physical objects. For example, Henry Ford invented the Model T car but he did not assign the meanings of cars, which were provided by its users and society at large.

If technologies are socially constructed by users, innovations emerging from developing countries are likely to look different from those from countries such as the USA. It is possible to imagine that a television, web browser or mobile phone may possess different attributes as it is a reflection of the habitus out of which it emerged.

What motivates people to innovate may therefore also help us understand the motivations for hacking. The motivation of individual exploration, for example, has similarities with the Hacker Ethic discussed previously. There are studies which evidence the fact that certain groups feel happy when they innovate and that such exploration draws on the novelty the user finds in breaking conservative institutionalised forms of practice (Tuomi, 2003, pp.25-27). This kind of rule-breaking is essential to hacking. The strong relationship between innovation and hacking demonstrates the importance of understanding one in order to understand the other and therefore formed a significant aspect of my research.

My initial interest was to study the ways in which Civic Hackers attempted to address inequality through more appropriate technologies. Various researchers have discussed the appropriation among and penetration into societies of mobile technology (Papa and Papa, 1992; Venkatesh et al, 2012). Although this approach can be quite technologically determinist in nature, it does provide some insight into the production of technological meaning by user innovation. According to this view, a piece of technology is the result of certain choices by the manufacturer and is therefore not a neutral product. Instead, it embodies power relationships between the manufacturer and the user and thus is inherently political (Horst and Miller, 2006; Horst, 2006). Bar et al (2007) use the metaphor of cannibalism to describe this appropriation of technology. In their view, cannibalism is the appropriation of the body in which it is consumed, swallowed and then made into something new.

The concept of learning by doing, experimenting, 'bricolage', tinkering and exploring to advance ones' own knowledge is often done as part of a community and in collaboration with users (Levi-Strauss, 1966). This type of 'hacking' by users challenges power structures and constructs technologies which are more appropriate to local needs. This is the basis for many ICT4D projects;

> *"The long-term, innovative effects occur when users appropriate the technology, when they make it their own and embed it within their lives. The appropriation process is fundamentally political: it is a battle for power over the configuration of a technological system and therefore the definition of who can use it, at what cost, under what*

> *conditions, for what purpose, and with what consequences. This confrontation, we argue, is deeply creative and fuels a powerful innovation engine. Users re-invent the technology while they try out its features, tweak devices and applications so they better answer their needs, come up with different ways to use services, and develop new social, economic and political practices around the possibilities open by new technological systems."* (Bar et al, 2007, p.2)

I would argue that it is possible to see similarities here with the Hacker Ethic described in section one. The negotiations and resistance between user and those in power are a link between hackers, innovation and the ICT4D movement;

> *"Usage in turn progressively reveals the politics embedded within the technology's original configuration, gradually disclosing who really is in control. Soon however, users begin experimenting with their cell phones, exploring how they might adapt them, or adapt their practices around them, so the technology better serves their own interests. They may modify the device, download or program new applications; they might invent new unintended uses for the technology, or invent new practices that leverage its possibilities. We view this experimentation process in large part as an attempt to re-negotiate the power relationships embedded in the technology. This creative*

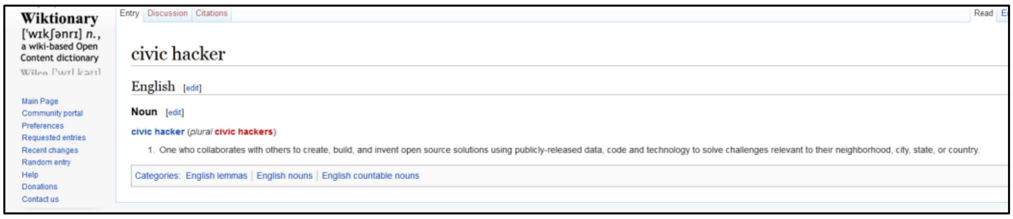
> *re-negotiation process is the core of what we call appropriation, the process through which users take something external (alien, or foreign, something given to them by others), and make it their own."* (Bar et al, 2007, p.3)

2.3.4 Conclusions

Theories of Information and Network Societies provide a useful stance from which to understand the role of hacking in contemporary society. Networks of information are a central feature of society and also the primary sphere in which hacking interacts. These theories also provided me with a useful starting point for my own research into Civic Hacking. Technological innovations are often created by users and communities of developers working together. This is a key feature of the Hacker Ethic and is, I would argue, one of the reasons why hacking forms part of the ICT4D movement. Collaboration with local users of technology often means that the results are more appropriate to their needs. Such projects seek to address inequalities in the way in which information is distributed globally so a discussion of network society theories is important to understanding the often-unequal distribution of information between and within societies. Although there are a number of criticisms of these theories as outlined in this chapter, they do help us to understand a potential relationship between the Hacker Ethic and the ICT4D movement.

It was clear that these ideas would be key features of any research into hackers who are motivated by humanitarian causes. On the other hand, it also highlights the distinct lack of social research into this area, a gap which I aimed to address through my research.

From the figures below (Fig. 1 and Fig. 2), it is apparent that, by 2014, the term Civic Hacker had entered the online vocabulary. The volume of mainstream media sources dedicating resources to covering this issue can be seen as indicative of its increasing emergence as a social movement. Google trends demonstrates the relative level of search interest in Civic Hacking which emerged from nowhere around 2013 onwards. This is particularly significant when contextualised against the gradual downward trajectory of 'hacking' as a search term since 2005, although still relatively high.



civic hacker

English [edit]

Noun [edit]

civic hacker (plural civic hackers)

1. One who collaborates with others to create, build, and invent open source solutions using publicly-released data, code and technology to solve challenges relevant to their neighborhood, city, state, or country.

Categories: English lemmas | English nouns | English countable nouns

Figure 1 Wiktionary Result for Civic Hacker, Wiktionary

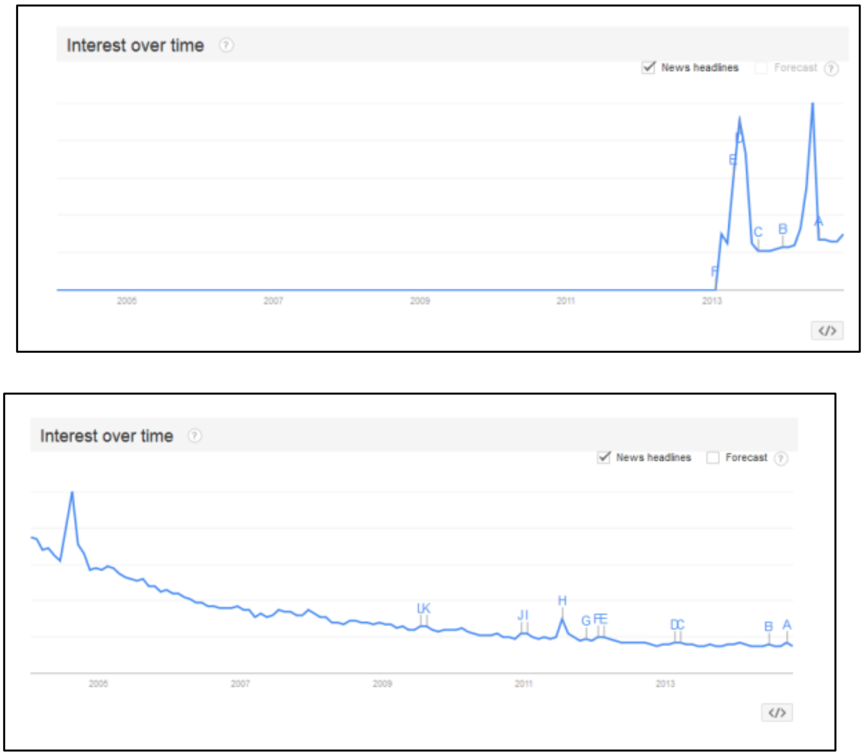


Figure 2 Google Searches 'Civic Hacking' (top) vs Google Searches 'hacking', Google Trends

2.4 Chapter Conclusions: Building on Previous Research

In the previous sections, I have outlined the existing body of literature which was relevant to my own research project and which allowed me to formulate the conceptual framework which I employed within my thesis.

As shown above, substantial work has been conducted into the nature of hacking from a sociological perspective (Jordan, 2008). In many cases, this was found to present hackers in quite binary terms, portraying them as either heroic

(Levy, 1984) or deviant (Sterling, 1992). To try and address the limitations of this approach, I intended to employ a more rounded framework developed by authors such as Kelty (2008). In particular, my research would conceptualise hacking as a set of non-technologically specific practices described as Hacker Ethics (Kelty, 2008; Himanen, 2001; Levy, 1984). These would form the basis for my own research into Civic Hacking.

A starting point for my research would therefore be to avoid a technologically determinist stance and instead draw upon work which supports the social shaping of technology (MacKenzie and Wajcman, 1999; Pfaffenberger, 1988; Sherry, 2005). The above literature on hacktivism also indicated that hacking does not always need to involve technical 'hacks' as such but can include activities such as use of internet privacy tools. Building upon these theories, I wondered if this notion of 'hacking without hacking' also held true for Civic Hackers. The politically activist aspects of hacktivism and FOSS also seemed relevant to Civic Hacking and I was keen to explore whether libertarian politics would feature within these groups. On the other hand, I was interested to explore whether these were based upon similar ethnocentric notions of hacking, rooted in US ideology.

I also identified literature which took a rather idealistic view of hacking (Turkle, 2007; Coleman, 2003; Stallman, 2002; Barbrook and Cameron, 1995). My research strategy was to take a different direction, one which was more pragmatic in its view of hacking. The approach I intended to follow was best embodied by Raymond (2000b), Kelty (2008) and Lovink (2016).

I intended to build on existing literature which considers the influence of hacking on mainstream society. The approach most relevant to my research came from the work of Coleman (2013) and Kelty (2008) which positions hacking as having informed a number of areas beyond purely hacker culture. These concerns were highly relevant to my own research since Civic Hacking is an example of hacking influencing wider practices. In my own work, I was interested in whether this idea could be applied to Civic Hacking and also to build upon this and develop the ideas further to explore whether hacking was in fact indicative of any wider socially determined changes rather than technological ones.

In researching Civic Hacking, it also seemed relevant to consider literature on technology and development (ICT4D) and 'the digital divide' (Castells, 2001; Franklin, 2007), since Civic Hackers were attempting to make interventions in those debates. Since many of the stances within these fields are to some extent predicated upon the idea of an information or network society (Webster, 2006), these theories were central to my own stance, albeit with a critical approach some of the existing literature. This led me to consider the role which hackers play within such a society, as those who can manipulate informational networks, and the influential position that gives them. A further understanding of the relationship between hacking and humanitarianism came from literature on end user innovation (Tuomi, 2003) and appropriation (Lessig, 2004).

The above literature allowed me to formulate a conceptual framework from which to begin my own research project. It also allowed me to develop research questions which would address research gaps or built upon existing work through empirical data and thus make a contribution to the field. Based on the above, I identified several research questions which would build upon this existing body of literature;

- What are the different types of groups involved in hacking for social good and how are they situated within the wider history of hacking as a culture and practice?
- In what ways are the technological artefacts produced by Civic Hackers shaped by the ethics of these groups and wider social factors?
- To what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?
- To what extent are Civic Hackers indicative of the proliferation of the Hacker Ethic into wider areas of society?
- What type of communities are formed by Civic Hacker groups?

Having discussed, I will next describe the methodological approaches which informed my research project and the ways in which I applied these to my empirical chapters.

Chapter 3

Research Methodology and Methods

3.1 Introduction

In order to build upon the above conceptual framework, I needed to apply a range of appropriate research methodologies and methods to my own data collection and analysis. This chapter provides a description of the research methods and methodologies I used or was influenced by within my project. I will explore how each of the approaches listed below were applied to my research questions, what each offered and how these various different methods relate to each other. This includes discussion of their limitations and ethical considerations.

- Methods informed by Virtual Ethnography, Mobile Ethnology/Ethnomethods, Multi-Sited Ethnography and Conference Studies;
- The study of technologies as cultural artefacts;
- Social Network Analysis;
- Narrative Analysis.

I shall then discuss how these methods were applied to my research as described within each of my empirical chapters (Chapters 4-7) to address my research questions. I shall provide a detailed discussion of how my data sources were selected, and my methods and tools, with a rationale for their use.

3.2 Research Strategy

Ontologically, my research was situated within a constructivist view of social groups, framing the social world of participants as the products of ongoing social interaction, and therefore making use of qualitative techniques and inductive analysis (Bryman, 2008). Epistemologically, my approach was interpretivist in nature, attempting an understanding of Civic Hackers rather than an explanation of their behaviour (Eriksen, 2001).

I employed a grounded approach in which my theory developed from the data collected and fed back into an ongoing process of analysis (Silverman, 2013, p.108). This strategy made sense within my own project and related to the particular methods selected, as described below. Although I began my research with a set of broad questions and theoretical frameworks, these were continuously reviewed based upon my findings. This also built upon the theoretical framework discussed in chapter 2.

3.2.1 Rationale for Using Multiple Methods and Methodologies

Within my research, I made use of a range of quite different methods and overlapping methodological approaches so I shall show how these form a consistent whole and provide some justification for their selection. The methods discussed in this chapter are linked together by the common epistemological approaches described above. All of my methods are consistent with an approach which treats my research subjects' views of the world as being socially constructed. This extends to a particular stance regarding the relationship between technology and society, one in which technology both informs and is informed by society.

I began my research process with quantitative methods such as online data or Social Network Analysis as a starting point and then 'fleshed it out' with qualitative methods including participant observation and interviews.

I made use of online and offline data sources, an important technique when focusing upon a group such as hackers who live and work in both online and offline settings. When exploring themes such as the communities formed by Civic Hackers or their narratives, I began with online data from forums, social media or search engines and then found the offline qualitative data to test my ideas. For other themes, for example the ways in which technological artefacts were shaped by Civic Hackers, I placed myself within an offline 'real world' situation such as a hackathon and then went online to capture different aspects of this event.

One criticism of this selection of methods would be that they were too many and too contrasting, however, there are several reasons why I considered that these methods and approaches were best suited to address my research questions:

1) My research subjects spent a great deal of time online and tended to mix their online and offline lives relatively easily. This approach of combining online and offline data allowed me to obtain a more rounded and holistic view as well as some level of depth or 'thick description' (Geertz, 1973), capturing the essence of this group. My research often took the form of snapshots or slices of different, but related, times groups and places. So, while this involved using different data sources and methodological techniques, a participant observation approach remained consistent between them. These methods also allowed me to be quite flexible and adjust my ideas as data emerged, while revisiting topics time and again to obtain more data which allowed me to re-test my ideas.
2) I placed a clear emphasis upon finding novel approaches to conventional fieldwork which were appropriate to the subject I was researching. Although traditional fieldwork did play its role, I found it necessary to adapt this to suit the various field sites and subjects I was focused on. Hence, I drew upon influences such as virtual Ethnography, depending upon what was most appropriate.

3) Each different methodology, and the four different research sites to which I applied them, allowed me to address different or overlapping research questions. This was based upon the most appropriate method in terms of addressing my objectives, as I shall describe below. Since the individuals in the hacker groups I was researching were highly mobile and often difficult to define, this combination of different sites and methods proved useful. It also allowed me to triangulate across multiple sites, both micro and macro level. This included the narratives used by Civic Hackers, not just in telling verbal stories, but also through online written text and video. It was also, however, important that these different methodologies tied together into a whole, based upon my overall research aims and theoretical framework (see Section 3.1.4).

The above reasons support the rationale for adopting a multi-sited approach by explaining why using one methodological approach or a single field site to approach Civic Hacking. I adopted multiple methodological approaches and sites for data collection because each of these multi-methods of data collection were the most appropriate in terms of addressing my various research questions.

3.2.2 Where does Ethnography Begin and End?

Defining what is meant by Ethnography, and how it is distinguished from individual methods such as participant observation, is an important debate within the social sciences (Franklin, 2012). This debate is relevant to my own research project since I made use of methods which were informed by Ethnography (informal interviews and participant observation) but I would not describe my research as an Ethnography due to the multiple and dispersed field sites involved and the relatively limited time periods I spent immersed within my subject communities.

Ethnography is no longer just an approach used by anthropologists and its influence can increasingly be found in other disciplines (Melhuss et al, 2011), however, anthropology does provide us with some important definitions. Ethnography is typically defined by length of immersion within a single culture in order to provide depth of understanding (Delamont, 2004). The aim is cultural interpretation which goes beyond reporting events and details of experience and attempts to gain an 'insider's view' rather than standing back and giving a detached view. This allows meanings to emerge, rather than imposing them from existing models, and to understand meaning (Atkinson and Hammersley, 1994). It is worth noting that Ethnography can be both a research process and an output, and that a key characteristic is generating a written Ethnographic narrative in which meanings are translated (Van Maanen, 2011).

A number of methods are typically utilised within an Ethnography. Participant observation involves making sensory observations, a mode of being in the world, by taking part in and doing what the research subjects actually do (Sandiford, 2015; Gray, 2013). Ethnography also tends to make use of interviews which are targeted but also quite open, and they differ from more formal interviews and appear more like spontaneous everyday conversations (Agar, 1996), alongside gathering of artefacts, newspaper articles or government reports to support analysis (Eberle and Maeder, 2011).

However, it is worth noting that although Ethnography usually involves participant observation, not all participant observation (or indeed qualitative fieldwork) can be described as Ethnography (Scott-Jones and Watt, 2010). Indeed, most qualitative research involves some form of 'observation'. The term Ethnography is highly contested and has been subject to debate by a number of researchers (Forsey, 2010). Particularly multi-site and virtual Ethnography (see 3.2.1) can be shorthand for fieldwork-based, immersed observations that emphasise reflexivity, and researchers can believe themselves to be doing Ethnography when they are not (Franklin, 2012). Ethnography has based its validity upon going to a location to "spend time with people, to interact with them and live amongst them, and to develop a first-hand understanding of their way of life" (Hine, 2000, p.2). From this point of view, a purely online Ethnography might seem removed from this approach of extended first hand study. Ignoring these online interactions, however, when studying communities who themselves interact this way, and without yourself interacting in this way, will not provide the holistic insight which is so important to an Ethnographic 'thick description' (Geertz, 1973).

This debate is particularly pertinent within interdisciplinary work (Berg, 2009) which moves between online and offline settings (see 3.2.1). On the other hand, as discussed in Section 3.1.2, some researchers have argued that the societies we aim to study have changed and that this dependence upon immersion in a single site is no longer relevant.

My own research was a mixed methods approach which allowed me to triangulate findings using different techniques, and also to apply the most appropriate method(s) for the research question being addressed (Mason, 1996). It included a strong emphasis on techniques, including participant observation and informal interviews, which are informed by Ethnography. However, my focus was upon a number of different and dispersed communities which did not make it easy to achieve long term immersion. Often, my participant observation within events only spanned several days and therefore it cannot strictly be described as an Ethnography, but it certainly was strongly informed by Ethnographic techniques. I also blended qualitative research with more quantitative methods such as Social Network Analysis (see Section 3.1.2). My research therefore moved between macro and micro level analysis.

As I shall discuss in Section 3.1.2, I also made use of methods informed by mobile Ethnography and Ethnomethods which are influenced by Ethnography but which have been adapted to the challenges of studying contemporary groups and fields which do not lend themselves easily to traditional Ethnography. This was certainly the case with Civic Hackers since they formed a relatively dispersed group of individuals involved in different activities. These methods and field sites therefore formed components of a multi-sited and mixed-method approach which allowed me to address my research questions which were;

- What are the different types of groups involved in hacking for social good and how are they situated within the wider history of hacking as a culture and practice?

- In what ways are the technological artefacts produced by Civic Hackers shaped by the ethics of these groups and wider social factors?
- To what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?
- To what extent are Civic Hackers indicative of the proliferation of the Hacker Ethic into wider areas of society?
- What type of communities are formed by Civic Hacker groups?

3.3 Methodologies

The following section provides background and context to the methods which I made use of in my research;

3.3.1 Virtual Ethnography

Although my own project made use of a number of mixed methods and research sites rather than being an Ethnography, it was heavily informed by Ethnographic methods. However, the nature of Civic Hackers as a globalised, highly mobile group who operate both online and offline meant that some alternative approaches were required. In particular, work on virtual Ethnography was influential for me since much of my qualitative data collection took place within online environments. For the researcher, the study of online communities presents some unique ontological and epistemological challenges (Slater, 2002; Wittel, 2000). For example, the question of where and when this research is taking place arises. As an Ethnographer, one might question what a field site is comprised of and where it is situated (Clifford and Marcus, 1986). Pink suggests that the role of digital devices in shaping the ways in which we interact with and view our environments is increasing and cannot be separated from our 'natural' environment. For example, a range of urban spaces are marked by the presence of digital screens or the constant chatter of radios in the background (Pink, 2015, p.119). This could also be extended beyond the physical surroundings into cyberspace. It is not uncommon for many of us to be simultaneously present in virtual and physical environments by interacting with social media on a mobile phone whilst walking through a real city.

Ethnography is accustomed to dealing with 'the other' (Czarniawska, 2007, p.9). Relatively recently, however, the Ethnographer's *lens* has turned onto 'the everyday' (Amit, 2007), and yet an ingrained feature of the Ethnographic methodology remains; the idea of legitimacy through first-hand experience (Clifford and Marcus, 1986). To a large extent, the internet has challenged this legitimacy since many aspects of culture no longer take place within discrete geographical places in which physical, face to face interactions can take place (Gupta and Ferguson, 1992).

Amit (2007) builds upon this idea in a discussion of carrying out Ethnography at 'home', and the use of telephone contact to remain engaged with informants, which raises some interesting issues in relation to the nature of carrying out Ethnographic data collection with subjects who are globalised and highly distributed. There are unique challenges in conducting fieldwork among one's own community or within communities which are highly mobile. Researchers involved in Ethnography must be willing to adapt their methods to suit these new circumstances, a trait which has always been central to anthropology (Elliot et al, 2017; Van Maanen, 1995). This use of new methods adapted to contemporary field sites (discussed below) was particularly important to my own research since the groups I was studying were highly mobile, globalised and moved between online and offline settings.

A particular research stance is to question the concept that the legitimacy of Ethnography derives from first hand physical travel to 'field sites' (Hine, 2000; 2015). Instead, one might critically approach the relationship between authenticity and face to face contact (Beaulieu, 2004). Online Ethnography is a valid approach when exploring groups who exist in online settings but also forces us to consider the changing nature of societies and to adapt our methodologies to suit (Nadai and Maeder, 2009). These issues which I encountered were also found within the theoretical works discussed in Chapter 2. This was particularly important to my own research since Civic Hackers where not situated within a single, defined site. This made the kind of traditional, in-person interview and observation upon which research legitimacy is predicated difficult.

Boellstorff argues that humans have always lived in virtual worlds and he carries out a philosophical analysis of the nature of reality and what it means to be human (Boellstorff, 2008). He draws attention to unique online phenomena such as the fact that a user of the Second Life virtual world can become 'removed' from their in-game body when away from the computer, thus raising issues about the nature of Ethnographic legitimacy (Boellstorff, 2008).

Miller, on the other hand, has argued that online social networking is not a 'new' practice (Miller, 2011) but rather a new way of carrying out well-established practices, albeit in a sometimes very different form, e.g. global or in a faster way. For this reason, and in sharp contrast with Boellstorff, he carries out a great deal of real-world Ethnography rather than relying solely on internet-based data. Miller and Slater (2000) approached the internet as a set of social practices rather than focusing on the technology as an artefact as such. In this way, they re-evaluated the nature of a fixed-place, long-term Ethnography, instead moving between place and time during their Ethnographic studies.

I therefore found it vital within my own research to incorporate methods informed by virtual Ethnography, such as participation, observation of chat rooms, email and Voice over Internet Protocol (VOIP) interviews, with other methods which were appropriate to the fast-moving nature of digital communities, such as mobile ethnology and ethnomethodology, 'following' technologies as cultural artefacts and Social Network Analysis (discussed below).

3.3.2 Mobile Ethnology and Ethnomethods

These research challenges make the use of both 'Ethnomethods' (Garfinkle, 1967) and 'mobile ethnology' (Czarniawska, 2007) valuable *alongside* methods influenced by virtual Ethnography and more traditional qualitative fieldwork methods such as participant observation and informal interviews. These approaches were useful in terms of my own research since Civic Hackers comprised a mobile community.

A degree of "vulgar competence", a level of proficiency in the society being studied, can allow the researcher to understand, in enough depth, some of the complexities involved with the group they are studying (Garfinkle, 1996). This certainly has implications for the study of groups such as hackers who possess highly complex practices such as computer programming, narratives of technologies and engagement in online debates regarding technology. In the case of my study, the hackers I studied were also involved in academic research themselves and quite self-analytical, making a certain degree of involvement in their 'world' as academics a useful method of obtaining access to data. Within my own research project, I devoted a period of time to embedding myself within the Civic Hacker community, even developing my technological skills in order to integrate more easily.

'Mobile ethnology' refers to a method which acknowledges some of the unique challenges in studying contemporary 'actors ' who are highly mobile and can be present in more than one 'place' at the same time by means of technology. Methods include shadowing actors, diary studies, and 'following' objects and 'actants' (discussed below) (McDonald and Simpson, 2014).

Modern fieldwork means a "field of practice", not simply a physical space or group of individuals (Czarniawska, 2007, p.8). This "symmetrical ethnology", heavily influenced by Latour and his Actor Network Theory (ANT), treats both human and non-human actants equally as part of this wider field of practice

(Latour, 2005). Czarniawska emphasises the importance of "stepping into" this field of practice (2007, p.10) since this is where accounts of these practices are produced. She also argues that the use of this kind of fieldwork can help narrow down internet-based data (2007, p.16) which has often been problematic due to its vast nature.

Thus, changing the nature of traditional fieldwork (Hannerz, 2003) raises the need for a more mobile ethnology and various techniques to cope with some of these issues (Falzon, 2009). Examples of these include;

- Shadowing, for example, essentially involves following particular human *actants* in their day to day lives;
- "Diary Studies" are the analysis of both digital and non-digital forms of narrating past events such as blogs, photographs or asking participants to maintain daily logs. Diary studies present a solution to the problem of Ethnographers being "all places at the same time", when their subjects are highly mobile. Participants can be asked to engage in "observant participation", carrying out their own fieldwork in situations where the researcher would find it too difficult to gain access;
- And, finally, "following objects", whether human or non-human such as a particular piece of software. This technique might, for example, involve taking a piece of software and following it from its creation through various stages. On the other hand, one could look at the 'end' result, a hacker conference, for example, and retrace the processes involved,

allowing the researcher to see within the 'black boxes' which lie behind technologies.

As a researcher, I would argue, the above methods can help to deal with the issues involved in attempting to study a highly mobile and globalised group such as hackers. It is a 'bottom up' approach to carrying out research which addresses the power structures which are often inherent to anthropologist when acting as an "*inquisitor*" (Clifford and Marcus, 1986, p.77). In this way, the separation between 'researcher' and 'researched' begins to blur (Garfinkle, 1996) so that, as Rosaldo (1986) argues, no longer can the Ethnographer hide behind "the door of his tent".

There are a number of anxieties for researchers involved in multi-sited research (Nadai and Maeder, 2005; Hage, 2005). Firstly, that it may appear at first glance to go against the concept of Ethnographic fieldwork as dealing with the *everyday* knowledge of communities through face-to-face encounters while mobile studies may seem more global and abstract (Gustavson and Cytrynbaum, 2003). However, researchers are often involved in the study of global systems and so cannot be confined to a single site (Leonard, 2009). There may be concerns regarding challenges to the traditional 'power' of fieldwork, suggestions that the mystic of fieldwork may be lost in the shift away from location based Ethnographic expertise (Candea, 2007), however, mobile methods in fact reduce the "them-us" dualism often present in research and instead promote a more 'nuanced shading' (Marcus, 1995). This particular methodology has tended to favour overlapping and often contradictory interdisciplinary approaches, particularly studies of science and technology and those involving 'space and place', since modern societies are often, by their nature, mobile. From this perspective, my own research is situated within the sociological study of science and technology while drawing influence from areas such as development studies.

Marcus presents a number of "modes", or techniques, which the researcher can employ when conducting multi-site Ethnography in order to define and trace the movement of their objects of study, all of which are focused around the concept of 'following' (Marcus, 1995). This concept overlaps with constructivist anthropology and cultural studies in which a phenomenon or object can be traced by the researcher and also has something in common with the method of 'shadowing' described above. Following as a method might focus upon a "thing", so in a study of hackers this might be a particular technology or chat room, "people", "metaphor", "plot, story or allegory", which could be discourse regarding hackers, "life or biography", for example the life history of hackers and "conflict", in the case of my research this could be contest between the Civic Hackers and official sponsors of hackathon events.

In a partially online setting such as my own project, the multi-site may be not just physical but online, making it possible for an object to exist in more than one 'place' simultaneously. I therefore decided that a multi-sited research project presented a particularly useful approach for my own research. This allowed me to overcome some of the challenges of studying a mobile and globalised group such as Civic Hackers who are not confined to a fixed site. The various methods employed for this are described in Section 3.1.3 and how they helped to answer each of my research questions while also linking together into a whole.

3.3.3 Conference Studies

One of the places in which hackers often come together at physical locations are conferences and other real-world events (Coleman, 2010). These events formed important fieldwork sites for my own research so I shall consider the emergent body of literature into studying conferences through participant observation.

Garud made use of Ethnographic techniques such as participant observation, interviews and photography, taking extensive notes at conferences over a significant length of time (Garud, 2008). In addition, he also performed textual analysis of conference papers, brochures, pamphlets and presentations (Garud, 2008). Garud argued that such events represent under-studied forums for actors to meet, interact and exchange information about a particular field. These “discourse spaces” are sites of conversation between participants embracing different visions of the future and “selection environments” where certain approaches are legitimised over others (Garud, 2008). In this way, he argued that conferences can serve as settings in which fields are defined, what he terms “field configuring events”. Garud suggested that this makes conferences useful places in which to study new and emerging fields with no widespread agreement as to the boundaries and membership (Garud, 2008). In terms of my own research, Civic Hackers represented one such group in that they also participated in this type of event. Aspers and Darr (2011) also studied a number of ‘trade shows’ in order to explore the role played by these events in constructing the real time computer industry in the US. The authors employed surveys, observations, interviews and informal conversations to test their hypothesis. They conclude that a full appreciation of conferences as holistic events are essential to gaining a deeper understanding of how new fields are created. Coleman claims that they are “perhaps the most significant place for simultaneously experiencing the past, present and future of a project” (Coleman, 2010, p.58).

I identified a gap, however, in the research around the physical places in which those involved in technological innovation, specifically hacking, meet up and interact in person (Richterich, 2017). Despite the importance of online networks to hackers, more than ever hackers participate in and rely on physical spaces (Pawluch et al, 2005). Coleman described the hacker conference (often abbreviated to ‘con’) as a semi-autonomous event, which is participant run, with hosts rather than organisers, giving the impression of something which is relatively unplanned and spontaneous (Coleman, 2010, p.53). This identified importance of real world events to hackers therefore suggested that they would be particularly useful in terms of addressing my own research aims among Civic Hackers.

Hacker conferences formed important field sites where I could observe the ways technological artefacts, narratives and other practices were expressed as ‘rituals’ of confirmation, “social dramas”, in which the lives of hackers are condensed and celebrated within a single real-world event (Coleman, 2010, pp.53-54). Such events have potential for exploring the relationship between virtual and non-virtual domains. For groups such as hackers which are often thought of as ‘virtual’, the significance of these real-world events makes for interesting research in itself and was thus a focus for my own fieldwork.

I also drew upon data beyond the conference itself including the final report produced by the event hosts, Internet Relay Chat (IRC), mailing lists, web pages, wikis and blogs alongside the real (Coleman, 2010, pp.54-57). Analysis of digital objects was a methodology which I made extensive use of in my own research project as I will discuss in Section 3.1.3.

3.3.4 The Study of Technologies as Cultural Artefacts

The field of Cultural Studies provides some useful approaches for the analysis of science and technology. Its influences in the critical theory of subjects such as art and space (Adorno, 1996) from a social and cultural point of view seem to adapt well to the study of code, computer games, algorithms and other features of technologies.

Often, these *Software Studies* take the form of quite specific research projects, focusing on micro-level aspects of software and their relationship with social processes (Wardrip-Fruin, 2009). It is worth stressing at this stage that Software Studies do not comprise a distinct and homogeneous field but can be said to encompass a variety of different disciplines including philosophy, computer science, media studies and anthropology. Manovich (2013), suggests that in fact a large proportion of academic literature which involves the relationship between humans and the modern world could be classed as software studies.

In 'Behind the Blip' (2003), Fuller provided a pioneering discussion of software culture and argued for software as an *object* of study and criticism within the context of its historical, social, political processes. Within my research, I have drawn upon this approach to technological objects when analysing the software and hardware, the *objects*, produced by hackers. Objects, as Turkle (2007) suggests, have the ability to "familiarise theory", to bring it closer to reality through their evocative nature and personal associations. I also explored the relationship between these objects to try to understand what tied them together (Fuller, 2005; Fuller, 2017).

The relevance to my own research derives from, in part, the importance of an epistemology which views technology as a cultural artefact. The idea of technology as socially shaped (MacKenzie and Wajcman, 1999; MacKenzie, 2006; MacKenzie, 2010) forms a central role in my own research proposal and I intended to build upon Fuller (2007) and others, including Kitchin and Dodge (2011) and Chun (2011) by attempting to interpret these artefacts and the societies which produce them. It might be argued that these authors analyse a piece of technology in almost the same way as others might approach architecture, a painting or piece of music from a cultural point of view and this provided me with a way to approach computer code as a form of artistic expression (Cox, 2013). Previous studies have also explored the gendered nature of technology or ethnocentricity in terms of language (Barker and Downing, 1980; McCormick and Sanders, 1982; Dyer 1997; Frost and Sullivan, 2003, cited in, Castells et al, 2007).

3.3.5 Social Network Analysis

Social Network Analysis (SNA) is a quantitative method which allows the researcher to analyse the relationships within a network of individuals (*nodes*). SNA can involve a large number of different metrics and analytical techniques (Scott, 2000), however, the following section covers those used within my project. They were selected based upon their appropriateness to my research aims.

The most basic link (tie) between nodes is referred to as the 'Degree'. In order to assign a level of analysis to the ties themselves, this can be subdivided into the 'In-Degree', the volume of incoming ties, and 'Out-Degree', the volume of outgoing ties. So, for example, this would include a message which is directed towards the individual or which emanates from them. Centrality is also an important aspect and provides a measure for assessing the statistical significance of a node within the network. A high In-degree in Social Network Analysis can be indicative of "prestige or popularity" (Prell, 2011, p.99). In terms of my own research, the following Centrality measures were also employed in order to gain a more in-depth picture of my chosen network;

- Eigenvector Centrality which is a measure of an actor's sum degree, weighted by the degree of the other actors. In other words, it tells us whether someone is connected to other influential people;

- Betweenness Centrality which implies that an individual is a 'bridge' within that network. They would be considered essential to the structure of the network since if they were removed it would collapse. These actors tend to have some level of control over the flow of information within a network;
- Closeness Centrality is essentially a measure of how quickly actors can reach others within the group without needing to go through intermediaries. In other words, how quickly and efficiently they can relay messages through the group.

The proliferation of social media and other online forums has produced a vast source of data for the sociologist and anyone interested in the analysis of how groups use the internet (Shen and Monge, 2011). There are techniques available which allow some of the data from these sites to be extracted for Social Network Analysis using tools such as Gephi and NodeXL. A growing number of articles have made reference to this approach (Hansen, 2011; Hansen et al, 2012; Wohn and Na, 2011; Vergeer et al, 2011; Cormode et al, 2011; Smith et al, 2009).

Methodologies such as these are indicative of the ways in which the internet is changing the social sciences and how we might carry out research. The digitisation of data makes it possible to analyse purely online data such as that from search engines, websites and other digitally 'native' artefacts (Rogers, 2009). Although a new and often under-validated area, studies have used this digital data, including hyperlink analysis and mapping of IP addresses, to inform sociological inferences through Social Network Analysis and Narrative Discourse Analysis (Park and Thelwall, 2003; Smith, 1999).

In their article on mapping Twitter networks, Smith et al (2014) suggest six models which appear around conversation types within Twitter based on hashtags. These are Polarised Crowds, Tight Crowds, Brand Clusters, Community Clusters, Broadcast Networks and Support Networks (Section 3.2). The idea of Broadcast Networks was of particular interest to my own research as it was similar to the types of networks used to describe hackers previously.

> *"The members of the Broadcast Network audience are often connected only to the hub news source, without connecting to one another. In some cases there are smaller subgroups of densely connected people—think of them as subject groupies—who do discuss the news with one another"*
>
> *(Smith et al, 2014)*

Kozinets argues that Social Network Analysis (SNA) can also play a central role in 'netnography' or online Ethnography (Kozinets, 2010, pp.49-55). Kozinets suggests that, while the 'automated' gathering of data through Twitter or from hyperlinks provides a useful source, qualitative fieldwork techniques can allow the researcher to gather data which can be analysed using SNA techniques based on a greater depth of analysis, albeit with a potentially smaller sample. Within my own research project, I combined digital data with more detailed qualitative data in order to provide more depth to my findings.

SNA can be incorporated with the gathering of online data as part of qualitative fieldwork (McDermott, 2010). The use of digital methods such as Sentiment Analysis (Davies, 2011) and Hyperlink Analysis (Marres and Rogers, 2005) have become increasingly important in social research (Lupton, 2015). Digital sociologists should look to combine and recombine the digital objects at their disposal in order to answer social and cultural research questions and "organise a compelling account of an event" (Rogers, 2013).

3.3.6 Analysis of Narrative

It is difficult to find a single definition of narrative since it is used in various ways by different disciplines. For example, narratives have been defined in terms of everything from the plot structure of stories to news articles and even photographs. Narratives can be interpreted from texts, spoken word or visual materials and can take the form of myths, diaries, songs and many other sources (Abbott, 2008). Alleyne, however, poses the question "if narrative is everywhere, is it anywhere?" (Alleyne, 2015) and therefore narrative needs some level of specificity to bound the concept.

Narratives should be defined by their shared "contingent sequences", that is, the consequential linking of events or ideas into a meaningful pattern (Riessman, 2008, p.5). In describing 'what a narrative does', however, I feel that Riessman strays into functionalism, describing narratives as serving particular purposes for an individual or group. It would be better, I would argue, to view narratives as expressions of particular aspects of those individuals or groups.

It is also important to distinguish between the story, what the narrative is about, and narrative discourse, the way it is told. The same story can be told in different ways, through a variety of discourses (Gee, 2013). Narrative is essentially the presentation of a story involving a sequence of connected events in which earlier events cause or influence later events as time passes. Within a narrative, the story time in which events take place, is not the same as the narrative time, in which the narrative is told (Ricoeur, 1980). The telling of this story within a social context, can be described as 'discourse' (Wetherell, 2001). Alleyne explores whether a text can be defined categorically as a narrative or not, or whether it should instead be viewed as a spectrum, with varying degrees of 'narrativity' or 'narrativehood' (Alleyne, 2015, p.78). The 'unit of analysis' for a narrative can vary from a single answer to a question, to someone's entire life story and can exist beyond the individual as constructed by groups, communities and organisations.

It is also worth noting that, as well as analysing 'external' narratives, researchers themselves also *construct* narratives in the course of their data gathering and analysis. For example, the capture of interviews or recording of a field journal create in themselves narratives. At the same time, methods such as transcription and journaling can act as a form of interpretation. This difference between 'Narrative Analysis' and 'narrative of analysis' is an important distinction within narrative research (Polkinhorne, 1988).

Riessman categorises Narrative Analysis into the following approaches;

1. Thematic Analysis: exclusively focused on the thematic content of the narrative;
2. Structural Analysis: concerned with the ways in which narratives are organised;
3. Performance Analysis: analysis of the ways in which narratives are performed;
4. Visual Analysis: the analysis of 'non textual' narratives.

Within my own research, I chose to focus on Thematic Analysis as my primary analytical approach for a number of reasons which developed quite naturally as my project evolved. Thematic Analysis tends to be dominant within qualitative research, particularly those influenced by interpretive phenomenology. It is also more easily applied to participant observation and has been used previously when combining data sources such as field notes, interviews and archived text. These traits were also common to my own methodological approach.

It is important to stress that my approach was not structuralist Narrative Analysis, even when examining the order of events within these narratives. It was, rather, concerned with the content in its complete form more than how it is presented. This is a common approach within thematic analysis, although the lines between the two are sometimes blurred and it is possible to incorporate aspects of structural analysis into thematic analysis (Riessman, 2008).

It could be argued that online research is inherently tied to narrative, or at least textual, analysis. Kozinets describes it as "positioned somewhere between the vast searchlights of big data analysis and the close readings of discourse analysis" (Kozinets, 2015, p.4). Since the majority of online sources such as blogs, social media and websites are textual in nature, the reading and analysis of these texts, narratives and stories are central to this method. Kozinets argues for a methodology which treats different social media streams in a holistic manner.

It is worth considering at this point the difference between first and second order narratives. In other words, are the narratives being told by those involved or rather the narratives which have been constructed by researchers in order to understand aspects of social life (Alleyne, 2015)? For example, Kelty (2008) found that hackers themselves tell narratives of Protestant Reformation (Section 2.2.2) whereas he used his own Ethnographic narrative to try and make some sense of this. Media narratives of hackers are also examples of second order narratives although they could also be studied as narratives themselves. In reality, most Ethnographic writing tends to be a combination of the two.

Since many of the data sources used in this chapter were blogs, it is also worth considering the nature of online blogging as a form of narrative and the potential methodological considerations.

The move from private journaling and diaries to the presentation of self and autobiography through public blogs has presented the researcher with a large volume of online data sources which would not previously have been available. Blogging can be viewed as similar to a journal with the main distinction that it usually has an audience in mind which may change the nature of the types of narratives expressed in terms of form and content (Alleyne, 2015, p.104). Social media sites such as Facebook and Twitter also present a type of online journal or scrapbook through which narratives can be extracted (Alleyne, 2015, pp.107-108).

Dhiraj Murthy (2008) also notes that blogs may blur the boundaries between researcher and subject, allowing a greater degree of interaction and also critique of one's research.

Interestingly, however, many of the blogs included in my research would not be described as 'personal' but rather 'official' blogs which are written and managed by individuals representing the organisations behind Civic Hacking e.g. NASA, US Government. This raises some issues regarding their bias and forces us to consider the ways in which they might differ from more personal blogs in which the narrator is usually quite forthright (albeit within their own bias) and where unrestricted 'rants' or 'brain dumps' are common.

3.4 Research Methods Used For Each Chapter in the Thesis

3.4.1 Background

Current theory suggests that methodology should be selected based on its merits subjected to scrutiny and that a ‘mixed methods’ approach is in favour in studies of online communities (Bryman, 2008) due to the fact that it allows the researcher to test findings against contrasting data sources, obtained through different methods.

I therefore chose to make use of online research methodology running parallel to, and complementing, more ‘traditional’ data collection such as face-to-face interviews and observation which I used to validate and triangulate my findings. This mixed methods approach also included multiple research sites, drawing data from a number of different places, both on- and off-line, by applying different techniques. In the following sections, I will show the relevance of these various sites and methods to my research questions.

All online data, including video and text, was stored using applications such as *CutePDF* and *Zotero*. In addition, I maintained a field diary throughout my research 2011-2016 with my observations and findings.

3.4.2 Chapter Four: Portraits of Hacking

In order to build upon the conceptual framework in Chapter 2, I intended to explore what were the different types of groups involved in hacking for social good. In order to address this research aim, I first carried out a combination of online and offline interviews and participant observation which allowed me to create portraits based around the different types of hacker. From this phase of my research, I identified various themes which I planned to follow up in later research.

Data Sample, Collection and Analysis

During 2010 and 2011, I carried out a sample of data collection and analyses using internet research, participant observation and interviews in order to establish some initial findings regarding my research aims. The results of this study are presented in Chapter 4.

At first, the hackers of my research topic proved a relatively challenging set of individuals to access as an outsider since they formed quite a 'closed' network, reliant upon online forums, and they had a high level of technical knowledge and understanding of jargon which I lacked. Therefore, I approached them by a process of purposive sampling in which I identified a number of 'peripheral' members, ranging from academics to journalists to those with a casual interest in this area, often with similar research interests to my own. These potential informants were identified through initial internet research methods using advanced searching techniques such as Boolean keywords and filtering on date, format or source. The original sample group is shown in Fig. 3 in which the named individuals have been anonymised.

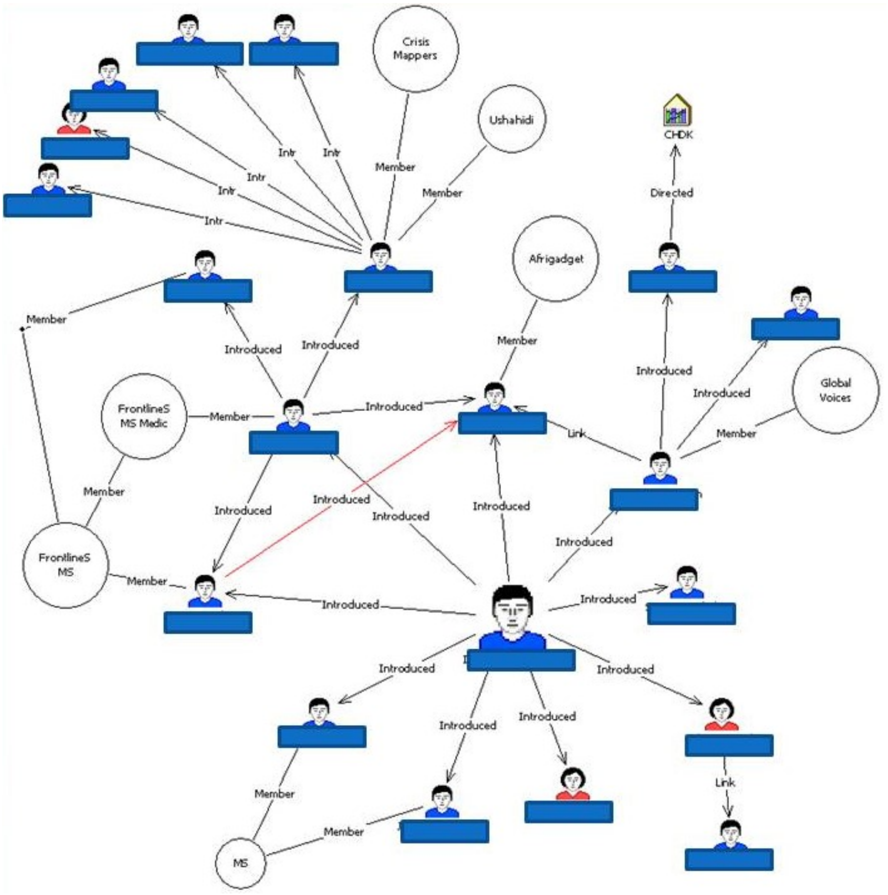


Figure 3 Initial Research Sample of Potential Informants

The response rate to my initial email approaches to these potential informants was relatively high, with 77% responding (n=31 on 06/05/2011). Questions were then either sent directly to these initial respondents, or the respondent provided what they deemed were more suitable contacts, then to these new informants, so that the cohort could be expanded by 'snowball sampling' (Berg, 1988). This provided me with a sample of individuals and groups (n=7) who were increasingly 'closer' to the hackers, upon whom I then focused my research (Fig.4).

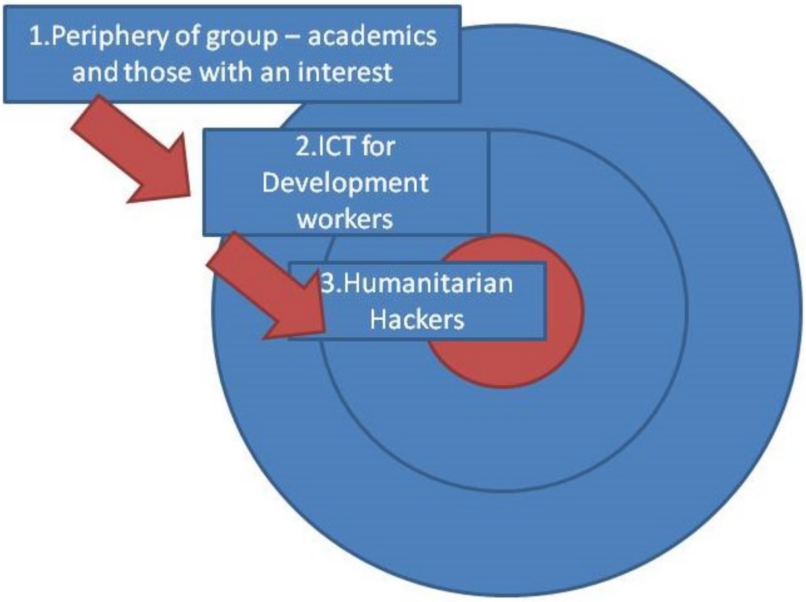

1.Periphery of group – academics and those with an interest
2.ICT for Development workers
3.Humanitarian Hackers

Figure 4 Direction of Access to those Directly Involved in Civic Hacking

Having identified several potential groups of hackers, I then set out to situate them within a field site in which participant observation and interviews could take place. Several of these groups held online and physically located '*hackathons*', one of which I attended at Goldsmiths, University of London, during November 2011 to gather real world interview and participant observation data and to make further contacts. The globalised nature of these groups also meant that they were often located in different geographical regions with no real-world contact. This made it essential for me to 'follow' them in online settings, rather than basing my research within a particular fixed site. My analysis of previous Civic Hacking events suggested that members made extensive use of Twitter, blogs, Facebook and YouTube sites. I therefore also identified a number of online data sources based upon interviews with Civic Hackers which were used by these groups. I then collected data from these online sources which were analysed and interacted with for themes and trends. Interviews, tweets, emails and blogs were then coded (Lewis-Beck et al, 2004). This coding allowed me to identify particular themes and topics within my data and to group them together for further study. Analysis was based upon a sample of seven subjects who were interviewed at various points over a period one year. I also identified conducted online research from social media and websites related to the groups and events. I looked for themes within the data based upon the conceptual framework described in Chapter 2.

I used the results of this data collection to form a series of individual portraits (Miller, 2011). These were grouped around the three types involved in hacking for social good which I identified while conducting interviews and observations; Ethical Hacking (those involved in hacking of computer networks for ethical purposes), ICT4D (those involved in using ICT to address global development issues) and Civic Hacking (those involved in hacking open source technologies to address social issues). By exploring each of these, I then identified a number of themes which I took forward in more detail through my subsequent research.

As proposed by Miller (2008; 2011), I chose to present the data as a series of three portraits which provide case studies of individuals and groups involved in hacking for social good. These are similar to the vignettes, sometimes employed by social scientists to explore an individual's actions in context, to clarify judgements and to discuss with them sensitive experiences (Barter and Renold, 1999). Vignettes can be particularly useful when employed alongside other methodological approaches, such as participant observation and interviews. They also have similar qualities to a biographical narrative although they do not always necessarily follow this structure (Jacobson, 2013).

In 'The Comfort of Things' (2008), Miller describes in some detail the process of producing Ethnographic portraits for the residents of a London street:

> *"I call these chapters portraits because I employ an approach that may have become somewhat passé in mainstream anthropology, a form of holism. A feeling that, in many cases, there is an overall logic to the pattern of these relationships to both persons and things…on this street it seemed useful to see individuals and individual households as somehow analogous to a society. So each of these portraits is sketched, and then filled in, according to what seemed to be the style of those sitting for their portrait…there is no satire or parody, no horrors I set out to expose. I am an academic, trying to listen to and learn from the same materials that are here on exhibition." (Miller, 2008, p.144)*

While not an Ethnographic in the pure sense, my own analysis did build upon a tradition of more narrative descriptions of technologies which includes 'Dreaming in Code' (Rosenberg, 2008), 'The Soul of a New Machine' (Kidder, 2011) and 'Rebel Code' (Moody, 2002). This approach is related to the 'Sociological Imagination', the attempt to explore the relationship between personal experience and wider society (Mills, 1959).

I was initially directed towards a number of the ICT4D projects and individuals by a key academic contact in Spain who carries out research in this area, and from there I was able to 'snowball' to other participants through email correspondence. I also discovered other projects and individuals independently through internet research using keywords in relation to Civic Hacking, and I identified potential informants with whom I then made contact using email. This is one of the methods which led me to realise that many of these individuals were independently known to each other, and that this was not simply the result of bias in my sampling process. I initially emailed a number of informal questions to each participant, who either answered my questions directly by email or else agreed to arrange a more detailed, but informal, interview using Skype. I also met with a number of the participants in person and attended several Civic Hacking events.

Sometimes, research is the result of a personal involvement within a particular group. In my case, I had no previous knowledge of these groups besides an interest in hacking more generally, and this made it more challenging to gain access to the groups and individuals I wished to study. I would argue, however, that it has also encouraged me to approach the topic with new perspectives.

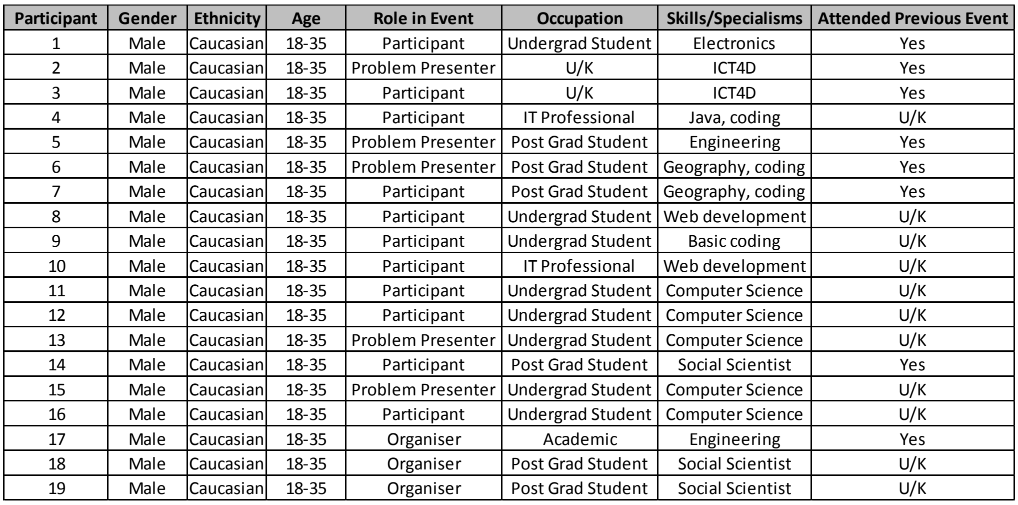
3.4.3 Chapter Five: Event Fieldwork

Having identified Civic Hacking as my research target, I next conducted research based around a particular event (hackathon) which I had identified would be useful in terms of observing the participants' practices, based upon the literature discussed in Chapter 2. Through this, I aimed to address my research question 'in what ways are the technological artefacts produced by Civic Hackers shaped by the ethics of these groups and wider social factors?'. Event Ethnography was particularly useful in approaching this question since it allowed me to observe first-hand the construction of these artefacts within a social context. Several of the themes identified during my research for the portraits (Chapter 4) also featured within this data sample and went on to be important in later research (Chapters 6 and 7).

In this chapter (5), I drew inspiration from previous fieldwork-based studies of hacker conferences (Coleman, 2010) as well as the methodologies of Latour (1999) and Czarniawska (2007) described above. All of these authors have employed shadowing and observation of relatively small groups and individuals through the course of their work, often over the course of just a day, and the 'following' of objects with emphasis upon the social processes which led to their construction.

Data Sample Selection, Collection and Analysis

Chapter 5 was based upon research carried out over a two day period in May 2012, during which, I attended the UK event of Random Hacks of Kindness (RHoK), pronounced ‘rock’, at Southampton University. Random Hacks of Kindness arranges global hackathons in which hackers in different cities meet up to hack together, using open source code to solve social problems. This particular event was made up of approximately twenty attendees, predominantly Southampton University students, all males aged between 18 and 35 years old (Table.1).



Participant	Gender	Ethnicity	Age	Role in Event	Occupation	Skills/Specialisms	Attended Previous Event
1	Male	Caucasian	18-35	Participant	Undergrad Student	Electronics	Yes
2	Male	Caucasian	18-35	Problem Presenter	U/K	ICT4D	Yes
3	Male	Caucasian	18-35	Participant	U/K	ICT4D	Yes
4	Male	Caucasian	18-35	Participant	IT Professional	Java, coding	U/K
5	Male	Caucasian	18-35	Problem Presenter	Post Grad Student	Engineering	Yes
6	Male	Caucasian	18-35	Problem Presenter	Post Grad Student	Geography, coding	Yes
7	Male	Caucasian	18-35	Participant	Post Grad Student	Geography, coding	Yes
8	Male	Caucasian	18-35	Participant	Undergrad Student	Web development	U/K
9	Male	Caucasian	18-35	Participant	Undergrad Student	Basic coding	U/K
10	Male	Caucasian	18-35	Participant	IT Professional	Web development	U/K
11	Male	Caucasian	18-35	Participant	Undergrad Student	Computer Science	U/K
12	Male	Caucasian	18-35	Participant	Undergrad Student	Computer Science	U/K
13	Male	Caucasian	18-35	Problem Presenter	Undergrad Student	Computer Science	U/K
14	Male	Caucasian	18-35	Participant	Post Grad Student	Social Scientist	Yes
15	Male	Caucasian	18-35	Problem Presenter	Undergrad Student	Computer Science	U/K
16	Male	Caucasian	18-35	Participant	Undergrad Student	Computer Science	U/K
17	Male	Caucasian	18-35	Organiser	Academic	Engineering	Yes
18	Male	Caucasian	18-35	Organiser	Post Grad Student	Social Scientist	U/K
19	Male	Caucasian	18-35	Organiser	Post Grad Student	Social Scientist	U/K

Table 1 RHoK Southampton Conference participants

It is worth acknowledging that this data sample is relatively homogenous which may reflect wider lack of gender and class representation across science and technology and hacking specifically (see Section 2.2.3). There would certainly be scope for future work in terms of exploring this imbalance through the study of female focused Civic Hacking groups and also those with a wider race and class engagement.

Running parallel to the 'real-world' event was a linked online infrastructure of blog sites, Twitter feeds, IRC (Internet Relay Channel) and the GitHub online code depository, some of which were officially part of RHoK and others of which belonged to individuals involved. Participants also formed part of a wider network of global events, and during the period of my research, twenty-five events were held across fourteen different countries involving 905 attendees (Random Hacks of Kindness, 2010). The Southampton event was connected directly to some of these other events through Twitter, Skype and live webcams.

In light of my chosen research methodologies, I elected to 'shadow' one particular group at the hackathon for the duration of the weekend. However, I also regularly moved between different groups in order to gain a more detailed picture of the overall event.

My main research method involved participant observation, and I took on the role of attendee at this event relatively easily since many of the others were also postgraduate students. Despite my relative lack of programming skills, I was able to volunteer to help in less technically demanding aspects of the hackathon, and participants were often keen to act as teachers, instructing me as a new member of the group. With the use of a laptop, it was possible to 'blend' into the group, sitting alongside the other members in a circle and observing their actions while recording notes on the computer without this allocating me 'outsider' status. Many of hacker events are quite elitist and are based on an invitation-only system which might be seen to contradict the idea of a 'level playing field', and also may present some problems of access for the researcher (Coleman, 2010, p.52).

I was able to carry out informal interviews and discussions with the majority of participants during the course of the event. Often, this would take the form of unstructured conversations, during a coffee break or as they 'hammered out' lines of code late into the night.

In addition, I also gathered a quantity of online data from the Twitter feeds, website content and chat-logs and. This data would prove invaluable to the study of a group who so freely bridge the gap between online and offline interaction. I captured this data in real time so that I could analyse it afterwards.

In the case of several participants, I followed up these encounters with more formal interviews at a later stage using email, Skype and in person. Some of those I met at this event became important 'gatekeepers' who allowed me access into the closed Twitter networks and blogs which I used in later research (Chapters 6 and 7).

I began by observing the format and structure of the day from beginning to end and mapped out what I felt were the key aspects in my field journal. I then mapped these against my previously noted Hacker Ethics, and also looked for any new traits which were noteworthy. I paid particular interest to any indicators of the motivations of participants for taking part in the event and hacking more generally. I also documented the various stages of the event through photographs. I then went on to look at the structure of the teams at this event and their interactions and again noted down any notable trends and relevance to my research questions. I incorporated observations regarding the use of social media and the ways in which the group were connected to a wider community.

I chose a specific team and followed the process through which they created their code from beginning to end, noting my observations. An essential part this research was the exploration of the code produced by these groups as cultural artefacts. By viewing technologies as social constructions, I was able to 'trace' the journey that these objects took throughout the process of their creation. My aim in this was to interpret what these artefacts reveal about the groups which make them. I also identified commonly used narratives within these events by carrying out participant observation within the groups and noting down frequently-used narrative structures and formats. I was subsequently able to analyse these findings and map them against the Hacker Ethics in order to answer my research questions (see Section 3.4.5 on Narrative Analysis).

Many of the features which I noted during this event were then used to form the basis of my subsequent research on Social Network Analysis and Narrative Analysis (Chapters 6 & 7).

3.4.4 Chapter Six: Social Network Analysis

I next turned my attention to an online methodology in order to explore a different event from RHoK, the 'hack4good' hackathon. This addressed my research question 'what types of communities are formed by Civic Hackers?', building upon the theory described in Chapter 2. Social Network Analysis allowed me to understand the structure and significance of online relationships within this group as they related to a particular event. Several of the themes identified earlier (Chapters 4 and 5) also featured within this data sample and went on to be important in later research (Chapter 7). I chose to focus on a different event from RHoK in order to triangulate my previous findings and because the online data sample was larger which was more useful in terms of Social Network Analysis. I also made use of qualitative methods such as interviews with members of this Twitter network and participant observations among this group to expand upon Social Network Analysis (SNA) and gain a fuller insight.

Data Sample Selection, Collection and Analysis

Twitter is a social networking site which allows users to post and read 'tweets' of 140 characters to the network, in addition to standard social media activity such as messaging. These tweets frequently include 'hashtags' prefixed with the hash symbol ('#') which emerged from IRC chatrooms as part of computer programming jargon. Hashtags allow users to group tweets together under a common banner such as an event. In this case #hack4good referred to a humanitarian hackathon event. Twitter also allows users to 'mention' other users by referencing their user ID prefixed by the '@' symbol, to 'reply' to tweets and to 'follow' users.

A Microsoft Excel add-on called NodeXL was used to extract Twitter data relating to the hashtag #hack4good. This hashtag was chosen as it is related to hack4good, a popular event among the Civic Hacking community and is closely related to RHoK in that many of the same participants take part in both events and their event organisers often reference each other. I felt that this would provide an opportunity to establish whether the themes I noted at the RHoK event were more widespread within the wider Civic Hacker community. I also gathered data from Twitter pages away from the official #hack4good event feed where these kinds of interactions might have been taking place.

Due to constraints with NodeXL, my data collection was limited to 1000 unique Tweets and I focused on those occurring between 21/02/14-01/03/14 during the 'hack4good' event. This involved Tweets from 181 Twitter accounts and their users included both event participants and other actors such as companies and organisations sponsoring the event. It is worth noting that the hashtag around which data was collected (#hack4good) was an official channel so was likely to have inherent bias in the types of tweets and their nature. However, this was the primary hashtag being used so was necessary in order to gather enough data. This fact in itself was also useful in terms of providing opportunities for analysis around the power relations within this group. In this way, the use of this official hashtag was purposeful.

This data sample was relatively small which was important in that it allowed me to carry out more in-depth and detailed qualitative analysis of those involved. Due to the time constraints involved in my research project, it would not have been feasible to carry out qualitative analysis of a very large data sample. Thus, the data upon which this chapter is based is a combination of quantitative SNA and qualitative participant observation. It was important that my data gathering and analysis was driven by my research questions based upon real-world fieldwork rather than being overly defined by the existing technology or available data.

The initial SNA allowed me to define further a network boundary and establish a number of findings regarding the overall structure of the group. Through qualitative techniques including interviews and participant observation, I was then able to add 'thick description' (Geertz, 1973), noting my findings in a field journal. For example, this allowed me to assign certain attributes to nodes (participants) within the network based on their responses. I was also able to assign attributes to the ties (tweets?) themselves. I therefore included 'Directed' ties within my data i.e. the direction of the mention or reply in Twitter, as well as some qualitative data gained from interviews and observations (see Section 3.4.5 for details on Narrative Analysis).

Data obtained from Twitter is typically considered a total rather than partial data sample since all connections are *actual* and there are no *potential* connections within that given sample. By this, I mean that the Twitter users form a complete network population based around a particular hashtag rather than being based around a set of 'egos' (Scott, 2000). In my case, I was required to sample part of this network due to constraints in the SNA software I was using, however, my data should still be considered a total data sample since it still involves all actual complete connections within that given sample of tweets. For this reason, it was less relevant to consider 'Density' within the network, in other words, the number of connected vs unconnected nodes, since all nodes are considered to be connected in at least one way. It should be noted that I chose to exclude Twitter 'Follows' as a relationship tie. This was due to practical considerations regarding processing power since the SNA software I was using only allowed a maximum number of unique results (1000). In order to derive significance regarding the influence of group members or ties within the network I elected to use averages of my total sample as my threshold. For example, the average degree of various SNA measures compared against the group as a whole. The reason for this was that I was not dealing with a particularly large data sample which made it possible to examine each case individually in a more qualitative manner. I was also not working with the kind of factors which could be modelled exactly and instead I deemed it more appropriate to focus on more qualitative methods since there are certain subtle qualities which cannot be seen through quantitative data alone. Therefore, the average was used as a rough guide to narrow down my focus from the initial data sample.

There has been a previous study carried out on hackers using SNA (Lu et al, 2010), however, this was focused on a group of criminal hackers rather than an open-source hacker community as in my case. This is likely to produce quite different findings since criminal hackers are driven by different motives than Civic Hackers. Lu et al's study was also not based upon primary data sources but rather used text mining to gather data on the links between members.

Although SNA has links to qualitative fieldwork such as Ethnography and participant observation, a limited amount of research has been carried out using a combination of online and real world data. Several authors have previously argued that it is important to obtain this balance of online and real world data in order to validate this kind of research (Murthy, 2008; Miller and Slater, 2000).

It is important to note that the data below only represents how active participants were on this Twitter network (#hack4good) so any findings should be, and were, considered alongside other data sources such as real-world participant observation. However, this data sample provided a useful way of triangulating my other findings and of gaining a wider overall understanding of the group in a sociological sense.

In addition, my conversations with research subjects revealed that there were many other closed forums in which members of this community engaged but it was not possible for me to access them. It is also not possible for me to gain access to the private online messaging of my study group, so the data that I gathered represented only one snapshot of this community in action.

3.4.5 Chapter Seven: Narrative Analysis

Finally, I decided to adopt a more macro level analysis than previous chapters to explore some of the wider types of narratives being used within the Civic Hacking community online. This allowed me to address research questions 'to what extent do Civic Hackers express a democratisation of technology?' and 'to what extent are Civic Hackers indicative of the proliferation of the Hacker Ethics into wider areas of society?'. Online narratives allowed me to explore what was important to Civic Hackers through the stories they told and the ways in which they told them. Several of the themes identified earlier (Chapters 4, 5 and 6) also featured within this data sample, so it provided a useful way of triangulating these within a different site and using a different method. Moving from a more micro level analysis, of specific individual events and subjects, to a macro level view of narratives across different sources and periods in time, also helped me to gain a more holistic view of Civic Hacking.

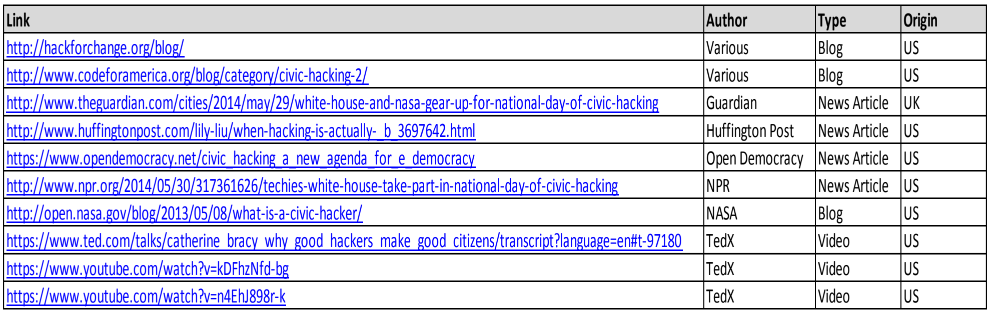
Although I made use of narratives throughout my research, including the narratives of hackers told through interviews, stories told at hacker events and on Twitter networks, within the research presented in this chapter I made use of formal Narrative Analysis as my primary research method. I defined narrative within my research project as a set of “contingent sequences”, the consequential linking of events or ideas into a meaningful pattern (Riessman, 1993). This meant conceptualising narrative as a particular story which its narrator was concerned with. I was primarily concerned with the *content* of narratives; ‘what’ was being said rather than how it was performed. Therefore, I focused on, for example, use of metaphors, and the type of narrative in terms of its ‘structure’, characters and what was being told through this content. Within each narrative were particular narrative ‘themes’ which emerged. Again, these themes were focused upon the content of the story being told rather than looking at themes within the way the narratives were performed in the sense of how narratives were presented or told.

Data Sample Selection, Collection and Analysis

Having identified through internet research that the term “Civic Hacker” had gained in popularity since 2013, I then searched the World Wide Web (in English only) using the Google search engine for news articles, blogs, videos, images and other online material which made use of this term.

The use of the Google search engine has been important in my research methods, therefore it is worth discussing this tool in more detail. A search engine is a tool used to search data which is indexed on the Web. There is an inherent bias built into different search engines depending upon a number of factors such as the way information has been indexed, the way they filter or rank results and the algorithms involved. In order to minimise the effects of any bias, the term Civic Hacking was also searched using the Yahoo, Bing, Ask and Dogpile search engines. The same websites featured in all these search results with only slight variations in their ranking. I selected Google as my primary search engine for this research because it has quite a high degree of functionality and a range of features such as trend analysis which were useful for providing some context to the data. I also used a number of Firefox web browser ‘Add-ons’ which allowed me to export and analyse search results.

Ultimately, it was important for me to select sources which had clear narrative structure and which it would be possible to analyse using a structured methodology. I was able to identify the following ten sources (Table. 2), largely originating in the US during 2012-2014 (with the exception of one from 2007);



Link	Author	Type	Origin
http://hackforchange.org/blog/	Various	Blog	US
http://www.codeforamerica.org/blog/category/civic-hacking-2/	Various	Blog	US
http://www.theguardian.com/cities/2014/may/29/white-house-and-nasa-gear-up-for-national-day-of-civic-hacking	Guardian	News Article	UK
http://www.huffingtonpost.com/lily-liu/when-hacking-is-actually-_b_3697642.html	Huffington Post	News Article	US
https://www.opendemocracy.net/civic_hacking_a_new_agenda_for_e_democracy	Open Democracy	News Article	US
http://www.npr.org/2014/05/30/317361626/techies-white-house-take-part-in-national-day-of-civic-hacking	NPR	News Article	US
http://open.nasa.gov/blog/2013/05/08/what-is-a-civic-hacker/	NASA	Blog	US
https://www.ted.com/talks/catherine_bracy_why_good_hackers_make_good_citizens/transcript?language=en#t-97180	TedX	Video	US
https://www.youtube.com/watch?v=kDFhzNfd-bg	TedX	Video	US
https://www.youtube.com/watch?v=n4EhJ898r-k	TedX	Video	US

Table 2 Online Narrative Sources

The ten websites which I used in this research were not a 'top ten' list but were instead selected following careful but more qualitative (and therefore subjective) consideration of their content and structure. I was also keen to select a broad range of different source types, media and originations in order to examine a cross-section of Civic Hacker narratives. Thus, sampling was purposeful not random *"…since the principle analytical goal in this part of the project was not to generalise to the population but to interpret the meaning…of stories…"* (Ewick and Silbey, 2003).

I also mapped these themes against the Hacker Ethics which I had identified in previous literature within Chapter 2 (see Appendix A);

- Collaboration
- Fun of hacking
- Community
- Practical Involvement
- Inclusivity

As Alleyne notes, thematic analysis is usually most effective if the researcher starts with a clear set of research questions but is also open to themes emerging from the narratives themselves and it is rare to begin without "some kind of prior theoretical or conceptual framework" (Alleyne, 2015, pp.70-81).

I ordered the number of mentions of each theme within a source as it provided an indication as to how important each theme may be to each source. I also utilised the concept of a thematic network (Attride-Stirling, 2001; Fereday & Muir-Cochrane, 2006) which could be mapped against the various narrative themes expressed by Civic Hackers which I identified in my research.

Attride-Stirling structures these narrative networks in terms of the following themes;

1. Global Themes
2. Organising Themes
3. Basic Themes

In terms of my data, these relate to 1) the overarching narrative theme of Civic Hacking; 2) the subthemes which approximately relate to each of the Hacker Ethics and; 3) the more subtle and detailed, low-level themes which branch off from each sub-theme. These different themes were identified through use of specific words and phrases via textual analysis and through more subtle indications of themes through narrative structure and plot. For each data source, there were usually a number of different narrative types at play, sometimes interwoven with each other (Fig. 5).

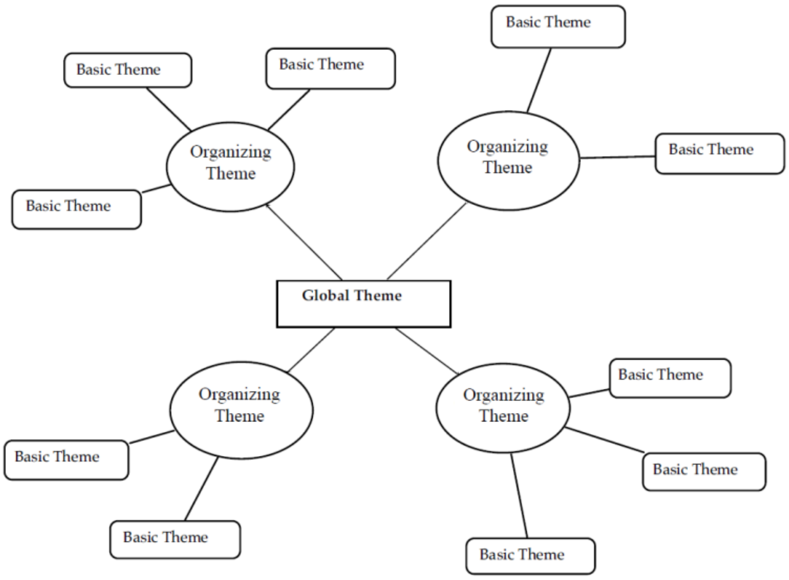


Figure 5 Hierarchy of Narrative Themes. Reprinted from Attride-Stirling (2001) with permission.

Since the data sources I was working with were not of the same structure, format or origin, it was not possible to apply an exactly identical analytical method to each one. In other words, it was not possible to directly compare data (produced by actors such as journalists and hackers) which took the form of blogs, videos or websites, in an accurate or reliable manner. I therefore sought to apply the most appropriate method for each case and also to examine the wider context and background of the data source by identifying the author, when it was produced and for what purpose.

I began by doing careful textual analysis for each paragraph, noting the main points in terms of episodes and events, and what propositions were being made. I sketched out the overall structure of each story including turning points in the plot, characters and key events. This identified certain episodes which reappeared in predictable sequences and common patterns including overarching ‘master narratives’. I examined my field notes, comparing findings from events with online text such as blogs and tweets. Finally, I re-applied the thematic categories I had developed through this process to the various narratives and looked for where these closely paralleled the “model” narratives I had identified.

The ‘unit of analysis’ is an important consideration when sampling narratives (Riessman, 2008). Although these units must be relatively ‘bounded’ in some way, this can vary. Within this chapter, the unit can be defined as;

- Blogs which contained a number of postings. Each of these postings could contain one or a number of narratives. Often, there might also be a single, chronological narrative running through multiple postings, similar to a diary;
- Videos of presentations which, again, could contain more than one story within an overarching narrative;
- News articles which tended to contain one, primary narrative.

I needed to make a decision as to whether or not to ‘clean up’ the content of these narratives while collecting them, that is, not to record verbatim “messy” language, thus making it more straightforward to analysis and interpret text. This was particularly useful when transcribing spoken narratives from hackathons and interviews. On the other hand, when dealing with online text such as blogs and social media, I did reproduce text verbatim within my own field notes to provide evidence for my claims although these have not been included within this thesis. This was relatively straightforward to do with blogs as they did not require transcribing, however, it did produce large volumes of text. Note-taking during all interviews and events was inappropriate since it would have served to distance me from the other participants, although in online textual research this was much less of an issue due to the fact that text was already recorded.

This means that narratives were not necessarily told in a precise way with identical word choice and emphasis, however, my emphasis was not upon exact specific content but rather the themes involved. The issue is unavoidable in sensitive situations and my strategy (to reconstruct what I heard, creating summaries in field notes) is the typical solution. The use of online data, however, offered a control for this since it allowed me to triangulate these field notes against textual data which could be reproduced.

I chose not to include transcripts or field notes of narratives in their whole form within this thesis but instead chose to select the most relevant parts. I was aware, however, that this choice in itself creates the possibility of some degree of bias and subjectivity in the selection process and raises questions as to how the reader will judge the authenticity of my research. On the other hand, qualitative fieldwork is often predicated upon persuading the reader of the documentation of a particular set of events and readers are required, to a certain extent, to trust the author's interpretation and representation (Taussig, 2011).

Validity and reliability can apply to both the research findings and the measurements used. In Narrative Analysis, the instruments and measurements used tend to be less defined than in quantitative methods. Therefore, it is important for the narrative researcher to offer reasons why the reader should believe that their work is reliable and accurate. Webster and Mertova (2007), argue that reliability can be improved by factors such as access to research data, honesty, authenticity, familiarity and so on.

For each data source, where possible, I situated it within a wider context, which varied from the local context of the narrator or a global social context. By doing so, I explored this to the extent that it revealed patterns about the narratives. It was not always possible to produce a biography or 'life story' of the narrator in an online setting due to anonymity of many online authors but I was often able to glean context about the particular blog or organisation involved.

Although I generalised these narratives across my units of analysis (narratives), my primary purpose was not to generalise across the population of Civic Hackers but rather to 'unpack' the metaphors involved in these narratives and interpret meaning. By doing so, regularities among the narratives became clear. I also looked to identify any similarities between written, pre-existing narratives from online settings and the spoken narratives of the events I studied and my interviews with respondents.

Once I had selected a sample of websites, I then identified the various narrative themes within them. I identified ten main narratives as featuring across these particular sites and also from previous data gathering;

1. Bad vs Good Hacking
2. Challenges/problems/solutions
3. Practical action/pragmatism/contribution

4. North American ideals
5. Democracy
6. Local vs Global
7. Not just about technology/Inclusion
8. History of science and technology
9. Support from government and official sponsors
10. Community/togetherness/common/collaboration/sharing

These narrative themes were drawn from a combination of two places;

- By taking the previously identified narrative themes from my hackathon fieldwork and study of a Twitter network. I then mapped these existing narratives against the selected websites by analysing the text for these same themes;
- I also identified any potential new, or subtly different, narratives taking place within these Civic Hacking websites.

These themes were developed inductively from my fieldwork observations. The narratives discussed in Chapter 7 were the outcome of this.

3.5 Mixed-Method and Multi-Site Research

It was vital that the various methods and research sites described above linked into a whole from which I could establish findings which allowed me to answer my overall research questions. Not only did I make use of several different methods but also different research sites for each. In addition, my chosen research sites moved between micro level focus on individuals, groups and events and macro level data from online narratives which bridged several wide-ranging groups and time periods. The rationale for taking this approach was both that it allowed me to triangulate my findings across multiple sites and through various different methods but was also useful when approaching a research group who were highly mobile and often difficult to define. Each of these sites and methods was also appropriate for answering different research questions. The linkage between these different methods and sites came from both the theoretical framework described in Chapter 2 and the research questions which I aimed to address. While a variety of different methods was applied across my research project, they had these research questions in common. These in turn were developed based upon a common conceptual framework. Similarly, the field sites I selected for my research may have varied but were connected by the overarching theory which underpinned this project. The rationale for selecting these data samples was also guided by these research aims. Therefore, my aim of developing a theory of the Hacker Ethics and their relationship to network societies is interwoven between individual portraits of hackers gained through interviews and observations, fieldwork at a Civic Hacking event, social network analysis of a Civic Hacker Twitter hashtag and analysis of multiple online narratives.

3.6 Limitations and Ethical Considerations

The internet is an unusual subject matter in that it is both cultural artefact, a text, and a field site. There are a number of general considerations when carrying out virtual fieldwork regarding the limitations and ethics of online research. For example, the difficulty of validating sources and assessing the authenticity of informants can be more complex than in the real world since you can't always be sure who online subjects are without 'real world' contact. The authority of the research in traditional fieldwork is often based on visiting a physical location and meeting informants (Hine, 2000, p.43). On the other hand, if we accept that the role of the researcher is to reflexively *interpret* a particular culture then such dilemmas become less relevant.

Both Miller and Slater (2000) and Markham (1998) also note, however, that internet based communities and everyday life beyond the internet are highly intertwined and therefore suggest that a degree of offline interaction with the people one is studying is essential. There is indeed a difficulty in assessing people's responses to questions without face to face contact and the level of immersion required to constitute fieldwork would arguably benefit from real world engagement. In the case of the groups I was proposing to research, there was a certain degree of real-world interaction which would require me to go beyond merely conducting online research.

Virtual fieldwork also raises a number of ethical issues which are less problematic in a traditional study. For example, questions arise as to whether these online forums are 'public spaces' in which individuals' views can be captured and used without permission. It is also possible to carry out a certain amount of covert observation on chat rooms ('*lurking*'), which would be more difficult in a real-world situation (Boellstorff, 2008). There is a responsibility on the part of the researcher when working in online settings to be open and honest with their research subjects about whom they are and what their intentions are (Buchanan, 2000). It is easier for the researcher to be dishonest about themselves online due to the potentially covert nature and "invisibility" (Murthy, 2013, p.848) of digital research.

During my research, I applied a number of ethical standards which were particularly important in an online setting. There is an inherent ambiguity when dealing with online data as to what is 'public' and what is private. For example, the majority of those using the #hack4good Twitter feed would be unaware that research was being conducted, however, it was not possible to contact all these individuals to gain consent. Within my own research, I informed any of these subjects in cases where I intended to make more in depth use of their postings. This gave them the opportunity to decline and I was clear in my explanation of my aims and how data would be used. I did not make use of any 'closed' forums within my online research so all data was publicly accessible. In the case of blogs, websites and hosted videos, I considered these to be in the public domain in the same way as news articles or publications and therefore it was not necessary to gain the specific consent of their authors.

I also applied more generic social research standards including avoiding undue intrusion of subjects, obtaining informed consent, anonymising data where possible and ensuring data security (Economic and Social Research Council, 2015).

During the early stages of my research design, I made an assumption that these 'hackers' were legitimate and therefore not involved in criminality (e.g. *phreaking* and *cracking*) so would be willing to speak to me freely. However, it became apparent to me that some individuals, particularly those in developing countries, may have been involved in both illegal activities through hacking ('*jail-breaking*') mobile phones and, in the case of 'political activists', potentially subversive activity in their own countries. This highlighted the necessity to abide by ethical ESRC Research Ethics Frameworks and consider any potential harm to participants or criminal activity involved. I have also conformed to the Goldsmiths Code of Practice on Research Ethics and Research Data Policy. As part of my research process, I had to undergo an 'upgrade viva' in which my initial data analysis was subject to peer review by academics within Goldsmiths, which also included a discussion of any ethical issues. All informants were advised that they would remain anonymous unless they consented otherwise and data I collected has been stored within an encrypted format and in line with the UK Data Protection Act (1998). The relevant consent form is included at the end of this thesis.

Based on my own pilot samples I identified a number of unique challenges which needed to be addressed within my own research project. Firstly, a high proportion of my informants were themselves highly educated individuals, often IT graduates from 'Ivy League' universities. A number of them were also carrying out their own research into the topic of ICT4D. The power dynamics of researching 'up' (Wiles et al, 2004; Altorki, 2014) for a junior researcher present some interesting issues. When researching such a self-aware group of academics it is important to acknowledge that they are likely to know 'tricks of the trade', are often quite senior and must be 'treated with respect', (Wiles et al, 2004).

I found during my interviews that many of the respondents questioned my use of certain terminology but also that they provided answers which were academic in nature, for example, quoting research literature. While it was important to let respondents provide the answers that they felt were important, I was also keen to direct interviews towards their own (personal) opinions and feelings. I was often able to use this knowledge of academic debates to my advantage, purposefully using controversial and divisive terms such as the Digital Divide in my questions as I found they elicited a strong response (Garfinkle, 1996).

In practical terms, some of the hackers whom I contacted had limited English so I was required to either simplify interview questions or contact them via another informant. In fact, in general, I needed to tailor my approach to suit the respondent in terms of style and questioning. With some of the later interview emails, I changed the questions slightly based on initial responses and also to suit the different career or educational background of the respondent. Interestingly, I have found that the most comprehensive responses have come from less formal email approaches, possibly due to the relatively relaxed working relationships of many in this hacking for social good group, and their comfort in using technology to communicate.

Since the focus of my research project was qualitative in nature, I was less concerned with sample size than gaining an intimate understanding of the practice of Civic Hacking through fieldwork. Clearly, however, sample size can be a limiting factor. The ability to gather a wider selection and depth of data would have increased my ability to form interpretations relevant to my research questions. Also, as my time spent gathering data within this group was limited due to practical considerations, extending this time would have increased the validity of my claims. For example, my time spent participating in hackathons and other events was quite limited and increasing the time spent at this event and the variety of different events I attended, would have resulted in a greater understanding of this group. In terms of Social Network Analysis, I was also constrained by my practical ability to gather large amounts of data and to analyse them. However, this was less important as I intended to analyse this smaller sample in depth. Breadth, rather than volume of data, was perhaps a more limiting factor. Since I only looked at this specific group of Civic Hackers, it was more difficult to generalise about hacking practices more widely.

In this chapter, I have described the methodologies which I employed in this research project to address my research aims. In the next four chapters (4-7), I shall present the data which I gathered during my research and my analysis of them.

Chapter 4

Towards a Typology of Hacking for Good

4.1 Introduction

A research thesis often begins with an introductory narrative description of the entry into the field site, describing the researcher's arrival at a location and what they encountered including visual observations. The intention of this is to ascribe to the researcher a level of authority based upon first-hand experience of a physical location and offering a degree of reflexivity (see Chapter 3). With research into mobile subjects, however, and particularly one which is highly dependent upon digital sources, this narrative vehicle becomes slightly problematic because of the temporal and geographical nature of the spaces in which it is reliant (Section 3.1.1). Mobile or digital research, for example, will often move from place to place following actors. It can be situated both online and in a 'real' place, and focus on events which occur both simultaneously and in the past. Although this kind of digital 'entry' narrative can be produced successfully by some researchers where data gathering was focused in one online 'place', such as a confined internet forum, the mobile nature of my own research subjects means that I did not deem this approach to be appropriate. Instead, I will provide an overview of hacking for good as my research sphere and briefly describe my initial contact with and entry into this 'field of practice'. Thus, I will provide an understanding of how I first identified the field I intended to research and gained access to those involved in this activity.

4.1.1 Research Aims

The following analysis is based on an initial sample of data which I gathered during 2011-12 using the methods, primarily interviews and participant observation, as discussed in Chapter 3. The aim of the analysis was to identify themes and questions, supported by those raised in the theoretical context, Chapter 2, which would be explored and expanded upon in subsequent research (Chapters 5-7). The initial research sample also allowed me to define the subject groups upon which I intended to focus. This allowed me to address my research question 'what are the different types of groups involved in hacking for social good and how are they situated within the wider history of hacking as a culture and practice?'.

This initial sample of research subjects comprised seven individuals in addition to hacking groups, events and online resources involved in hacking for social good (as described in Section 2.3.3). Data was gathered over the period of one year using methods described in Chapter 3. Since there was no clear definition for those involved in this activity, it raised some issues around defining the boundaries and membership of this 'field site' which I had to address when carrying out my research. The globalised and mobile nature of these groups and individuals also meant that they had to be studied in quite a fluid manner, rather than focusing upon a specific location or group in a static sense (as described in Chapter 3).

These three portraits are followed by a discussion of the key themes which emerged from them and which presented scope for further analysis. These themes built upon the research topics and questions for my thesis.

4.2 Research Findings

4.2.1 Portrait One: 'Ethical Hacking' and Civic Hacking

Pete is sitting in the lobby of a prestigious central London club, surrounded by silverware and chandeliers, men in pinstripe suits, the tinkle of teapots on the trays of the waiting staff. To say he looks out of place would be an understatement. He flicks back his silver ponytail, a baggy shirt and pair of crumpled trousers his nod to formality, making a change from the t-shirt, jeans and sandals he was wearing when we first met. He inhales on a black e-cigarette and interlaces his fingers, playing up the techno-Gandalf role with the fluidity of years of practice.

"...a wealthy socialist is a worried person I assure you," he says with a smile. We are talking about Pete's 'history of hacking'. I want to know how he became involved in hacking in the first place. Like most of the hackers I have spoken with, Pete doesn't view hacking as a career as much as a lifestyle. He first got into electronics and engineering in the 1970s, a love of "playing with stuff" which he continues today although now he has less time.

> *"I was playing with broken radios when I was eight years old…not necessarily doing anything with them except enjoying the fact they looked exciting….the first kind of hacking I did was phone hacking when I was a teenager…all that meant really was discovering that pressing the receiver was the same as dialling a number…randomly phoning numbers and seeing what happened…"*

Pete has always been interested in how technologies work, particularly in what is "going on down the wires" which he believes is the key to understanding how technology works. He points at the sockets on the wall beside us and tells me that he is less interested in the gadgets at either end of those plugs, "black boxes" he calls them, than the data travelling in between.

> *"I'm thinking about where it goes…where it leads to…"*

This might explain why he is less interested in the hacker debates about, for example, whether open-source software is morally superior to proprietary. It is the hardware in between that he cares about and it was this fascination with data which led him to experiment with 'packet sniffing' in 1976. This in turn led to his employment by a number of companies as a 'penetration tester' ('pen tester') in a field which would later become known as 'ethical hacking'.

During his 20s, Pete was focused on running an IT company but as he began to earn more money, he was able to charge differing amounts, depending on his ethical view of the company involved he tells me with some enthusiasm, and even to carry out some work free of charge. It gives him an opportunity to "put back into society…hopefully helping stop the bad guys". It is this kind of ethic, a belief that technology should be used for social good, which I would argue that Pete has in common with some Civic Hackers. It is a desire to use hacking for social good which has been a part of the Hacker Ethic since the early stages of computing development at MIT (Section 2.1.2).

He describes himself as having a "quasi socialist mind-set", not more right-wing but certainly more pragmatic than he used to be. As a youth, however, Pete was quite militant, involved in the animal rights movement and struggling to deal with personal problems. He thinks that most "extreme passions" are the result of personal issues, in his case the suicide of his father. As he began to "untangle" those issues, he lost some of that passion or at least channelled it into different areas. On the other hand, the results of his father's death on his family left him with a strong belief in the social welfare system.

> *"….because I found myself, within a few weeks of being on the street…after my father died….but we ended up in a council house, I do believe in a level of support, society can provide, can afford to provide for people who find themselves in difficult circumstances…so from personal experience I think that's a good idea…"*

So how does Peter, the impoverished and rebellious youth, the 'hacker', wind up here in this centre of commerce, and having drinks with mainstream, high profile members of government? Well, for a start he is good with technology. He has a natural feel for technology, an intuition and a drive to understand how things work which seems to be so common among those involved in hacking. He also spent time working in IT behind the 'iron curtain' during the 1980s and saw what he describes as the failings of communism. This led him to a realisation that he could do more good, and earn more money, by working 'within the system' as a businessman.

Ultimately, Pete has a passion for technology and can talk endlessly about his personal 'history of hacking'. He describes helping to build his friends Astron 1 computer kit in the late 1970s which he finished quickly because he had worked so much with electronics. He talks about the Commodore PET computer which was built with only one port at the back and designed for scientific calculations by HP. This IEEE Port, a data transfer connection, was not really known about or used by most people outside labs and appeared in the same market place as the original Apple and Osborne computers. Pete was involved with a group of techies in Hove, East Sussex, who built a hard drive called a Winchester which could be connected to this port. Pete can still remember every detail about memory size and specifications, and how they grew in size to what we know today. He talks about the ability to bolt on extra hard drives and his attempt to connect two monitors to the port just to see what would happen. When this failed he,

> *"...got down into the 64 bit machine code and looked at the way it interfaced. I needed to assert myself and then see if it collided with the person who was already there, he would then stop, withdraw and try again in a random amount of time, this became a technique known as CSNA/CD which is the basis of Ethernet....I wrote this off the top of my head to allow a chum of mine to run his two small businesses.....no one else used it and it didn't occur to publish or market it....I just did it to fix a problem".*

Pete believes that the average person is only interested in the 'top layer' of a technology;

> *"...what I'm thinking about is the hardware and the drivers, then you'll create a system, maybe applications, I think that's a useful skill set to have, particularly when you're doing penetration testing...or if you're going to make use of technology in an unusual way...I also like to do that in the studio..."*

He also sees a lot of parallels between hacking technology and other non-technological interests such as urban exploration and music. Again, this aspect of the Hacker Ethics seems quite common among most of the hackers I have spoken with and I identified it as a trend within Section 2.1.2.

> *"There's a group called 'Circuit Benders'... they take old studio equipment and make it do more extreme things...weirder noises and stuff..."*

Pete has been involved in non-technical forms of hacking since 1967, the same year that he bought a box of guitar pickups and attached them to a violin from a jumble sale, with an old Wah-Wah peddle and an amp. Around the same time, he also built his own record player, from parts, designed and built the case, *"stole an amplifier from here, a speaker from there...because we didn't have any money..."* It seems as though a lot of Pete's early experiences with hacking came about as a result of pragmatism, a result of his lack of money and desire to access technology.

> *"One of the first....the second computer I ever touched, aged 17, was a Vidac 330 which was made by a company called Computing Techniques Ltd...I don't think it had a massive market...I used it as a synthesiser..."*

I ask Pete what he thinks about hacktivists, and people who use technology for political or activist goals,

> *"...that's what I would criticise Anonymous and Lulzsec for...they don't care about the fall outs for the individual...they're so focused on a) making a name for themselves and b) annoying their targets..."*

Pete does not believe that technology is a human right in the same way as water or education. In fact, he dismisses the idea of human rights generally, describing the concept as "man-made". But he does think that those with technocratic power have a responsibility to the rest of society. Unlike some of the ICT4D activists I have spoken with, Pete hasn't thought a great deal consciously about the use of technology for social good but he does not believe you can or should force companies to give away free internet "in the same way as libraries". This, he says, is his problem with the reality of communism and part of what first turned him away from it in the 1970s.

He sees himself as more of a pragmatist. And it is here that he reveals himself as having something in common with the ICT4D 'hackers', discussed next, who emerged during the early 1990s. Rather than focusing on ideological principles and philosophical discussions, Pete tries to focus instead on the practicalities and use whatever technologies are most appropriate. From running a business, he has learned to look at what competitors are using and make that his drive rather than worry about whether "Bill Gates is evil". Pete learned to hack Windows not because he has a problem with it or because he likes to use it, but simply because that is what companies, and therefore hackers, are using. This motivation may be that of earning more money, but it is certainly not ideological.

Discussion of Ethical Hacking

One of the reasons I chose to include Pete in this study was to provide some context in which to situate those involved in hacking for good, both historically and ideologically. On the other hand, I am not suggesting that Pete should be viewed as some sort of philosophical forerunner of Civic Hackers since this is too simplistic a view. On his own admission, he has nothing in common with any wider hacking community and had not previously heard of projects such as Random Hacks of Kindness. However, his use of hacking for social good, whether intentionally or simply as a result of pragmatism, is indicative of individuals and groups who, I would argue, have something in common with Civic Hackers. Pete was consciously involved in the use of hacking for social good. So he provides some indication of the sort of ethics within 'hacking' as a broader practice which have more recently become important features of Civic Hacking.

4.2.2 Portrait Two: ICT4D Activists

During the early years of the 1990s, there was a significant increase in the proliferation of Information Communication Technology (ICT) across certain parts of the globe, linked closely to the development of the internet and World Wide Web. This, in turn, generated a large amount of debate among development professionals as to the implications of ICT for addressing various humanitarian problems, often referred to as ICT4D (Section 2.3.2).

Based upon my observations, Steve is relatively typical of a professional working in international development, and he was present in the early days of what would become known as ICT4D. In 1990, he was working in London when a university friend who worked for Oxfam suggested that he go to South Africa and set up an IT consultancy. South Africa was experiencing the final stages of apartheid and Steve became involved in what he calls the "mass democratic movement". This involvement was largely as a result of boredom with his job but he soon became immersed in a world of non-profit organisations. Ever since, he has acted as a bridge between the non-profit and business worlds, raising funding for various ICT4D projects.

Steve's views do not appear typical of someone one might term a 'hacker', based on my literature review and other interviews. He argues that funding tends to go where it has been given previously, in other words to reliable and tested ideas. Because there is a constant funding stream and little competition it does not drive innovation to the same extent. As he puts it, people do not *have* to buy these products so there is less need for the producers to be useful. Instead, he suggests that "social enterprise", a competitive business approach to development innovation, is one potential solution. This is essentially a blending of non-profit and commercial organisations.

On the other hand, Steve tells me that he has always enjoyed 'hacking' in terms of taking technology apart, modifying and tinkering. But he doesn't see hacking as a solution to development issues. He believes technological innovation really occurs when the cost reaches zero, as people have less to lose from experimentation. He points towards companies like Facebook and Twitter which emerged from the US where access to technology is cheap. But in Africa, where a single mobile phone might be shared among a dozen people and the daily salary is relatively low, Steve thinks there is more to lose from experimentation. This is interesting as it seems to go against the idea that the need for cheap technology in low income communities may be a driver of hacker innovation discussed in the second part of my literature review.

My interviews suggest that there is an interest in some less economically developed regions in the use of open-source and hardware hacking, as a way of overcoming restrictions in terms of lack of money or limited wireless network.

This has led to people with no formal training exploring ingenious ‘hacks’ to build wireless routers from cans, computers from old TVs or adapting phones to hold several SIM cards. There is a strong link between this kind of ‘grass roots’ pragmatic hacking and the ICT4D movement since most of those I have interviewed are involved in and have a strong interest in both areas, however, I do not believe that they can be described as belonging to the same professional ‘field’ since their motives differ. Individuals such as Steve, who are involved in ICT4D, view this kind of hacking as a side-project, a hobby or topic of interest rather than a method of professional practice. It is still removed from their core work which tends to revolve around more structured projects which, although often open-source, seem to have much less of a Hacker Ethic. Based on my sample, those involved in ICT4D often seem to hold post-graduate level qualifications from the US or Europe and have backgrounds in corporate IT so would probably not be described as ‘hackers’ in the terms defined within my literature review. Those involved in Civic Hacking I describe later have more in common with this ‘grass roots’ level hacking although it also has its origins in ICT4D and it is difficult to separate the two. On the other hand, it might be that the demographic of my research is subject to bias due to language limitations or the nature of my ‘gatekeepers’.

Although not involved in it himself, Steve has seen this kind of ‘grassroots’ level hacking and does accept that there is a growing culture of mobile phone innovation in Africa. This involves the development of applications, SMS based services and crowd sourcing such as the Text Eagle project which divides translation out among a number of people. He thinks that there is a lot of funding in the area because it is in the interest of phone companies to encourage such projects since it drives more traffic to their network. This is not the case with other types of less commercially viable 'hacking' such as certain open source software.

In terms of 'home grown talent', Steve describes parts of Africa as "hives of innovation", particularly Kenya which he calls the "hottest place in Africa at the moment" for ICT entrepreneurial spirit. He thinks that this is due to the fact that the costs of accessing IT have reduced more there than any other place in Africa.

Like others I have spoken with, Steve is uncomfortable with the term 'ICT4D', although many of my participants do seem to use and associate with it, some suggested just because there is not an alternative commonly agreed phrase. Steve also finds the idea of development generally too "paternalistic". Steve argues that technology is a driver of social change everywhere not just the 'developing world'. In fact, he explains that some systems such as *MPESO* (a mobile money payment platform) are more sophisticated than anything in the US or UK and might actually influence these countries to adopt similar technologies.

Steve says that he doesn't see a lot of hardware hacking in Africa. Instead, he thinks that this kind of modification tends to be from places like China where technologies are commercially developed such as cell phones that hold two SIM cards. But he says there is a lot of software hacking in Africa. Projects that develop open source software for interrogating data such as medical records and crime statistics galvanise strong communities of African software developers around them. Steve thinks that the best projects tend to combine expertise from

Africa and outside. He sees open-source as a good alternative to off-the-shelf software but believes that when people in Africa see commercial products being used in the rest of the world they tend to want them too.

My interviews suggested that a level of pragmatism was quite common among this group. Few of them cited ideological or political motives for using open source software or modification of technology. Instead, they tended to seek out the most appropriate technologies for a particular project. Most of those asked did not associate themselves strongly with any kind of political activism.

The majority of those I spoke with did not overtly engage with the kind of Hacker Ethic as described in Section 2.1.2. This raises questions regarding to what extend this group might be described as hackers. The next type (Civic Hackers) I discuss could well be described as having had a more overtly hacker culture in terms of both the lifestyle of certain members and their relationship with technology. However, individuals such as Steve, who emerged from the early 1990s ICT4D scene, did form a group who emphasised aspects of a Hacker Ethic such as collaboration, the use of technology for social justice and technological exploration.

As a type, the subjects I have described in this section comprised a relatively loose and heterogeneous collection of individuals from varying backgrounds who at first glance may not have appeared to have much in common other than that they worked in a similar area and became involved in this activity around the same period in time. This raised questions as to the extent to which they shared enough in common to comprise a single group. On the other hand, when asked to provide me with other subjects for my research into hacking for good, almost all these respondents referred back to each other, suggesting that there was a network of some kind, however unbounded that may have been. The nature of this network, and what connected those involved, is discussed later in this chapter and provided a research topic for subsequent research (Chapters 5-7).

Like Steve, Ken's development career started in the early 1990s, however, he has been involved in IT since the 1980s when he first learned to programme a Commodore PEC computer at a local club. At this stage it was still just a hobby. Ken describes growing up on Jersey in the Channel Islands, close to a world-famous zoo where his parents were both keen amateur naturalists. He credits this upbringing with an interest in environmentalism. But he tells me that Jersey is a small place with relatively few challenges so when Live Aid was developed in the mid-1980s, Ken realised that there was "a lot more going on in the world", as he puts it.

In 1993, he volunteered to go to Zambia to help build a school and began to realise that so much development work "wasn't working". According to Ken, there was not much you could do with IT and development around this time, although he doesn't know when ICT4D actually became a distinct area. The internet and email were not yet prolific, certainly in the developing world, and mobile communication still further away. Ken visited Uganda in 1995 before deciding to study development at university.

Ken later went on to found an organisation called Frontline SMS which provides free open-source software to 'crowd source' data without the need for an internet connection. This kind of technological workaround, I would argue, has elements of hacking in that it involves an ethic of exploration, collaboration, democracy and informational freedom.

When I ask Ken whether he is a 'hacker', however, it becomes apparent that this is not as straightforward a label for him to define. Although he knows people who might be called hackers, he does not relate to this term himself. In this way there are similarities to some of my other interviews. A number of respondents felt that, although they might be considered part of a hacker community or at least a community with some hacker 'characteristics' in common, they did not themselves possess the level of technical skill required to attribute themselves this term. This technical skill seemed often to involve a level of coding experience necessary to perform workarounds and modifications on technology. Interestingly, however, my interviews indicated that 'hacker' was not a term that many would assign to themselves, seemingly because it was seen as 'self-aggrandising'.

It might be more useful to consider those such as Ken as working on the periphery of this technical 'elite', although they may conform to certain aspects of hacking, they tend to act as supporters and facilitators of those who hack in a technical sense. An aim of my research increasingly became to make a greater level of contact with the technical experts behind these humanitarian projects, whether they would term themselves 'hackers' or not.

Interestingly, a strong trend within my participants was the fact that they spoke in terms of 'hacking', as a verb, rather than 'hacker' an adjective, a term endowed upon an individual. Groups and projects were also termed 'hacks' or described as having elements of 'a hack' more than the individuals working within them, suggesting something of a collaborative ethos.

Like most of my contacts, Ken is a keen 'Tweeter' and uses a blog as a forum to share and pass on new ideas. He recently offered some advice to those interested in the use of ICT for development which is indicative of a spirit of collaboration and community among ICT4D activists,

> *Collaborate if it's in the best interests of solving your problem, even if it's not in your best interests…make full use of your networks, and remember that the benefits of being in them may not always be immediate (www.kiwanja.net/blog, Oct 18 2011)*

So, while Ken might not be termed as involved in hacking as previously defined, I would argue that there was a Hacker Ethic (see Section 2.1.2) within his projects and the groups he was involved with due to their collaborative and open source nature. If we view a technological product like FrontlineSMS as a cultural artefact, it can be interpreted as the product of a community which possesses this Hacker Ethic since its very code is open to modification, makes use of a collaborative interface and is designed to be easily accessed by the general population.

Others, however, fitted less into a hacker typology. Unlike Steve and Ken, Bill is a computer scientist and works for a multinational IT corporation based in India, primarily focused on the academic research side of ICT4D rather than 'practical' development work. Computers are his focus and he told me it is often too difficult to start with the end-users due to language barriers and lack of education so his company tends to work with community centres and local organisations. This differs somewhat from the collaborative approach of other practitioners involved in ICT4D.

Bill is more sceptical of open-source than others, not surprisingly given the fact that he works for a proprietary software company. And his view of development can be seen as reflective of this approach, less collaborative, less distributed and less inclined to promote hacking as an 'ethic'.

Bill tells me that most technologies are used by the richer minority parts of Indian society rather than the majority population. He feels that there is too much hype among ICT4D practitioners and that non-technologists don't always understand the limits of IT.

In terms of 'hacking' in ICT4D, Bill tells me that development organisations often have so few 'hacker' skills that they need to opt for off-the-shelf software. He thinks that in some ways open source is more elitist in terms of education since the level of education you need excludes most people. He also points out that in India few people pay for legitimate software such as Microsoft anyway, choosing instead 'pirated' copies, so there is less demand for free, open-source platforms than in places such as the UK.

He has seen hardware hacking of computers and phones but it tends to be related more to maintenance than modification. For Bill, ICT inequality has less to do with access to particular technology as it does with education and the relevance of a particular technology. As he explains it, part of the reason television is relatively widespread in Indian society is that people find it “useful”. They want to be able to watch cricket or their favourite TV show. Neither is the popularity of a technology about access to global information systems but locally created ones. Part of his interest is in how one enables local creation and uploading of information. Often, international resources like Wikipedia are not relevant in other places since they can be quite culturally specific or in the wrong language. Instead of bridging the divide Bill talks about creating the same system in another place, almost setting it up ‘fresh’ in that particular country.

Jon works for the same corporation as Bill but is based in Southern Africa rather than India. Like Bill, he sees himself as an academic, a sociologist, with a PhD from Stanford in communication technologies. After graduating, he worked for the private sector in economic development and was somewhat inspire by the ICT4D work being pioneered at Stanford. However, at this point it was not really referred to as ICT4D and he says that it wasn’t until around 2000 when the internet really began to “take off” that ICT4D emerged. Jon started to see the growth in mobile communication across the countries he travelled to and this also played a role in developing his interest in ICT4D.

He has worked in ICT4D for around seven years and has seen a number of what he would call hardware hacks of phones with everything from putting a skin on it to “getting into the guts of the phone”, loading software, jail breaking and installing second SIM card inputs. He is interested in these different levels of appropriation and in phenomenon such as ‘beeping’ but does not really deal with hardware or even hacking as a concept. Jon is an academic and less involved in the practical side of things. I ask him whether his company adopts these lead user innovations and hacks but he thinks they probably have more impact on smaller companies.

Jon is not a hacker, or a coder, and does not identify with that term. He feels that some of the people involved in ICT4D have a hacker instinct but then others have more traditional development approaches and a range of other backgrounds. He recognises a sub-community who love the hacker approach but does not associate with that himself.

Jon sees hacking in this context as not just about technology but also renegotiating the power of corporations and telecoms companies through intellectual property. He thinks that this is often where the Hacker Ethic can be found rather than hardware hacks. He sees a lot of it as about pragmatism rather than ‘hacking’. He is fairly unclear about what hacking means in this context and asks whether telecoms companies would see ICT4D as hacking their systems.

Discussion of ICT4D Activists

I believe that the above individuals I have interviewed make a reasonable case for the presence of a virtual community (see Chapter 2, Section 2.1.2) among this group of ICT4D workers. It is clear that the people in this community generally knew of each other, either through real world conferences, or by way of academic articles, blogs or online forum discussions. The individuals involved were scattered geographically, and came from a range of backgrounds and with differing motivations, yet they all referred to one another when asked by me to name others with an interest in hacking and development. This community formed around both a shared interest in technology and a desire to apply this technology to social development. It was also apparent from my interviews that a wider community of people involved in hacking for humanitarian causes existed, involving those I will describe in the next portrait.

However, most of these ICT4D participants featured above did not see themselves as hackers and would not have used that terminology to describe themselves. This is interesting when compared with my next group, Civic Hackers, since the latter tend to identify much more overtly with hacking as a method and lifestyle.

4.2.3 Portrait Three: Civic Hacking

The heavy November mist hangs outside the lecture theatre. Inside, the seats are full and people cling to the edges of the steps. This is part of an event, organised by two organisations Ushahidi and FrontlineSMS, facilitated by Goldsmiths College. A simultaneous meeting is going on in Nairobi, all largely coordinated online. The people present have a shared interest in the use of ICT in addressing problems - social, environmental and political. They are practitioners and those with an interest in global development such as academics and journalists.

The presenters start by providing a demonstration of their technology. Ushahidi is a free and open source software organisation which allows people to gather and analyse data from sources including email and SMS. Ushahidi can be linked to FrontlineSMS to allow data to be gathered more easily in challenging areas. The presentations show the wide range of uses for these platforms and a number of people from different backgrounds are present from journalists to environmental charities in the UK. I meet a number of the individuals whom I have encountered already in person and others are participating via social media as they cannot attend the event, highlighting the extent to which these groups form a community. Many of those I meet at this event know each other from other similar events both online and 'real world'.

The audience is shown some of the different uses for this technology including mapping of harassment incidents in Egypt, violence against children in Benin and to monitor station closures during a London underground industrial strike. One of the presenters uses Skype to present remotely from Haiti. It becomes apparent that a very large number and range of different groups and uses for this software is developing, again posing questions as to what, if anything, brings these people together into a community beyond this specific event.

During the event, a number of individuals and organisations make use of Twitter and other social media in real time to post comments, video and photos from various parts of the globe. Some of these included contacts I had interviewed previously. Tweets make use of the #smsmap '*hashtag*' which allowed me to easily gather and analyse this data. A '*hashtag*' is a phrase used in social media, originating in IRC, to group posts together - in Twitter using the 'hash' ("#") symbol.

The majority of tweets originate with the organisers themselves who provide updates on the discussions taking place. Many of these are then commented upon or '*re-tweeted*', reposted, by participants or those outside the physical event:

> *Where did @Ushahidi come from? It was built around the citizenship sharing community online – after post-election violence that occurred in Kenya. #smsmap*

Other tweets are more practical, relating to participants feelings regarding the event or making plans with others:

> *I'll be @FrontlineSMS & @ushahidi's #smsmap @Goldsmith's this eve, anyone else I know going?*

This conference is one of many similar events which seem to form a central role in the lives of those involved in Civic Hacking. The idea of '*commons*' or ‘*camps*’, events where like-minded people can meet to work on projects and solve problems have emerged from the hacker scene, as did ‘*hack spaces*’ where hackers would gather to work on and share projects. These events are a significantly under researched area (Section 3.1.2). One could again view events such as this one as an indication that a way of working specific to hackers has been adopted more widely in other areas of society (see Section 2.2.2).

It is apparent from the presentations that these organisations produce a number of very different tools, a great deal more than I had initially anticipated. These applications are easy to modify at different levels, both by coding and by a more user-friendly web based platform. The organisations are on hand to support but there is also a forum for users to support each other. Like many hackers, those involved in this event make use of Internet Relay Chat (IRC) which presented opportunities for online observation and gathering of digital data which I developed on in subsequent chapters.

One of the debates which emerges from this event among those present is the question of whether technologies such as Ushahidi really ‘empower’ people. Do they represent a democratisation of information, or do they still remain limited in terms of language, access and education? This idea of democratisation of information is a common topic among this group and references are made to the ‘Arab Spring’ and how crowd sourcing tools were used to share and manage information outside of government regulation. This could also be viewed as a proliferation of a Hacker Ethic regarding freedom of information, use of technology for the benefit of society and liberalism into wider society beyond that of just computers (see Section 2.2.2).

In fact, this raises issues among the attendees regarding whether such events would take place without these technologies or if they simply made them easier, a slightly technologically determinist argument but a popular topic nonetheless.

On the other hand, some I have spoken with have also argued that rather than representing a democratisation of information, such technologies in fact widen, or at least highlight, inequalities in societies since certain groups have less ability to access them than others, for various reasons. Some discussion takes place, for example, at this event as to whether these technologies are still dependent upon governments and corporations which have a certain amount of control over how people access them.

Several of the presenters also discuss the theme of 'appropriate technology' and argue that the right technology might in fact be dial-up internet or a notice-board, depending upon the situation. They claim that it is important to involve the user of a technology from the beginning and that localised practices of working are better than centralised. These discussions all make me think of themes which run through hacker discourse – the idea of collaboration, end user innovation, decentralisation, even the concept that hacking doesn't need to be technological.

It is worth noting that a separation between this group and the ICT4D hackers discussed above was not always clear. There were a number of overlaps between them in terms of participating in similar events, collaborating together and their working practices. There was, however, certain elements to these Civic Hackers which distinguished them from ICT4D professionals. They tended to be younger, having started this kind of work within the last ten years or so, and not having been a part of that early 1990s ICT4D movement or earlier development work. Often, their starting point was quite practical, beginning with an interest in technology before moving into humanitarianism. They were what has been termed ‘digital natives’ (Prensky, 2012), having grown up with technology and seeing its use in all aspects of life as obvious. They typically made use of ‘web 2.0’ technologies such as social media, wireless networks and mobile technologies to a greater extent than ethical hackers or ICT4D workers. This was intrinsically related to a greater emphasis among Civic Hackers on democratisation and collaboration in solving problems. In some ways, it might be argued that this approach has also shaped technologies with a particular slant towards these attributes, for example, use of ‘crowd sourcing’ platforms.

One of the organisers of this event is Heather. I first encountered Heather through an organisation/social movement known as Random Hacks of Kindness (RHoK) before she moved to work for Ushahidi as a ‘Director of Community’, again another example of the links within this community. Random Hacks of Kindness arranges global hackathons in which hackers in different cities meet up to hack together, using open source code to solve social problems. Past projects have involved modification of mobile phones to make them more accessible to those with sight impairment, a phone application to allow cheap monitoring of water bacteria, and a platform for cheap mobile advertising for charities.

Although not a 'techie' herself, Heather is a key member of this community and well known to many due to her ability to organise and bring hackers together around social causes:

> *@Heatherleson speaks about the importance of different open tools working and hacking together #smsmap*

Heather is interested in the idea that hacking is not just about technology and sees herself as a "social hacker", collaborating and exploring to create new relationships. In her blog, she describes how this concept of hacking for pragmatism predates computer networks:

> *"My Grandfather never bought a new tractor. He taught himself how to fix one and saved money....on the same premise, my father who has invented gadget and kludges with whatever was laying around the yard or found in a discount bin...." (http://textontechs.com, August 16 2011)*

RHoK is interesting in that, although a series of open source hacking events, it is sponsored by corporate IT companies including Microsoft, Google and Yahoo. This is fairly typical, however, of a growing trend among 'mainstream' business and government to adopt aspects of hacking approaches and even imagery whether to make themselves appear more legitimate or because the Hacker Ethic is influencing mainstream business models (see Chapter 2). Most of those I spoke with did not see this corporate sponsorship as a negative thing, taking a much more pragmatic view.

Heather also put me in touch with Willow, who goes by the nickname Bl00. She organises a group called Geeks Without Bounds (GWOB) in the Pacific north west USA which aims to link hacker groups with existing humanitarian organisations so that they can assist in developing and modifying ICT. In an email, she explains:

> *I got involved with hacker and maker spaces, where building of the future actually happens - that's been for about 3 years now.*

Willow is more involved in the techie side of hacking than Heather but still does not consider herself a 'hands on techie'. Instead, she acts as a go between and spokesperson for hackers, attending conferences and hackathons:

> *I don't have a lot to do with actual coding or building, but I love the people who do, and they seem to like me pretty ok too.*

Willow often talks about the inherently social nature of hackers and dismisses the stereotype of them as loners. Like many of the others I have encountered, she is articulate and has built a vast network of contacts around herself, both in the real world and online. Willow also feels that in humanitarian crisis, it is often too late or too expensive to develop new commercial tools, and that companies are not interested as they cannot make a profit. This is therefore one of the reasons she feels that open source hacking of existing ICT can be more appropriate in such situations. Willow attends many of the 'typical' hacker gatherings such as DEFCON and the Chaos Computer Camp and uses them as a platform to discuss Civic Hacking on her blog. The idea that hacking should be put to a socially conscious goal is something she often talks about:

> *We are 'geeks' who care to use our skills to solve more than just #firstworldproblems....the culture of hacking in the United States has long been Hacking For The Sake Of Hacking. And we can do better than that....I am asking the hackers and security kids of the world to take a look at some of the applications and services associated with humanitarian efforts and explore how they might be improved.... a hacker is by the very definition a good citizen... (http://blog.bl00cyb.org, August 5 2011)*

She then explains how she started off her involvement by organising 'maker sessions' in which hackers meet up to build and tinker with things:

> *I like processing through things physically - actually getting my hands dirty, working with other people around an object, etc. But again, it was mostly a bunch of privileged kids making lights blink. Or balloons go really high. Or working with lasers. And that was also lovely, and necessary, but there are pretty drastic problems that need to be worked on in the world. So I became interested in education and humanitarian response.*

Like Heather, Willow embodies an idea of hacking which goes beyond the technical. She is involved in 'traceur', free running and urban exploration, and acknowledges the concept that hacking is not just about computers which I identified in the first chapter of my literature review:

> *....hackers are people who tinker with systems other people take as granted. They were the farmers who re-appropriated parts from their failing machinery to create things which actually worked for them.....Yes, they can be people who use a back door to teach an irresponsible company a lesson. And yes, they can be people using new open data to create ways of responding to disaster. Developers are people who build on systems which exist, new ways of interacting with those systems. While the line seems fuzzy at first, and is certainly contextual, it is an important one..... (http://blog.bl00cyb.org, July 15 2011)*

Willow also disagrees with the idea that hackers should be divided into 'good' and 'bad' and is quite opposed to the term 'hacktivism' which she says sets up a contrast between hacking generally, which implies criminal, and "hacking for good" which she thinks should be the same thing. Willow argues that a hacker spirit is a positive thing and should be encouraged in wider society:

> *....hackers are therefore the people who are taking responsibility for themselves and their environments, their communities...while systems are important for efficiency and sharing, those systems should constantly be tested, pushed, bettered. I don't think we're so much taking back the word "hacker" as making it into a thing everyone should strive to become... (http://blog.bl00cyb.org, July 15 2011)*

On the other hand, she does not think that a lot of the projects that she works on have a Hacker Ethic because the corporate sponsors are wary of the associated imagery.

These more recent Civic Hackers differ in many ways from those associated with the ICT4D movement of the early 1990s. Erik Hersman has an almost mythical status among this new type of Civic Hacker. He founded Ushahidi in Kenya and has a background in computer programming but is also incredibly sociable, with a large network and participation in conferences. Erik is conscious of a Hacker Ethic in his work and blogs about hacker innovation in Africa. In his blog, Erik rejects the term ICT4D, demonstrating this divide with the previous generation of Civic Hackers:

> *I have a cognitive dissonance over the term "ICT4D". The term "ICT4D" is confusing, hypocritical and has a whiff of condescension that makes me cringe....if the same things are done in poor communities in the US or Europe, it's not called ICT4D, it's called civil society or a disruptive product... (http://whiteafrican.com, November 2, 2011)*

4.3 Overall Discussion of Findings and Design of Subsequent Research

Four main research themes emerged from the research interviews described above which related to my research questions which I explored in project. These were:

1. Theme 1 centred around the different types involve in hacking for social good and defined the participant group (Civic Hackers) for my research;
2. Theme 2 was concerned with the ways in which technological artefacts produced by Civic Hackers are shaped by their ethics;
3. Theme 3 emerged from an interest among these groups in the democratisation of technologies;
4. Theme 4 focused upon the types of communities formed by Civic Hacker groups and explored what form these took.

4.3.1 Theme 1: Different Types of Hacking for Good?

This theme related to my research question 'what are the different types involved in hacking for social good and how are they situated within the wider history of hacking as a culture and practice?' My research participants and groups seemed to naturally divide into three distinct and roughly chronological typologies, roughly based upon what I term 'types' involved in hacking for social good, although there is considerable overlap in some areas. I have defined these types as;

1) An individual example of an 'ethical hacker' who has been involved in this practice since the early conception of personal computing in the 1960s and who applies her/his skills in what s/he describes as a socially conscious manner;
2) A variety of examples of ICT4D and development projects and individuals involved in this activity, many focused on overseas development work;
3) Examples of Civic Hackers who are involved in open-source hacking with the aim of solving social or humanitarian challenges.

These types provided me with an analytical tool to explore those involved in hacking for social good in relation to my research questions, thus deriving findings. For example, there seemed to be a number of key traits which differentiated these types discussed below. It is interesting to note that, despite the fact that I found all of these types to be involved in hacking as an activity, what this meant varied greatly from, for example, open-source development to penetration testing. They therefore provided an interesting basis upon which to discuss the definitions of hacking for good and also allowed me to define the research group which I intended to focus upon.

This typology of hackers might be viewed as a normative approach in that it attempts to produce a standardised model of these groups, however, this was both useful and necessary in that it allowed me to more tightly define my research field. The typology was also based upon data which allowed me to form a model rather than starting with any predefined theory.

1) The first type, the Ethical Hacker, consisted of just one individual who was not part of the same community as the other two types. This individual was more tied to the practice of hacking as breaching network security (‘cracking’), albeit in a legal and ‘ethical’ manner. This individual was involved in computer hacking in its early emergence around the 1960s and adhered to the original MIT Hacker Ethics. However, Pete was interesting from the point of view that he described himself as an ethical hacker and I believe he is representative of a wider group, many of whom might be described as the predecessors of Civic Hackers. This was because he displayed many of the ethics associated with hacking such as an interest in ‘hacking’ beyond computers, exploration of technology, promotion of informational freedom and, of most note, a belief in the social good of hacking. This individual overtly linked his technological practice to wider social issues, both in his personal life and in society more widely. The Ethical Hackers provided a useful reference point within which to situate the other types of hackers since they bore some ethical and historical relationship to this movement. Despite this relationship, however, those involved in this activity could not be described as overtly involved in hacking for social or humanitarian good. I decided, therefore, not to make further use of this type of hacking as part of my subsequent

research since they were not directly relevant to my own research questions;

2) The second type, ICT4D Hackers, provided some further historical context to demonstrate from where I believe hacking for social good emerged. This was partly from the ICT4D movement which resulted from a merging of ICT and humanitarian development during the early 1990s. The members of the ICT4D group generally tended to be highly educated males, the products of US and UK higher education institutes, with backgrounds in IT who became interested in development work during the late 1980s and early 1990s as a result of a heightened interest in the topic of humanitarianism more generally, according to my interviews. There were certain groups that I did not have access to, including those hackers with more technical skill who make more use of closed internet forums. In addition, my language skills limited me to English language forums. So while this sample of those involved in ICT4D displayed features of hacking and exhibited elements of a Hacker Ethic, they did not self-identify strongly with hacking as a practice. I therefore decided not to focus upon ICT4D activists within my own project;
3) Finally, the third type, Civic Hackers, were involved in more recent developments in the blending of ICT with humanitarian work. Although there were a number of overlaps with ICT4D activists, these individuals were largely either not involved in the ICT4D movement, possessing little knowledge of it, or opposed to it as a concept. The Civic Hackers produced a number of quite different applications, discussed below,

> which seemed influenced by the technological affordances available, such as ‘web 2.0’, social media and wireless networks, but also, I would argue, as a result of a stronger and more overt self-identification with the Hacker Ethic. My interview data suggested that globalised events, simultaneously online and offline, where hackers met up to collaborate on humanitarian projects, formed an important part of this movement. I identified this last type, Civic Hackers, as the primary group upon which I would focus my subsequent project, due to the opportunities which they presented in terms of addressing my research questions.

Based upon my literature review (Chapter 2), one theoretical framework for exploring this group was the argument that a Hacker Ethic is increasingly becoming integrated into wider areas of society, including humanitarian work. In order to test this inference, I identified that it was important to explore further the extent to which elements of the Hacker Ethic, as described previously (Section 2.2.2), feature among those involved in Civic Hacking and the extent to which group members self-identify with hacking as both a practice and a culture.

Civic Hackers can be distinguished from the other types which I have identified by their overt involvement in hacking for social causes. While there are overlaps with ICT4D activists in terms of their humanitarian motivations and use of technology, Civic Hackers are much less focused on global issues and also approach locally sited social issues through their activities. The range of problems which they attempt to solve can vary widely but tend to emphasise appropriateness and involvement of end users. The technologies used and produced by Civic Hackers can also be very different but there is a definite popularity of crowd sourcing, mobile devices, open data aggregation and use of 'web 2.0' and social media. However, they also place an emphasis upon involvement of non-technical participants and do not view hacking as a practice which is only confined to technology. This is a social group and one which blends real world events with online forums. Collaboration is a key feature of these events and this extends to a wider appreciation of democratisation of technologies. I was interested to note that this group expressed an interest in the history of technology. They were also pragmatic rather than idealistic in their approach towards hacking, and were willing to involve government and corporations in their events.

4.3.2 Theme 2: The Social Shaping of Technological Artefacts

This theme related to my research question 'in what ways are the technological artefacts produced by Civic Hackers shaped by the ethics of these groups and wider social factors?'. The findings in Section 4.2.2 suggest that the technologies produced by ICT4D workers in the early 1990s were quite different in some respects from those being produced today by Civic Hackers. From my interviews, it became clear that those working within the ICT4D movement often established much more centralised and traditional methods of working, and they sometimes created technologies which did not focus on the needs of end users.

Based upon my interviews and observation, the emphasis in more recent Civic Hacking projects, on the other hand, has been on the Hacker Ethics described in Chapter 2. This, I would argue, is more strongly aligned with the Hacker Ethics described in my literature review and might be seen as a proliferation of such Hacker Ethics into other fields, such as humanitarian work.

One way in which I approached my fieldwork was by drawing upon the strong body of research into the social shaping of technology and technologies as cultural artefacts (See Section 3.1.2. I believe that by exploring the technologies produced by Civic Hackers, asking what kinds of user interface they have?, what form does their code take?, how are their buttons constructed?, inferences can then be made regarding how they were created and what they tell us about the groups that produced them.

I was concerned with the groups involved in the shaping of these technological artefacts. I was also aware, however, that these groups, and therefore technologies, might also be shaped by wider *societal* factors (see Chapter 3). By adopting this approach, it was possible to 'trace' these technologies, following them through time to analyse how they have changed with the various types involved in hacking for social good.

1. Ethical Hackers such as Pete, who emerged from the early hacking culture of the 60s and 70s, were more involved in *testing* existing technologies than producing them. What they did produce was more focused on the security aspects of computing, particularly into the 1980s as state and corporate control began to tighten around technologies, particularly

Microsoft, and the idea of criminal hackers emerged. This was the point at which the idea that technology should be used for good, started being applied to trying to protect technologies and make them safer for users. However, Pete's description shows how ethical hackers were also involved in early analogue and hardware hacking whether for music or networking. Ultimately, it was these early hackers who were responsible for creating much of the technology behind personal computing and the internet (see Section 2.2.2);

2. Those involved in the ICT4D movement since the early 1990s are more closely linked to more traditional humanitarian and development groups, either as professionals or volunteers. There are certainly some within this type who can be described as involved in hacking in that they are involved in open source development and adhere to at least some of the Hacker Ethics. In terms of the technological artefacts produced by these groups, however, they tend to be informed more by traditional software development than the Hacker Ethics. Although some of those involved display these ethics and are involved in what might be described as hacking, the typical participant described above tends to be male, white, middle class and from a UK or North American higher education system and closely linked to the corporate IT industry. The technologies they produce are reflective of this, often involving data access and analysis tools. In this type, the developer sees a problem and sets out to build a technology to solve it. There is, on the other hand, also a clear link to the type of end-user hardware hacking carried out among developing

communities with less access to technological wealth which provides the potential for exploring how technologies might be shaped in differing ways in various cultures, particularly outside of the North Atlantic;

3. The more recent groups involved in hacking for social good have a new approach towards humanitarianism and have developed a different set of technologies from previous groups such as ICT4D, since they are influenced by both the available tools and social background. In some ways, their approach is much more closely aligned to the Hacker Ethics. From my research, my findings were indicative of the fact that aspects of the Hacker Ethic, including appropriateness, collaboration and decentralisation, can be seen in technologies such as crowd-sourced data collection and mobile phone tethering. It was this group, (Civic Hackers), who became my main research focus, and I went on to look in more detail in Chapters 5-7.

4.3.3 Theme 3: The Democratisation of Technology?

This theme related to my research question ‘to what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?’. A common theme which emerged within my interviews and fieldwork was the extent to which the technologies created by hackers involved in humanitarian work did, or should, represent a ‘democratisation of technology’. In other words, whether technologies such as social media and mobile phones are increasing levels of access to technology and information.

Within the portraits set out above, there was an indication that the technologies associated with hacking for social good were opening access to a larger range and depth of the global demographic. This idea was evident as an aspiration among the earlier Ethical Hackers, but was very much an ideal among those involved in both ICT4D and Civic Hacking. Among the ICT4D community, this viewpoint was closely connected to debates regarding the Digital Divide and lead-user innovation (see Section 2.2), whilst among Civic Hackers there was a sense that this democratisation of information technologies was already a fact of life, as reflected by the spread of social media, crowd sourcing and cheap mobile technologies.

As I will describe later (Chapters 5-7), I decided to explore whether this focus on democratisation was a feature of Civic Hacking through applying the methods discussed in Chapter 3 (Social Network Analysis, Narrative Analysis, interviews and participant observation), across participants of a Civic Hacking event, online Twitter activity relating to a different Civic Hacking event and the narratives used in online data relating to Civic Hacking. It was useful to analyse in greater detail what form the technologies produced by Civic Hackers took in order to test whether they were indicative of a group which values the democratisation of technology. An alternative, less technologically deterministic approach, would be to ask whether changes in wider society, the influence of Hacker Ethics for example, are being reflected in the kinds of technologies produced by Civic Hackers. And whether such changes include a move towards greater democratisation of technology, data and information.

4.3.4 Theme 4: Virtual Communities

This theme related to my research question 'what types of communities are formed by Civic Hacker groups?'. It became clear from interviews that the groups and individuals I was studying comprised some sort of community, in that people knew one another and were involved in the sharing of ideas and content via a system of networks, both online and in the real world. This also, however, seemed to form a highly globalised network, and was made up of a highly heterogeneous set of individuals in terms of gender, occupation and age. This led me to question just what it was that connected such a community.

There are a number of key sociological texts in this area, mentioned in Chapter 2, which may provide some insight and which I intend to use as analytical frameworks for exploring this theme (Section 2.2.2). My own observation revealed various common traits among this community from demographic background to shared interests. However, most of the members had never met in real life. English was the predominant language in this community which may have biased my data collection (see Section 3.1.3) but it was clear from my interviews that an interest in technology, formed a shared 'language' among these participants, overcoming cultural or linguistic barriers.

A core element of my interviews focused upon individuals' motivations for participation in Civic Hacking, and I found that the majority were keen to use their technological skills for the greater good of society, whether global or local. As discussed in Section 2.2.2, the motivations for participation in a virtual community have previously been used, particularly when studying hackers, in order to explain what causes individuals to form those communities. These have included 'communities of interest' and 'communities of innovation' and 'gift societies' (Raymond, 2000b; Rheingold, 1993; Seymour-Smith, 1986). Much of this theoretical work had, however, yet to be tested against empirical data from hacker communities, mainly due to access to first-hand informants. One method I made use of as described in Chapter 3 was the use of Social Network Analysis (SNA), supplemented by more in-depth qualitative fieldwork, to explore and test some of these previous theories on my own groups. This will be discussed in more detail in Chapter 6.

4.4 Summary

The three portraits presented in this chapter comprise a sample of the data gathered during this initial phase of research based upon interviews with seven subjects, participant observation and online data collection from social media, blogs and websites over the course of one year (2011-2012). I have presented the findings from this data and the wider themes and questions which emerged from this analysis.

The typology which I identified above served only as an interpretive framework around which to analyse my data. In reality, there is considerable overlap between the views, motivations and background of all these participants, regardless of the type to which I have assigned them. The ICT4D activist type, for example, can be seen to identify to some extent with those Hacker Ethics such as informational freedom and collaboration (Chapter 2). Similarly, there are some members of the Civic Hacker type who do not consider themselves hackers and who could not be said to engage with a Hacker Ethic or working practice.

The next phase of my research focused upon the group that I have termed Civic Hackers. At the same time, I acknowledge that this group cannot easily be considered in isolation from the wider ICT4D community and from other types of hackers, such as the Ethical Hacker of my first portrait. I chose to focus upon the Civic Hacker group because, based on the above data, they offered the best opportunity for addressing my research questions relating to the social shaping of technologies, relationships between hackers and democratisation, and the proliferation of the Hacker Ethic into wider society and hacker communities.

It became apparent from this initial research sample that many of the participants I was able to access were not themselves hackers in terms of having technical involvement with hacking. I believe that this is mainly the result of approaching ‘spokespeople’, those involved in the more vocal public relations side of Civic Hacking. While these individuals make an important contribution, they were not the focus of my research interest, and so a key aim of my next research phase was to gain access to those involved in the more practical aspects of Civic Hacking, since these individuals would hold the most potential for exploring hacking as a practice. On the other hand, these peripheral members, and their involvement in technical communities, did also represent an interesting, and under-researched, group.

From the research I had carried out so far, I identified the use of conference-type events (‘*hackathons*’, ‘*commons*’, ‘*camps*’ and ‘*unconferences*’) as potentially important venues for the study of Civic Hackers. These events formed spaces during which Civic Hacker groups, usually virtual communities, based online and distributed globally, came together within a physical environment. They therefore presented important opportunities to gather ‘real-world’ data with which to triangulate any online data I might gather. These events were also under-researched and so they offered a chance to address this lack of understanding. It is one such event which provides the focus for the next chapter.

Chapter 5

Analysis of the ‘Random Hacks of Kindness’ Civic Hacking Event

5.1 Introduction

Having identified Civic Hackers as a distinct group on which to focus my research project and some of the events in which they participated, I set out to conduct research focused on one such event. In this chapter I shall present the findings of fieldwork involving participant observation and interviews which I carried out at the Random Hacks of Kindness (RHoK) hacking event in Southampton during a two-day period in 2012 (see Section 3.1.3). Through a combination of online and offline research methods, I explored the event which Civic Hackers took part in, the technologies they produced and the individuals involved. Based around the RHoK event, this chapter explores the motivations of Civic Hacking participants, building upon the theoretical framework provided in Chapter 2, particularly the idea of a Hacker Ethic.

5.1.1 Research Aims

My starting point for approaching the RHoK event was an attempt to understand the motivations of those taking part, particularly the basis for my conceptual framework in the Hacker Ethics. This was related to my research question ‘in what ways are the technological artefacts produced by Civic Hackers shaped by the ethics of these groups?’. I also hoped to gain some insights into the type of community formed by this group, the relationship with democratisation and finally the extent to which the Hacker Ethics are increasingly seen in wider areas of society.

5.2 Research Findings

5.2.1 The Formation of Groups and Problem Topics

Observing how the initial event unfolded produced a number of findings which allowed me to address my research question regarding the relationship between Civic Hackers and the Hacker Ethics. The first distinct stage of the RHoK event involved the presentation of ‘problem definitions’ in which several of the participants outlined a rough idea for a technological solution to a problem, usually environmental, social or humanitarian (Fig.6). There were also two ‘remote’ presentations from representatives of development organisations, based in Zimbabwe and South Africa, using Skype.

This is fairly typical of these events as they tend to involve an element of interaction with globally distributed groups and individuals sharing similar interests. A key part of RHoK and other such events is an emphasis upon awareness of this wider global network using social media. Some of the problems presented at RHoK events were in fact connected to other events, either held previously or occurring in other countries.

Figure 6 The Presentation of 'Problem Definitions'

Once these problems were presented, they were decided upon by the participants and smaller groups of between two and five formed around each topic. This decision process, however, did not take shape in an organised manner but rather occurred quite organically. Participants seemed to gravitate towards a particular group as a result of a shared interest either in the topic or the technology involved.

Some of the participants arrived with well-formed ideas already and in-depth Power Point presentations, often relating to a previous project they wanted to progress. Others seemed content instead to turn up and 'see what sounded interesting'. Where a difference of opinion did occur between two individuals' ideas, or where there was not enough interest in a particular topic, the participants tended to negotiate a middle ground, finding a crossover between the two topics or agreeing to look at their idea at another event. There had been a certain amount of discussion prior to the event (which continued afterwards) around potential topics to work on using social media, and the RHoK organisers encouraged people to post problems on their website before the event. In this case, some participants formed groups of two, or worked alone on their idea but alongside another group with similar interests. After all, it seemed important to the day's proceedings that people were choosing to be there and that everybody had a chance, within reason, to do what they wanted.

5.2.2 The Civic Hacker Work Ethic

The ways in which the RHoK participants approached the event was useful in terms of addressing their relationship to the Hacker Ethics. Once the topics were chosen and groups formed, the participants sat in loose circles around tables. Some sat off to one side, at their own table where they could concentrate more intensely, only leaving at sporadic intervals to ask a question of the rest of the group. This layout is fairly typical of hackathons and seemed to differ from more formal settings such as conferences. Even this physical layout, I would argue, is in some way reflective of an aspect of the Hacker Ethic - the decentralisation, described in Section 2.2. The approach of these participants towards the task at hand seemed, at times, almost offhand, as though they didn't really need or want to try too hard, as if it was all just a bit too easy:

> *"…I guess my reasons for attending were to use my skills to help people, to meet new people who are interested in similar things to me, and to have some fun…" [RHoK 2012 Participant]*

In other moments it was intense, driven and focused to an extent which one rarely sees in conventional work settings. But this did not feel like 'work' as such – there was no obvious sense of obligation or hardship involved; only what hackers often describe as passion, joy and creativity:

> *The day starts at a crawl. No agendas here, not a registration table or name badge in sight. A few people gradually start to trickle in. There is no strong structure around timings and a relaxed atmosphere sets the scene. People are after all, they say, choosing to be there. I volunteer to put up a few signs, hastily scrawled together on the back of a research paper. My general feeling is that people are friendly, welcoming and inclusive in a low key sort of way; a sense of 'in it together' comradeship that one might associate with a gym class. More informal say than a tutorial, perhaps, less so than a festival. There has been a pub meeting beforehand which a few of those here attended. The organiser of the event, organiser in the loosest sense of the term, goes through a set of slides, discussing the aims of the day, its structure, health and*

> *safety formalities – it's all fairly fluid. We then go around the room then and people introduce themselves, talking about their interests and what kinds of technical skills they have to offer [Field notes, May 2012, Southampton].*

This formed an interesting moment in the proceedings, the point at which the event took on, for the first time, the feeling of a more formal conference or a class, the difference being that its participants were neither being paid to take part or required to - they were instead choosing to donate their weekend, their spare time, to take part in the type of activity which the majority of them had spent the preceding working week doing (Fig. 7). It was the first moment at which one might begin to question the motivations for taking part in such an event, and indeed the wider social context into which this phenomenon might be situated. Often, these projects were closely aligned to their own work or academic research. Many of them spent the time leading up to the event and after they left working on the projects. It is a passion, something they enjoy, their life. Many of the participants also involved their family in the RHoK activities with wives, girlfriends and children dropping in and out.

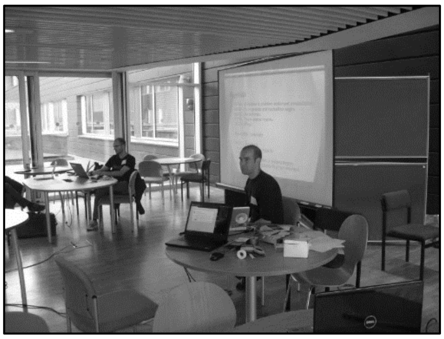


Figure 7 The Organiser Opens the Event

The groups divided in terms of skills and specialisms - a cluster of two coding Python over here, another coding PHP over there. No roles were ever assigned in any formal sense, no instructions given. People seemed just to know what to do and found it obvious that they should – the kind of improvised and impromptu creativity of music or art. The groups often got on with their work in near silence and when they did break to talk it was to discuss a problem or ask a question before continuing on again in this way (Fig.8).

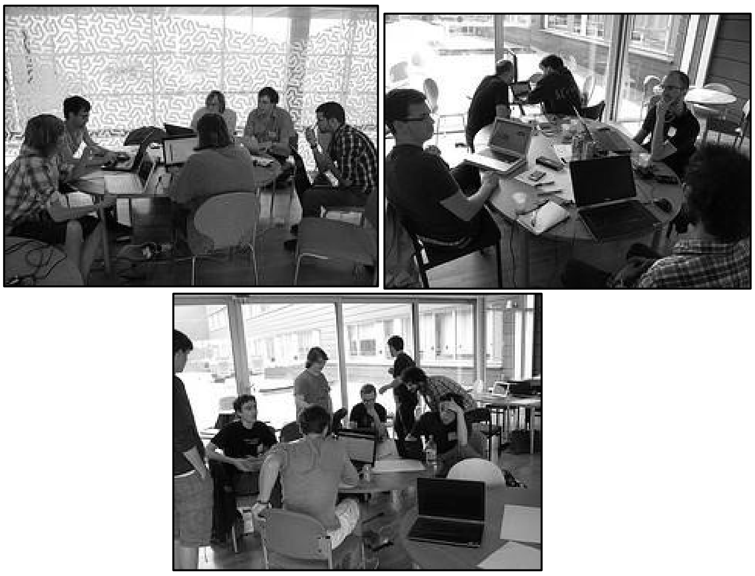


Figure 8 The Subdivision of Groups

I observed that everyone was included not just those with the most skill. There was an unstated understanding that people were giving up their time voluntarily and so allowances should be made:

> *The attendees are 'hacking' but they are not necessarily self-defined 'hackers' as defined. Of course they share a common interest in technology but they are geologists, social scientists, web developers. Their goal is to find out*

> *how technology can make the world a "better place" - that and the challenge of testing their technical skills [Field notes, May 2012, Southampton].*

Everyone's skills were made use of and the multidisciplinary makeup of the group included web designers, geographers, engineers, computer scientists and knowledge from many other fields. It was apparent, however, that the focus of the event was largely technological and that there was little involvement from 'non-geeks' such as designers, user interface experts or development workers, a fact which some of the participants were keen to see change:

> *"...It is easy to end up with some great technology which solves some hard problems, but no-one can understand it, or wants to use it, because it hasn't got a sensible interface. I think in many ways the involvement of development workers is even more important. If we're creating technology to help people then we need to make sure we are creating technology that they actually want to use. This is the problem we are having with WaterMe (the project we started at the RHoK event and continued since then) at the moment. We have lots of good technological ideas, and could easily progress with developing them, but we are all rather concerned as to whether what we are doing will actually be useful to the people we are trying to help! Really we need to have contact with development*

> *workers right from the beginning so that we can develop projects that will actually be useful to people…" [RHoK 2012 Participant]*

As the weekend progressed, the room itself became increasingly messy with cables strewn around the room, half-drunk cups of coffee and empty bottles and pizza boxes. However, the event organiser sat somewhere around the middle of the room, moving between groups to collect progress reports and direct the course of the event in line with some of the overall RHoK requests. It was apparently important to the event that updates were recorded and shared across the different global participants, forming a networked community which will be explored more fully in Section 5.2.3.

5.2.3 The 'Social Geek'

One of my research aims was to explore what type of communities might be formed by Civic Hackers. The idea that each of the RHoK events do not exist as disconnected, standalone entities but rather as part of a wider network of global hackathons seems of great importance to both the organisers and participants. In Section 3.1.2 I explored how this has been noted at hackathons and suggests that the hacker's existence as part of a wider networked community, both locally and virtually, is central to the hacker "*lifeworld*". This has involved the use of IRC, mailing lists, web pages and wikis before, during and after hacker 'cons' with hackers "fluidly moving" between the offline and online world to coordinate and comment upon events as they unfold. For some of the RHoK participants, however, this sense of community was not always apparent:

> *"We had various Skype conversations on the main screen during the day, and we could see video feeds from the other events, but I didn't really feel connected. I think that was partly because we were all so busy trying to get our code working that we didn't have time to get connected, and partly because the methods of getting connected were fairly difficult (Skype conversations were often difficult to hear, the video feeds were pixelated etc.)..." [RHoK 2012 Participant]*

Several of the participants of the Southampton RHoK created an Internet Relay Chat (IRC) channel, one of the oldest and arguably more stereotypical hacker communication tools of choice, in order to share more conveniently within that group. Added to this was a wide array of platforms including personal Twitter feeds, GitHub, Flickr, UStream and official RHoK websites, all used in different manners in whatever way best suited the situation with participants moving between them with ease:

> *"...our project is ongoing and is undergoing a transformation into a humanitarian start-up, so it's very relevant to be in touch with all the other Rhok'ers to pass on any useful knowledge..." [RHoK 2012 Participant]*

The Southampton group was linked to a wider network of global events (Fig.9). On occasions where expertise was needed in certain areas, Skype was used to communicate with those in other countries who possessed the required knowledge and skills.

markiliffe 19 mins
Really good chat with @elazungu about the upcoming #RHoKSoton hackathon. Really looking forward to the hacks!

elazungu 20 mins
interested in #HTML5 and real life bug reporting, hack on #taarifa, one of the projects to be presented at #RHoKSoton

SamuelSLee1 9 hours
@timdavies Tim, would you DM me your email address. Want to touch base before #DDC2012 about how we can best present ideas to #RHoKSoton

elazungu 14 hours
To all #RHoKSoton people, note the changed start time (9am) and MAC

Figure 9 Networked Online Interaction

A projector screen at the front of the room also displayed live video feeds of other global events which people were keen to dip in and out of, intended to give them a sense that they were part of something much bigger – global yet local, a typical feature of Civic Hacking as a movement. The event organiser used social media such as UStream, a live video broadcasting platform, to keep information flowing to participants and organisers in other countries. As well as a continuous live stream from a webcam, he captured regular updates and interviews which were then posted to the RHoK website and distributed widely through Twitter:

> *"Sketching out a plan for collecting sensor data in #taarifa and visualise it. @markiliffe gave us a tour of Dar via Skype. #RHoKSoton" [@NicoWeinert, Twitter, 02/06/2012 12:56]*

The participants of this event had travelled from across the south east of the United Kingdom, with the majority living in Southampton and several making the trip from Portsmouth, Oxford and London. It was apparent that previous events in London had attracted individuals from a broader geographical spectrum due to its size, however, the Southampton area did have what could be described as an emerging open-source hacking community. Many of the participants were involved in other open-source projects and might be viewed as being part of a localised community of Civic Hacking events and groups, with some having further links to a wider community through global events such as RHoK, contacts and online forums.

I found from observations that the participants in this event formed a complex community of some sort, however just what form that community took was less obvious. There were clear relationships between those within the room and those beyond on a global level; a variety of weak and stronger ties including colleagues, friends or the exchange of code; those with shared interests and knowledge; virtual and real-world.

It might be tempting to describe the group involved in RHoK, as a 'virtual community' based around common interests as described in Section 2.2.2. It is worth noting, however, that relatively little empirical data exists to substantiate previous theoretical frameworks used to describe hacker communities. At this point, I identified that there was potential for the use of both quantitatively and qualitatively grounded Social Network Analysis to explore factors such as the sharing of code and social media interaction in shaping these communities and to map the distribution of 'power' and 'influence' among members of the Civic Hacking community (see Chapter 6).

What is clear, however, is that these individuals differed significantly from the reductionist stereotypes of hackers and 'geeks' as reclusive or anti-social (see Section 2.2.3). In fact, far from being 'awkward', my findings make evident that the act of hacking relies heavily upon sociability and the ability to negotiate complex group dynamics. Although this may always have been the case to some extent, it is increasingly true due to the importance of social media and the understanding of social issues required among those involved in activities such as Civic Hacking and hacktivism.

5.2.4 A Metaphor of Power Cables

Despite the division of the room into separate 'teams',

there is little sense of rivalry or competition between the

> *different groups. The event seems to operate more as one group with participants frequently assisting each other with both ideas and technical equipment. One interesting manifestation of this atmosphere can be seen through the way in which power, specifically power cables, are shared among the group. During my fieldwork, I several times note an occasion whereby a member of the group finds themselves without a source of power. This could be the result of having no spare plug sockets or to connect to the wireless internet connection. There is at once hurry among those present to rummage in their bags from a choice of countless different power adaptors, to rearrange their own sources and clear tables to make space in order to ensure that no one is left without this important commodity for longer than is necessary. This is particularly noted upon a new member, a latecomer, joining the group. Power, it seems, is a currency at this event and appears to hold a great deal of symbolic efficacy. So we end up with a huddle of people around a table, remotely focused on their individual screens yet closely connected, sharing each other's power sources – All 'hanging' off the same Wi-Fi, 'tethering' from a single smart phone, bridging off devices, sharing connection [Field notes, May 2012, Southampton].*

It should not be surprising that this particular metaphor emerged since hacking is ultimately about sharing, collaboration and inclusion. To be without power, to be disconnected, within a Network Society based around informational networks is to be disenfranchised and without voice. This is, in some ways, the power of hacking - to find connection in situations where one might not otherwise, both in a literal and metaphorical sense. After all, one of the ideas which first inspired the ICT4D movement and, I would argue, still holds a certain degree of hesitant influence in Civic Hacking, albeit controversial and somewhat outdated, is that of a Digital Divide, discussed in Section 2.3.1. In some ways, the sharing of power cables within this small group might act as quite a useful metaphor for this idea. This sharing is intrinsic to the process of hacking and to the Hacker Ethic (Section 2.2.2). The idea of hacker communities as Gift Economies has been a central feature of many attempts to explain the motivations and how they might shape the structures of such groups (Section 2.2.2). So, for those involved in the RHoK event, the freedom to access technologies often walks side by side with the idea of an open and sharing society.

5.1.4 Coding the World: The Social Shaping of Civic Hacking Technologies

Previous notable studies of science and technology have focused upon a research method of '*following*' the various phases through which an object moves and thus revealing something of the processes by which it is shaped by its creators and the '*shadowing*' of individuals as they go about their working day (See Section 3.1.2). As I have discussed, such research methods translate well to an exploration of the social construction of technological artefacts, not only in terms of these processes involved, but also what the final products of this process might reveal about the groups which produce them. Within my own research project, I made use of these techniques to address my research question of whether the ways in which these technologies might be indicative of the ethics of Civic Hackers.

In the case of the RHoK hackathon, I observed three unique phases which can be identified as part of the process by which hackers construct their technologies (Fig.10) and which, I would argue, reveal some interesting insights as to their nature.

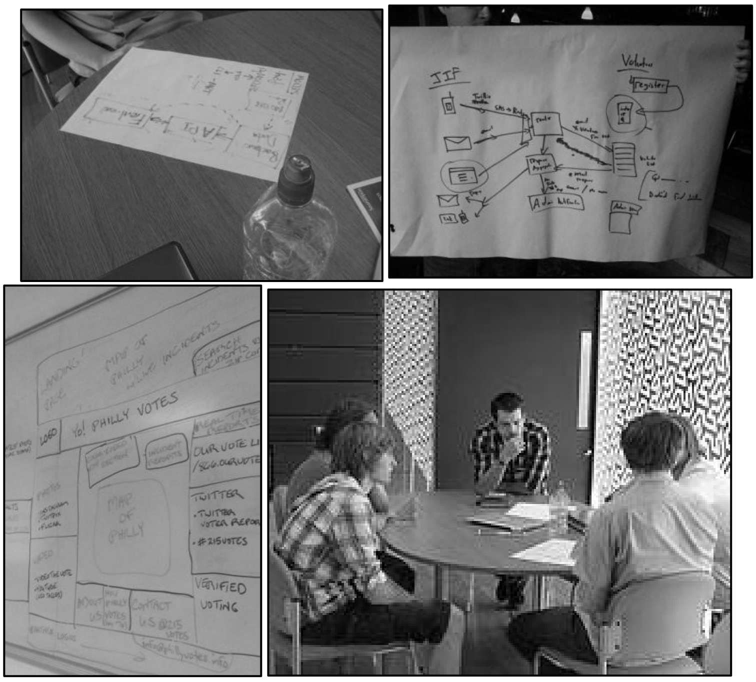


Figure 10 The Initial Phase of the Process

Phase One: Once the groups and topics were decided, the initial phase for the participants was to gather around their table and discuss the problem at hand, their ideas for solving it and to transfer these thought processes onto paper in the form of diagrams and plans. In the case of this particular team, for example, they began with a discussion of the overall problem and the background before beginning to sketch out a potential solution. One team member with less technical skill volunteered to carry out online research to identify drought locations which might be used for their project. This phase was a creative process, a team effort in which collaboration and working together was assigned importance. It was also a stage during which even the less technically skilled members of the group were included, before tasks were divided up among those with particular expertise. Once transferred onto paper, the ideas took the form of diagrams and sketches. These were quite rough and sketched out in an animated way, with boxes, lines, scored out, redrawn. This was quite different from the way in which code is carefully crafted through structured processes and defined stages. Instead, this phase provided everyone with an opportunity to work through ideas without having to worry about making more significant mistakes.

Phase Two: In the construction of these artefacts, the next stage was the translation of this paper-based plan into code. This stage seemed based around the idea that there were many smaller problems to be solved along the way. The majority of these kinds of projects involved, for example, accessing open-data from various different sources and in different formats and aggregating these into one platform to create what is known as a '*mashup*'. The hack, as such, occurred when the group made use of ‘workarounds’ and innovative scripts to make this work. Various tasks were allocated based on skills or programming expertise so one person might be knowledgeable in, for example, management of SQL databases while another may have experience in Java web development. The subsequent work was then carried out mostly alone or in pairs with often only minimal contact during this process. This was seen as the main phases of the weekend and a number of participants stayed up all night working on it. Their activities were only interrupted by occasional requests to provide video updates to the event organisers.

Phase Three: Once the code had been written and some kind of artefact produced, the next stage of the process was to share and distribute this artefact using various different means. The sharing of code and ideas was part of a continual process throughout the event with participants required to upload their source code to GitHub and upload video diaries to YouTube. As the event neared its conclusion, however, the event organisers began a more formal process of encouraging participants to upload their code and create links to the official RHoK site. At this stage, the groups also rushed to give themselves a name. The culmination of this was a presentation in Washington in which all videos from global participants were compiled and displayed. Finally, the participants were asked to vote on their favourite hack within the local event and the event organiser presents various prizes to the winning teams. For many of the teams, the process of building these technologies continued after the event itself through online collaboration and subsequent meetups.

I would argue that this process by which ideas are transformed to paper and then to code which was finally presented to and shared with a wider community, can be effectively explored by using the steps described in Section 3.1.2 to analyse the methods in which the material world is transformed into items of scientific knowledge. While scientists tend to capture and record the physical world, the hackers I observed began with ideas which were then transformed into a physical format on paper which could then be regulated and controlled. These paper-based plans were turned into code, a format which, like a piece of architecture, the skilled hacker was able to manipulate. The final outcome was a set of user-interfaces and technologies which were shaped by this process and also reflective of the social context in which they were created. This digitisation is all part of the process by which, I would argue, a "*lifeworld*" is 'translated' into code.

The artefacts created by the RHoK groups tended to be quite open in nature. They were free to be manipulated by anyone with the technical skill to programme and often to some without those skills. They were also what might be described as 'democratic' to the extent that they often focused upon the visualisation, through maps and charts, of crowd-sourced data. Often, data could be added by individuals without internet access through SMS using mobile phones, taking into consideration regional variations in internet access. Therefore, it might be argued that the final artefacts which were produced by these groups are reflective of the process in which they were created – an open process; a democratic process; a fluid process; a lack of centralisation.

But the artefacts created could also be seen as indicative of a wider social context in which the above ethics are valued. In some ways, the very code itself was a reflection of these Hacker Ethics and imbued with something of these values. A code can be both a string of symbols and a set of ethics by which a person lives their life. This visualisation of the world through data and information symbolically takes it apart, deconstructs it, and rebuilds it within a 'box' where it can be controlled and manipulated. After all, as already discussed, this ability to manipulate informational networks is where some of the power, both technically and symbolically, of the hacker lies.

5.1.5 Analysis of Some Commonly Used Narratives

One of my interests in this research project was in exploring what, if anything, might be seen as uniting this particular group into some sort of shared community. From this, I hoped to contribute to the wider understanding for hacker communities generally. It might appear rather obvious at first, however, for the participants, an interest in *technology* is a central theme which gives them some sort of distinct shared interest. This interest is what brings these people together, most of them did not know each other previously and many come from fairly different backgrounds, despite at first glance appearing to be quite similar.

During my observations at the Southampton event, I carried out some analysis of these different narratives as a way of exploring their interest in technology. Among more general discussions and 'techie' jokes, I found that narratives often fell into a number of main themes described below. Overall, I found that this shared interest in technology went beyond just the event at hand or Civic Hacking specifically and covered a range of different subjects, many of them quite revealing in terms of motivation and their relationship to the Hacker Ethic. These narratives are indicative of ties which go some way to explaining the ways in which this community which forms around, not just technology, but also wider interests. It is interesting to note that people tend to talk in terms of hacking as an activity rather than describing themselves as hackers. This is in fact true among many of the hackers I have spoken with.

Narrative Type #1: Narratives of Openness and Sharing

There was a great deal of discussion among the group that these types of events should be more open to a range of different people. In particular several individuals mentioned the idea that 'non-techies' are often excluded for technical reasons and spoke positively about the involvement of professionals such as designers, social scientists and development workers:

> *"....project managers, 'virtual media PA's to help individuals connect to other currently running hackathon seeking synergistic projects, 'helpers' to google everyone's questions, evaluate what is out there and help drill down to the detailed information that is needed right away, designers and media people for sure, everyone's presentations and video production would have benefited*

> *from a lot of help, I fell into a project management role quite soon which was new and fun!" [RHoK 2012 Participant]*

This theme was reflected in narratives around the types of technologies which Civic Hackers produce and the ways in which these kinds of technologies could be made more inclusive through user interface and adaption for smart phones. I noted several conversations regarding the ownership and sale of data by corporations and governments which tended to involve an emphasis upon the democratisation of information, strongly rooted in the open-data 'movement'.

This democratisation even extended into the event itself with participants discussing the ways in which the judging of the event could be made more 'democratic' using online crowd-sourcing technologies. These types of discussions might be viewed as indicative of an interest among this group in the 'democratisation' of technology, an important component of the Hacker Ethic. It also reflects an understanding that hacking is not just a technological pursuit but rather governed by a philosophical ethos which goes beyond technology and into wider areas of society. As I have acknowledged in Section 3.4.3, however, it is worth noting that this event was relatively homogenous in terms of gender, race and class. This may be reflective of science and technology more widely. In order to address this gap, there is certainly scope for future research into female focused Civic Hacking groups and those who may be more diverse in nature (see Section 2.2.3).

Narrative Type #2: Narratives of Technology

As mentioned above, the primary shared interest among this group was technology itself and narratives of technology were a primary means for sharing and consolidating ties between members. This took the form of a range of conversations both during hacking, in the numerous breaks between activity and even afterwards by email and message boards. Common discussions involved the new Ubuntu interface, the development functionality of Windows 8, rumours and gossip regarding new kinds of motion controlled laptops and touchscreen devices, stories of building homemade drones, ECG controls, and robots. There was a strong interest in 'dev kits', prebuilt devices which allow hackers to create interfaces between hardware devices such as buttons or sensors and software based applications:

"….I love messing around with Arduino sensors….." [RHoK 2012 Participant]

A typical theme of discussions also surrounded user interface and how many operating systems are badly made from a design point of view, thus excluding many users. The collaborative process of open-source was generally put forward as a more reliable solution to creating effective user interfaces than corporate IT development. Primarily, this can be viewed as a community which forms around a shared interest in technology. However, I would also argue that these views of technology also originate from within a wider 'world view' of openness, liberalism, and collaboration.

It is a common trait among most of the individuals I interviewed for them to talk in terms of hacks and hacking, an adjective, rather than describing themselves as hackers, a label often seen as too boastful to be self-assigned. Often this term seems only useful when describing to outsiders what they are not. Based on my observations among the RHoK hackers, the labelling of an individual as a hacker tended to be external and those involved in this activity often self-identified much more closely than that, for example, with particular technologies. It was interesting to note that the organisers of RHoK did, however, emphasise this 'hacker branding' in their marketing of the event and through their websites. This is not uncommon in other similar events such as Mozilla Summer Code. This re-appropriation of hacking terminology and, the attempts by corporate IT and government to jump on the 'hacker bandwagon', did not go unnoticed by the participants. They were certainly aware of the apparent conflict between the ideals of corporate IT and mainstream development organisations and those of the open-source hacking community.

Narrative Type #3: Anti-Authoritarian Narratives

As discussed in Section 2.2.3, a great deal of literature on hackers has been involved in a binary distinction between 'good' and 'bad', ethical and deviant, the complex reality of hackers is that the two blend together and that often deviance and criminality are the result of outwardly imposed distinctions (Section 2.2.3). There has been an anarchic streak running through the Hacker Ethic from the early MIT hackers which is also apparent in those I have observed. It was interesting to note that my initial observations of the RHoK event did not align with these framings:

> *The room is open and spacious and clean, not at all what I was led to believe from my previous readings of 'hacker cons'; those dark, chaotic circuses of code which drag on late into the night, fuelled by beer and fast-food and sprawling wires. But then this is not really like those other events – it does not seem related to a distrust of authority or even purely technology [Field notes, May 2012, Southampton].*

During my analysis of the narratives being used by participants, however, a connection to this anti-authoritarian theme could be observed. Many narratives among this group seemed to involve taking pleasure in the idea of 'getting one over' on authority while demonstrating their superior technological skill. This ranged from the use of 'legitimate' SQL injection, talk of how to bypass Wi-Fi access controls on the university campus to narratives of climbing fences in campus in order to take measurements for scientific experiments:

"....They locked the Wi-Fi access to your MAC address.....It's really easy to bypass that ....." [RHoK 2012 Participant]

Conversations frequently also turned to the work of GCHQ, the ethics of government and private sector data collection, the feasibility of hacking into university printing services and how one might hack PayPal. All theoretical, of course, and mainly the result of technological inquisitiveness but, I would contend, indicative of an anti-authoritarian trait which is important to the Hacker Ethic.

Narrative Type #4: Narratives Regarding the History of Technology

A final narrative theme which seemed to form the basis for a number of conversations relates to the history of science and technology. While attempting to code data into the correct geographical and temporal format, for example, discussions turned to the history of Greenwich Mean Time, the invention of mechanical timekeeping and navigational tools. I also recorded a narrative about a joiner who passed down his craft over hundreds of years which had been perfected over time and remains to this day. There was talk about the historical 'punch cards', the origins of modern computing, a story about secretaries typing out lines of code by hand and about the design drawn onto the window of the university campus:

"….That geometric pattern…it's a circuit design isn't it? ….." [RHoK 2012 Participant]

These kinds of narratives about the history of technology represent a shared language, a common point of reference which ties the participants of the RHoK event together despite some apparent differences in terms of occupation and age. It also features as the expression of an acknowledgment among them that they are part of something bigger, a longer line of technologists and inventors. This feels in some ways similar to the desire to recognise a wider global community at these kinds of events.

Hacker narratives of these types are indicative of the ethics which underpin this technological activity. I would argue that narratives of openness and sharing, exploration, anti-authoritarianism and exploration are evidence of a set of plural and fluid Hacker Ethics running through the RHoK group. These are concepts which provide shared interests among the members and the acting out of them through conversations and storytelling act to cement and reinforce their values.

5.3 Discussion

5.3.1 The Hacker Ethics and Civic Hacking among the RHoK Event, Community and Technological Artefacts

In this chapter I have gathered and analysed data based upon one particular group and event, comprised of nineteen individuals in one room over one weekend, trying to instigate positive changes through technological innovation. By doing so, I have addressed my research questions in relation to the ways in which technological artefacts are shaped by their ethics, the types of communities formed by Civic Hackers, their expression of democratisation and the extent to which this represents a proliferation of the Hacker Ethics into wider society.

I have shown some of the ways in which the RHoK participants were connected to a much wider global network of likeminded people and similar events. Previous theoretical framing devices of hacker communities provide us with some understanding of the motivations which lie behind these connections, the ties which hold them together. These may include a scepticism towards authority, liberal ideas regarding informational freedom or simply a passion for technology; the 'geek' within. So from these motivations, I would describe this as a 'community of interest' (Section 2.2.2). Specifically, however, these interests indicate important elements of what previous researchers have termed the Hacker Ethics (Section 2.2.2). Among this group, the telling of stories seemed to play an important role in the expression of these shared interests whether through narrating the history of technology, college pranks and rule-breaking, openness and sharing or technology. But I found that such narratives also had a *performative* quality, reinforcing beliefs and cementing ties among the group. This was something I was keen to explore further (see Chapter 6).

Some more binary previous theoretical framings of hackers were found to be rather flimsy when tested among the RHoK event. In this pristine room, far from the "dystopian, binary, deviant, North Atlantic, males" of hacker folklore (Section 2.2.2), I instead found a 'social geek'. One who is connected, and for whom connectivity is essential – a more pragmatic and realistic hacker. The importance of social media to these groups was one clear example of this sociability. This could be most clearly seen through the metaphor of the power cable. The importance of being connected, to the internet, to the grid, was symbolic of a society in which informational networks were central. The ability to manipulate such networks, thus circumventing physical and symbolic power structures is why hackers more generally occupy such a significant position within the 'Network Society', and potentially a threatening one in the eyes of authority (Section 2.3.1).

The RHoK Civic Hackers also, however, represented a cultural group which formed around an activity which not only challenged access to physical informational networks but was also acutely aware of the relationship between these physical networks and the social implications of them. Thus, this may go some way to explaining why these Civic Hackers assigned this connectivity such a central position within their ethics. There is an extent to which inequality of access to technology and informational networks are related to economic and social exclusion, both globally and locally.

Groups such as RHoK, which seek to apply hacking skills to addressing this inequality, are indicative of a new 'type' of hacker motivated by social good who see themselves as grounded in democratic social and technological movements such as open-data, open-gov and crowd sourcing (see Chapter 4). This 'type' are also influenced by, and in turn are shaping, Web 2.0 technologies such as apps, smart phones, wireless devices and social media.

Although events such as RHoK may have their origins in the world of technology, and hacking in particular, their scope can now be considered much wider. These types of events are now becoming fairly common in academia, business, journalism, even government.

Based upon my findings, I would contend that this group is strongly connected to the Hacker Ethics as described by previous authors (Section 2.2.2). I would argue the RHoK event was indicative of a particular way of viewing the world by hackers, a social and cultural worldview associated with collaboration, openness, exploration and anti-authoritarianism, related to but not determined by hacking as a purely technological activity (see Section 2.2.2).

There was no sense of competition among the RHoK participants, despite the fact that the event was essentially a challenge in which teams competed for a prize. Instead, there was a strong desire to include all members of the group, regardless of their technical skill. The structure of the event was relatively decentralised, with only a loose sense of leadership or structure. This was replicated globally as other teams and events took part independently with a low level of interference from the organisers.

I also found these Hacker Ethics to be present in the processes followed by Civic Hackers when producing technological artefacts at the RHoK event and the types of technologies involved. This involved a high degree of collaboration and inclusivity of different people, including those without technological expertise. The tools they produced were also quite open and 'democratic' in nature, often involving crowd sourcing or appropriate low-tech solutions.

Changes in working practices, described in Section 2.3.2, emerged within the 'Network Society' since the 1960s with a greater emphasis upon capitalism, more focus upon informational networks, decentralisation and knowledge based working practices. Many of the traits of these societies also form important areas of the Hacker Ethics - deregulation, liberalisation, privatisation and globalisation. It is therefore unsurprising that hackers emerged from the libertarian social and cultural movements of late 1960 North America and these open-source communities and their technologies themselves are in fact reflective of this background (See Section 2.2.3).

My findings in this chapter indicate that the RHoK even, and Civic Hacking as a movement, should be viewed within this wider context of Network Societies. The motivation of those RHoK participants with whom I carried out my research can, I would argue, be further understood through this theoretical framing device. In addressing the question of why these individuals volunteered their weekend, none of them registered a difference between the working week and leisure time. Instead, it seemed rather to form one large and continuous part of their lives, a blurring of work, study and leisure time. Those involved in this activity comprise a homogeneous group and frequently cite a range of motivations from the thrill of technological exploration to civic obligation - a duty of those with the ability to contribute to society. They also strongly correlate with the Hacker Ethics of creativity and passion as described in Section 2.2.2. This group seemed fascinated primarily with the processes I will describe below, the working through of problems, the testing of skills - a hack is, after all, an overcoming of a problem, technological or otherwise.

An exploration of the processes by which the various technologies were produced during the RHoK event as well as the nature of these outcomes as cultural artefacts was also revealing. I found them to be reflective of a process which is grounded in the Hacker Ethics of openness, sharing, collaboration and decentralisation, a *bazaar* (Raymond, 1999) through which the hacker *lifeworld* is turned into code. Here, the metaphor of a code seems most fitting – both the digital string of symbols and a set of ethics, a way to live one's life.

5.3.2 Proliferation or Appropriation of Hacker Ethics?

As such, the RHoK event reflected the fact that elements of this Hacker Ethic are increasingly widespread in many fields beyond hacking itself. One might argue that the Hacker Ethic has influenced wider societal changes in the IT industry and other fields (Section 2.2.2), I would like to propose an alternative viewpoint. Rather than viewing this as a dispersal of the Hacker Ethic into wider society, it is my contention that such Hacker Ethics themselves form part of a wider social and cultural movement which comprises all of these above groups. Instead of viewing wider emerging movements such as open-data, peer-to-peer sharing or crowd-sourced banking as being influenced by a *technologically determined* Hacker Ethic, I would argue that these movements, including hacking, are indicative of a wider and pre-existing social and cultural shift towards the democratisation of information networks. Therefore, while hacker events of the type witnessed during RHoK may be somewhat anchored in hacker culture, they also form part of a wider range of similar events outside of hacking specifically which have resulted from a social and cultural movement towards increased democratisation of information technology (see Section 2.3.2.

These movements should not be viewed as purely Hacker Ethics as such. Instead, hacking might be seen as an early example of this kind of movement which popularised it to some extent. Alongside this adoption of crowd-sourcing, 'unconferences' and other indicators of the democratisation of information in areas such as government, education and business, it is also interesting to note the extent to which there is a public interest in the important role that hacking has played in the wider mainstream history of technology. I would argue that examples of this can be found in the desire to include hackers in popular narratives of science and technology (Section 2.2.3).

Similarly, I found that the organisers of the RHoK event made conscious and overt use of 'hackerisms' in their branding of the event from its name to the format of the events themselves. There was a sense at times that the corporate sponsors were aligning themselves with overt uses of hacker terminology in an attempt to lend themselves an air of 'underground' legitimacy.

I would contend that such corporate branding and marketing of RHoK has parallels with the wider market in which a consumerisation of technology has taken place. At first glance, this appears in stark contrast to the act of hacking which aims to go beyond a 'black box' approach to technology. If we return to the original Hacker Ethic, however, we find that this is not as it first appears. In some ways, the development of technologies such as Facebook, crowd-sourcing, open-data, even Apple have contributed to a greater democratisation of information. For better or worse, the user-friendly interface of the Low Orbit Ion Cannon (LOIC) DDoS tool utilised by the Anonymous hacktivist movement allowed a far greater degree of participation by members of the public in what was previously a technologically exclusive act (see Section 2.2.4). More relevant was the role of social media in the Arab Spring uprising. While it certainly was not the instigator, and the population was quick to move to more traditional methods once social media channels were cut off by the government, it did allow for a far greater spread of participation.

On the other hand, while this kind of technology may be less elitist in providing greater access to information, it should certainly not be confused with hacking. Often, those using it do not fully understand what is going on behind the 'black box', thus creating opportunities for surveillance or misuse. It may also be a factor in exaggerating existing inequalities as there will always be those who have less access to these technologies than others.

There was certainly evidence within the RHoK event for the notion that changes in working practices within the Network Society are resulting in a blurring between work and leisure (see Section 2.2.2). It was an interesting exercise comparing the RHoK event to conventional paid employment. In some ways, the participants were taking part in what felt similar to work or university – they gave presentations, introduced themselves to the group, worked together with strangers, sat in front of a computer late into the night. An event such as RHoK, it seems, is neither work not hobby but something of both. Although unpaid, it was not quite the 'weekend only' leisure activity of the ham radio or model railway since it blurred much more into people's everyday activities.

This provides some potential explanation for the motivations of those involved in these kinds of groups. This emphasis upon 'work for work's sake' can be seen as reflective of the Hacker Ethic (Section 2.2.2) and I certainly found evidence within my own group of informants that this blurring of work and leisure time did exist.

As discussed in Section 2.2.2 it has been argued that, rather than dividing 'true hackers' from the 'mainstream' corporate IT industry, we should instead view the Hacker Ethic as having shaped these commercial markets and technologies. I contend, however, that this Hacker Ethic has had an influence upon areas beyond computer hacking. This can be seen, I would argue, across a range of interrelated emergent practices noted in Section 5.2.1.

5.4 Summary

The increasing global reliance upon technology and commercialisation of information has in some ways decreased the availability to individuals and exaggerated existing inequality (Section 2.3.2). In other ways, however, the availability of networked technologies has provided 'disempowered actors' within such society the means to challenge embedded power structures including corporate and governmental (Section 2.3.3). The technological artefacts produced through RHoK are expressions of this contest and reflect a wider move towards democratisation seen in various movements. Those at the RHoK event resisted corporate power and the traditional dominance of development work through collaborating on hacks to producing locally appropriate solutions. Their artefacts and narratives provided insights into this attempt to re-negotiate the power relationships embedded in the technology and redistribute information to the many.

The final outcome was rough – just a basic prototype, a seemingly messy collection of coloured blocks on a map. But that was not the point. After all the effort which the groups put in as they hammered out lines of code late into the night in an empty campus, the clatter of a keyboard echoing down the corridors. Then, huddled together around the blinking light of a single laptop came that moment when they realised that it actually worked. This ethic, *lifeworld*, had resulted in something. They had somehow captured it and made it real - staring at them through the code.

During my time at the RHoK event, it had become clear that there were a number of similar hackathon events in which Civic Hackers participated. I had also found that online forums social media played a central role in these events. I was therefore keen to make use of these online data sources in relation to another Civic Hacking event.

Chapter 6

A Community of Ethics: Social Network Analysis of the #hack4good Twitter Network

6.1 Introduction

Running alongside 'real-world' events such as the RHoK hackathon, it was apparent from my interviews that the Civic Hacking community also engaged in a large amount of online activity including Twitter, Facebook and blogging, which provided me with a potential useful data source for exploring this group. For many of the members, it seemed that online activity was as important to their understanding of what it means to be involved in Civic Hacking as was attending real world hackathons.

In this chapter, I will present the findings and analysis from research conducted on a Twitter network relating to #hackforgood, a series of global hackathons similar to, but separate from RHoK, which aims "…to present problems, form teams and solve the problems using each of our individual strengths in technology…" (Hack4Good, 2014). These events are organised by Geeklist which is a social networking site for programmers, coders and the tech community.

The network which formed around the #hack4good hashtag was used in a variety of ways explored in more detail below. This included the event organisers using it for promotion, co-ordination and publicity, by members seeking advice or engaging with fellow hackers and by members of the wider hacker/tech community who may have had an interest in these events. As discussed in Chapter 3, it was important to select a different event from RHoK in order to triangulate my findings against a different data sample and apply my research questions to a different field site. I also chose to focus on the official #hack4good network since this was the most used hashtag in relation to this event and thus likely to provide more data.

6.1.1 Research Aims

This chapter explores further the themes which emerged through my research at the RHoK event by triangulating them within a different 'field site' (see Chapter 3). My purpose here was to establish whether the same Hacker Ethics defined previously were also present within these groups among the online space of Twitter in terms of group structure and the activity of members. I hoped that this would address my research question 'what types of communities are formed by Civic Hacking groups?' to build upon both my conceptual framework and research findings from Chapters 4 and 5.

If we were looking for indications of the Hacker Ethic at work in a community, one would expect to see a fairly open and sharing community. In terms of Social

Network Analysis (SNA), this might be reflected as quite a decentralised structure and a flow of information back and forth between the members.

6.2 Research Findings

As described in Chapter 3, NodeXL was used within Microsoft Excel to import all tweets utilising the hashtag #hack4good. Since I was limited to a thousand tweets (due to processing power), the data sample was taken between 21/02/14 and 01/03/14.

This analysis provided 240 'vertices' (Twitter users) with 68 duplicates giving a total of 181 unique 'vertices'. Within this network, there were 154 'edges' (ties between users) and 29 'self-loops' in which the user links to themselves (e.g. by referencing themselves within a tweet).

The data gathered was then analysed further as described below. These analyses were intended to explore the following factors which would allow me to address my research questions;

- The structure of the network;
- The different roles of actors within the network;
- The nature of the ties between actors;
- To define field boundaries/key informants within which to carry out interviews and participant observation.

The research findings presented below are presented based upon the particular measure applied to the Twitter data sample, namely In-degree, Out-degree, Eigenvector Centrality, Between-ness Centrality, Closeness Centrality and Group by Connected Component.

6.2.1 In-degree

The In-degree indicates the number of ties received by an actor from other members of the network. It is often used as a measure of "prestige or popularity" (Section 3.2). Within the #hack4good Twitter network, In-degree ties consisted of 'mentions' or 'replies' in which actors were referenced by other members.

When the #hack4good network was grouped by level of In-degree the maximum In-degree was 24 incoming ties, and the average In-degree for the whole group was 1.318. Eight groups emerged, including a large group with members who all had an In-Degree of n=0 and therefore represent those with no incoming ties i.e. mentions. This large group represented 38% of the network or 58 actors, demonstrating that a high proportion of people had no inbound ties and suggests that they were not mentioned in tweets.

Unsurprisingly, those with a high In-degree were organisations and event organisers rather than individual members. The entity with the greatest number of incoming ties was @gklst who was the event organiser. The entity with the second highest volume of incoming ties was @gdnglobaldevpro, a community of development professionals organised by the Guardian newspaper.

I therefore extracted the individual 'human' (non-organisation) members who possessed an above average In-degree in order to see what might be revealed.

Due to the anonymous nature of Twitter, organisational actors were not always easy to identify based on their profile details, however, it was possible to get a sense in most cases.

I then selected only actors with an In-degree of greater than 2, which gave a total of 41 network members (see Fig.11).

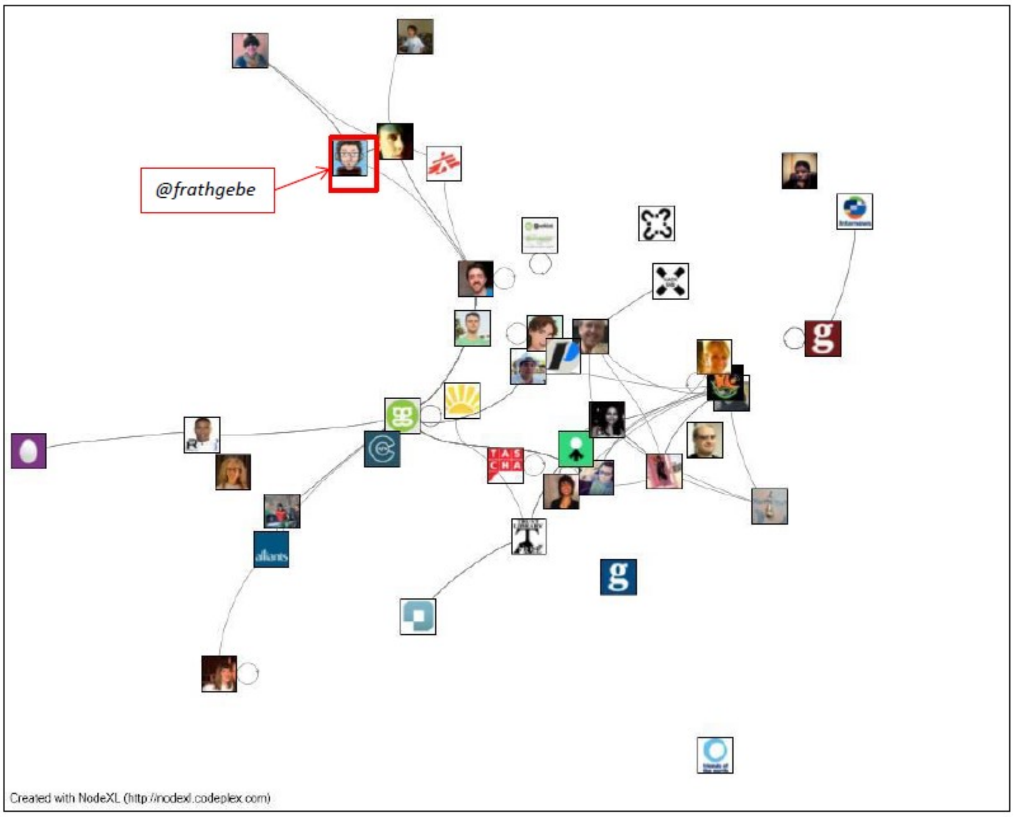
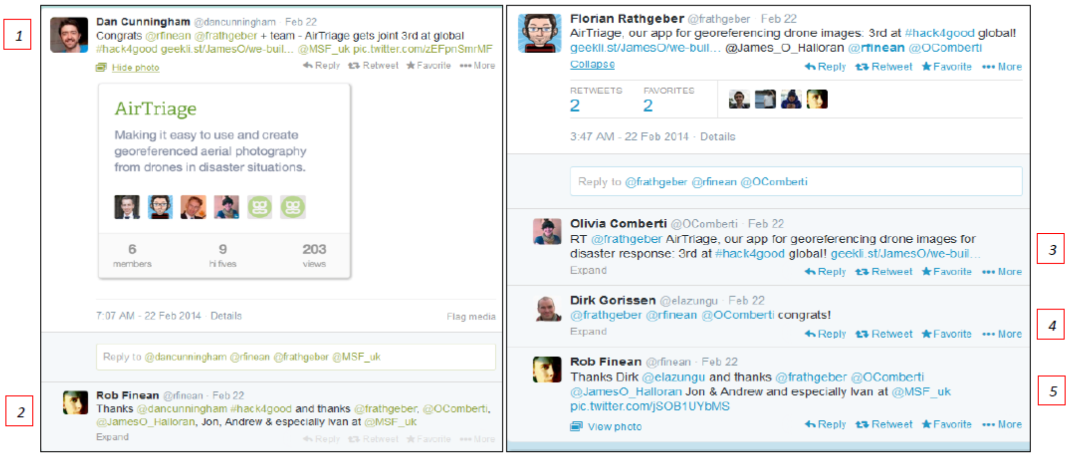


Figure 11 #hack4good Actors with an In-degree of Greater Than Two

The majority of these inbound ties were 'mentions' which meant that the network member being addressed had been referenced in the tweets of others. This might indicate that they have had some level of influence or significance within the network, or that there was interest in their activities. Where these individuals were mentioned regularly within this sample in relation to this hackathon, I inferred that they were more likely to be important in some way to this network and were therefore worthy of further data collection and analysis.

I examined one member, @frathgeber, since this user was mentioned five times in tweets associated with the #hack4good hashtag during my sampling period (see Fig.12). These tweets were all accounted for by fellow members congratulating the user for winning third place at the event, and on two separate occasions by the same individual.



Dan Cunningham @dancunningham · Feb 22
Congrats @rfinean @frathgeber + team - AirTriage gets joint 3rd at global #hack4good geekli.st/JamesO/we-buil... @MSF_uk pic.twitter.com/zEFpnSmrMF

AirTriage
Making it easy to use and create georeferenced aerial photography from drones in disaster situations.

6	9	203
members	hi fives	views

7:07 AM - 22 Feb 2014 · Details

Reply to @dancunningham @rfinean @frathgeber @MSF_uk

Rob Finean @rfinean · Feb 22
Thanks @dancunningham #hack4good and thanks @frathgeber, @OComberti, @JamesO_Halloran, Jon, Andrew & especially Ivan at @MSF_uk

Florian Rathgeber @frathgeber · Feb 22
AirTriage, our app for georeferencing drone images: 3rd at #hack4good global! geekli.st/JamesO/we-buil... @James_O_Halloran @rfinean @OComberti

RETWEETS 2 FAVORITES 2

3:47 AM - 22 Feb 2014 · Details

Reply to @frathgeber @rfinean @OComberti

Olivia Comberti @OComberti · Feb 22
RT @frathgeber AirTriage, our app for georeferencing drone images for disaster response: 3rd at #hack4good global! geekli.st/JamesO/we-buil...

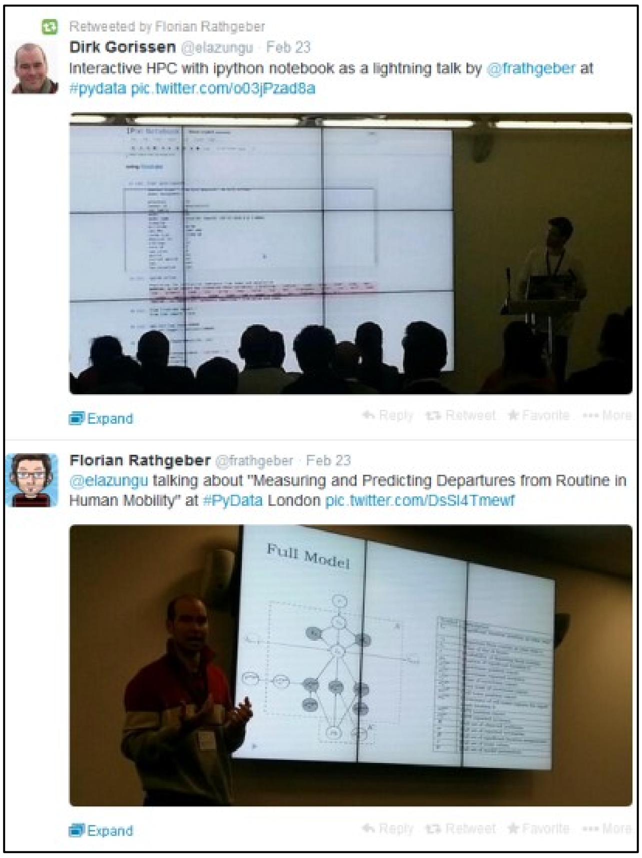
Dirk Gorissen @elazungu · Feb 22
@frathgeber @rfinean @OComberti congrats!

Rob Finean @rfinean · Feb 22
Thanks Dirk @elazungu and thanks @frathgeber @OComberti @JamesO_Halloran Jon & Andrew and especially Ivan at @MSF_uk pic.twitter.com/jSOB1UYbMS

Figure 12 Tweets Associated with @frathgeber

This might suggest that the high In-degree ranking of this member was related to a level of 'kudos' obtained through winning a prize at the hackathon. This form of 'social capital' gained by achievement has been described in other hacker communities (see Section 2.2.2) and is discussed in more detail later in this chapter (6.3.2). A high In-degree in Social Network Analysis can be indicative of "prestige or popularity" (Section 3.2) which was true in this case.

The extract from @frathgeber's Twitter page also demonstrated a relationship to the organiser of the RHoK Southampton event (Chapter 5) and to at least one of my other key informants (see Fig.13). There was therefore a suggestion that members such as this had important roles within the #hack4good community.



Retweeted by Florian Rathgeber

Dirk Gorissen @elazungu · Feb 23

Interactive HPC with ipython notebook as a lightning talk by @frathgeber at #pydata pic.twitter.com/o03jPzad8a

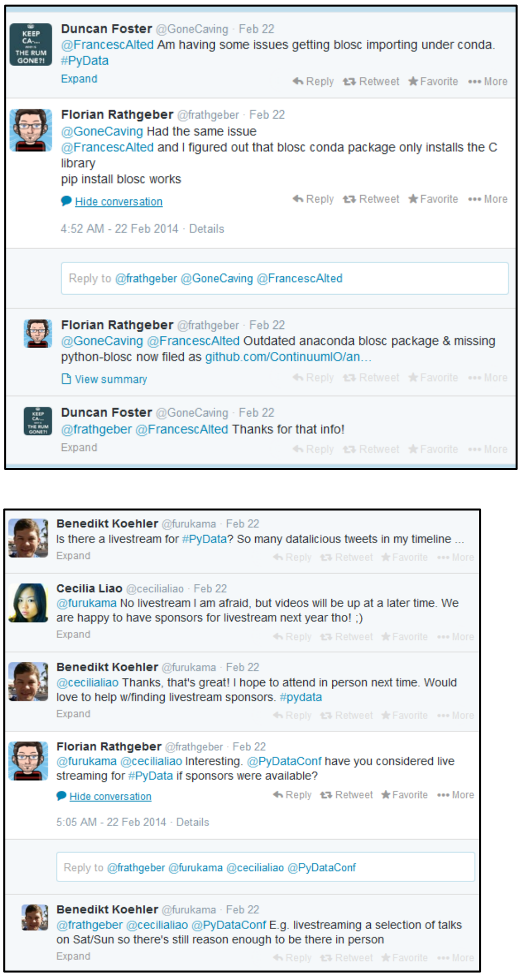
Florian Rathgeber @frathgeber · Feb 23

@elazungu talking about "Measuring and Predicting Departures from Routine in Human Mobility" at #PyData London pic.twitter.com/DsSI4Tmewf

Figure 13 Relationship Between #hack4good Actor and Other Community Members

The apparent significance in the #hack4good community of @frathgeber also led me to explore his personal Twitter page in more detail as he seemed to be quite an active participant in the Civic Hacker community. He had a number of questions directed towards him regarding technical advice and general information about events or the community. In this way, he might be viewed as quite an influential actor, as his peers sought advice from him as an expert. He was also a member of several different networks, acting as a common link or bridge between these otherwise separate groups. There was therefore a clear reflection on Twitter of the sharing and supportive attitude of network members which I noted in my fieldwork at the Southampton hackathon (see Chapter 5).

Analysis of the Twitter accounts of the other 40 members with higher than average In-degree values revealed broadly the same features. They all formed a central part of the #hack4good network through their influence, and this was largely derived from perceived technical expertise and advice to the rest of the group. They were involved in participating in the #hack4good event rather than being mere observers (see Fig.14).



Duncan Foster @GoneCaving · Feb 22
@FrancescAlted Am having some issues getting blosc importing under conda. #PyData

Florian Rathgeber @frathgeber · Feb 22
@GoneCaving Had the same issue
@FrancescAlted and I figured out that blosc conda package only installs the C library
pip install blosc works

4:52 AM - 22 Feb 2014 · Details

Reply to @frathgeber @GoneCaving @FrancescAlted

Florian Rathgeber @frathgeber · Feb 22
@GoneCaving @FrancescAlted Outdated anaconda blosc package & missing python-blosc now filed as github.com/ContinuumIO/an…

Duncan Foster @GoneCaving · Feb 22
@frathgeber @FrancescAlted Thanks for that info!

Benedikt Koehler @furukama · Feb 22
Is there a livestream for #PyData? So many datalicious tweets in my timeline ...

Cecilia Liao @cecilialiao · Feb 22
@furukama No livestream I am afraid, but videos will be up at a later time. We are happy to have sponsors for livestream next year tho! ;)

Benedikt Koehler @furukama · Feb 22
@cecilialiao Thanks, that's great! I hope to attend in person next time. Would love to help w/finding livestream sponsors. #pydata

Florian Rathgeber @frathgeber · Feb 22
@furukama @cecilialiao Interesting. @PyDataConf have you considered live streaming for #PyData if sponsors were available?

5:05 AM - 22 Feb 2014 · Details

Reply to @frathgeber @furukama @cecilialiao @PyDataConf

Benedikt Koehler @furukama · Feb 22
@frathgeber @cecilialiao @PyDataConf E.g. livestreaming a selection of talks on Sat/Sun so there's still reason enough to be there in person

Figure 14 Influence Derived from Perceived Technical Expertise and Advice

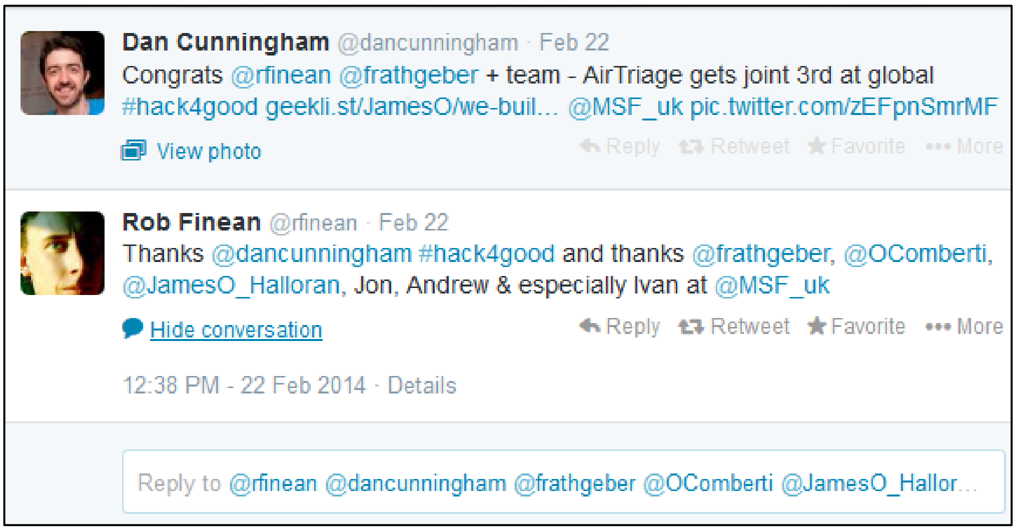
6.2.2 Out-degree

The Out-degree in a Twitter SNA analysis indicates the number of outgoing ties from a particular actor within a network. In my Twitter sample from #hack4good, these outgoing connections referred to mentions of other users in tweets or in replies to conversations. The Out-degree analysis revealed nine groups, with one large group in which all the members had an Out-degree of n=0 (no outward mentions) and a second large group which represented those members making n=1 outgoing mentions e.g. mentioning another actor in their tweets. From correlation of the In-degree findings above (6.2.1) with Out-degree, most users were referencing another actor rather than being referenced, while those who were being referenced tended to be an event organiser or community page. Those who showed quite a high Out-degree might be expected to be promoting something such as the event or informing others of something.

A relatively low proportion of the outgoing tweets were posted from the organising body, @gklst, while a high proportion (n=13) were from @dancunningham who was one of the individual organisers, and from @gdnglobaldevpro which is a Guardian newspaper community, although the majority of these latter out-going tweets were self-references in the user's own posts. This supports the idea that these kinds of tweets tend to be promotional in nature.

I excluded the event organisers and companies, and looked more closely at individual members who displayed a relatively high Out-degree, excluding any users with an Out-degree of less than 2, which left a total of 38 actors and 59 ties.

By selecting an individual member, such as @rfinean, who had an above average Out-degree (1.318) and examining the ties between this individual and other members it was possible to comment on the sort of relationships taking place. @rfinean was typical of members in this event. This user's outgoing tweets were used to thank other members in the hackathon event, particularly in response to them congratulating him on his success in the event (see Fig. 15).



Dan Cunningham @dancunningham · Feb 22
Congrats @rfinean @frathgeber + team - AirTriage gets joint 3rd at global #hack4good geekli.st/JamesO/we-buil... @MSF_uk pic.twitter.com/zEFpnSmrMF

Rob Finean @rfinean · Feb 22
Thanks @dancunningham #hack4good and thanks @frathgeber, @OComberti, @JamesO_Halloran, Jon, Andrew & especially Ivan at @MSF_uk

12:38 PM - 22 Feb 2014 · Details

Reply to @rfinean @dancunningham @frathgeber @OComberti @JamesO_Hallor...

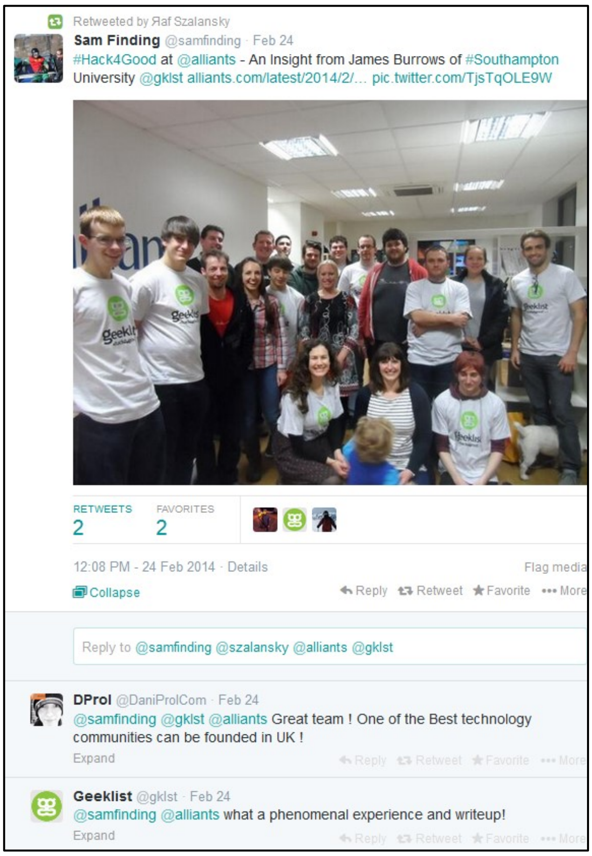
Figure 15 Kudos Within the #hack4good Network

Although this was based on data from only one individual, this finding was typical of the tweets made by other members in the #hack4good event. Within the #hack4good community there was an emphasis placed upon endowing kudos upon certain members of the group for their support, while also placing significance upon positive reciprocation of praise and promotion of positive behaviour in a fairly non-competitive spirit (despite the apparent ‘competition’ nature of the #hack4good events). This was a feature which I noted at the RHoK event and which was closely tied to the Hacker Ethics defined previously (Section 2.2.2).

6.2.3 Eigenvector Centrality

Eigenvector Centrality is a measure of an actor’s sum degree, weighted by the degree of the other actors (see Chapter 3). In other words, it tells us whether someone is connected to influential people within a particular group. Within the #hack4good network, the Eigenvector measure indicated that the majority of actors had little or no statistical influence within the network (0-0.006), i.e. the majority (76%) were not connected to anyone who was well connected. Again, this indicated a relatively centralised model in which the majority of members are not considered influential and are not particularly well connected. It is worth noting, however, that ‘unconnected’ in this case meant that they had not been referenced in tweets but did not necessarily mean that they were not connected in some other way.

By extracting the users with an above average Eigenvector Centrality (which was 0.006) the actors and ties could be explored in more detail. As with the previous measures, the actors with the highest Eigenvector Centrality were the hackathon event organisers, @kitchencred, @rekatz and @dancunningham, although interestingly the main organiser, @gklst, did not feature prominently. The individual member who scored most highly for Eigenvector Centrality in this sample was @szalansky who was not an event organiser. These tweets all relate to a photograph which was posted by this user and which mentioned a number of other users (see Fig. 16). This tweet has also then been 'retweeted' twice by other members.



Retweeted by Яaf Szalansky

Sam Finding @samfinding · Feb 24

#Hack4Good at @alliants - An Insight from James Burrows of #Southampton University @gklst alliants.com/latest/2014/2/… pic.twitter.com/TjsTqOLE9W

RETWEETS 2 FAVORITES 2

12:08 PM - 24 Feb 2014 · Details

Reply to @samfinding @szalansky @alliants @gklst

DProl @DaniProlCom · Feb 24

@samfinding @gklst @alliants Great team ! One of the Best technology communities can be founded in UK !

Geeklist @gklst · Feb 24

@samfinding @alliants what a phenomenal experience and writeup!

Figure 16 A Retweeted Posting Within the #hack4good Network

@szalansky's 'influence' in relation to this tweet was due to him referencing influential users in this posting, rather than through any reciprocation by these users, so one might argue whether this really implied influence at all. However, the retweeting of this photograph, and the comments made in them, may have demonstrated some level of interest in this posting and it clearly suggests that this individual was 'connected' to these influential members in some way. Within

Twitter though, it is worth noting that such an individual can link to influential members without them needing to accept or respond to a request therefore the individual may not be able to derive any benefit from being connected to them.

6.2.4 Betweenness Centrality

The level of Betweenness Centrality implies that an individual is a 'bridge' within their network. They can be considered essential to the structure of the network since if they were removed, it would collapse. These actors tend to have some level of control over the flow of information within a social network.

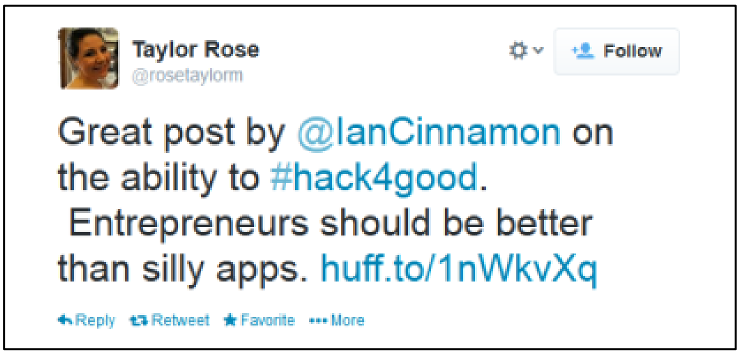
However, it is worth noting that on Twitter, this idea may be less straightforward than it at first appears to be. It is possible on Twitter for an actor to create links (tweets, mentions or follows) to anyone they wish, at any time, without reciprocation. Therefore, bridges within the online network can be fairly easily bypassed and should be considered more fluid than in a traditional social network. It may be more useful therefore to consider reciprocal 'follows' as being a more reliable measure of strong 'ties' when exploring relationships within the #hack4good network.

In my #hack4good Twitter sample, 107 out of 154 actors (69%) displayed an n=0 measure of Betweenness Centrality and the remaining 47 actors all had some non-zero level of Betweenness Centrality. The average Betweenness Centrality of the sample was 43.857. Extracting only those actors with an above average Betweenness Centrality left a total of 14 members. Of these, 6 were event organisers or companies/communities and the remaining 8 were individual members in the event. So this measure was less dominated by event organisers and thus may provide a more accurate indicator of individual influence within the network. The fact that event organisers were not the dominant actors in the Betweenness measure makes sense since they were at 'one end of the line' in terms of communication flow. They did not 'sit between' any other actors but were themselves the well-connected actors to which the bridge actors had a tie. Again, we see many of the same actors feature, including @szalansky and @rfinean. This led me to consider whether there was anything in common between these actors which made them influential within the #hack4good group. This is something which I will consider in more depth in my discussion (Section 6.3.3).

6.2.5 Closeness Centrality

Closeness Centrality is essentially a measure of how quickly actors can reach others within the group without needing to go through intermediaries. In other words, how quickly and efficiently they can relay messages through the group (Section 3.3.5). The hack4good network showed a number of groups by this analysis. For example, actors with only one mutual tie to another actor, who represented the maximum closeness (closeness=1), and those with no ties to other actors in the network but who referenced themselves (closeness=0). The average closeness for the network was 0.165. I selected any actors with Closeness measure above that value, which left me with 5 groups, including a total of 36 actors who might be considered above average in terms of closeness.

Looking at the specific tweets in more detail it was apparent that a number were promoting links to talks, blogs, links or articles by other members of this group (see Fig. 17).



Taylor Rose
@rosetaylorm

Great post by @IanCinnamon on the ability to #hack4good. Entrepreneurs should be better than silly apps. huff.to/1nWkvXq

Figure 17 A Tweet Promoting the Work of Others

They did not, however, tend to be promoting their own material but were making reference to the work of others. A number of tweets were also promoting a company which was offering open data to be used in the event. It is also worth noting that one of the actors was @twuoted, a 'quote tweetbot'. Although this actor was non-human, in some ways, this might be seen as validating the idea that this high Closeness group were 'messengers', since this app was designed to promote quotes throughout Twitter based around a particular hashtag. Within this group, almost half of the actors were organisations (47%). This compared to 21% for the above average Connected Component dataset (see Section 6.2.6) and 28% for the above average Betweenness sample. Based on just this data, the above average Closeness group could be viewed as consisting of the less active members in the event and of those more concerned with relaying messages or with promoting the work of others.

6.2.6 Connected Component

Networks can also be grouped by actors who mention or reply to each other in tweets i.e. have some sort of connection regardless of its type (Section 3.1.2). The graph in Fig.18 shows that, in the #hack4good online network, there was one large group with a number of smaller groups of decreasing size, some having no connections at all to other actors. As discussed previously, this is similar to the Degree measure but allows one to group those connected actors together to define well-connected groups within the network. I chose to explore this larger group as a way of defining a sample within which to carry out more detailed data collection and analysis. This larger group was selected because it was likely to provide a sample with a relatively high volume of connected nodes which would provide a large enough volume of ties to be examined in more detail.

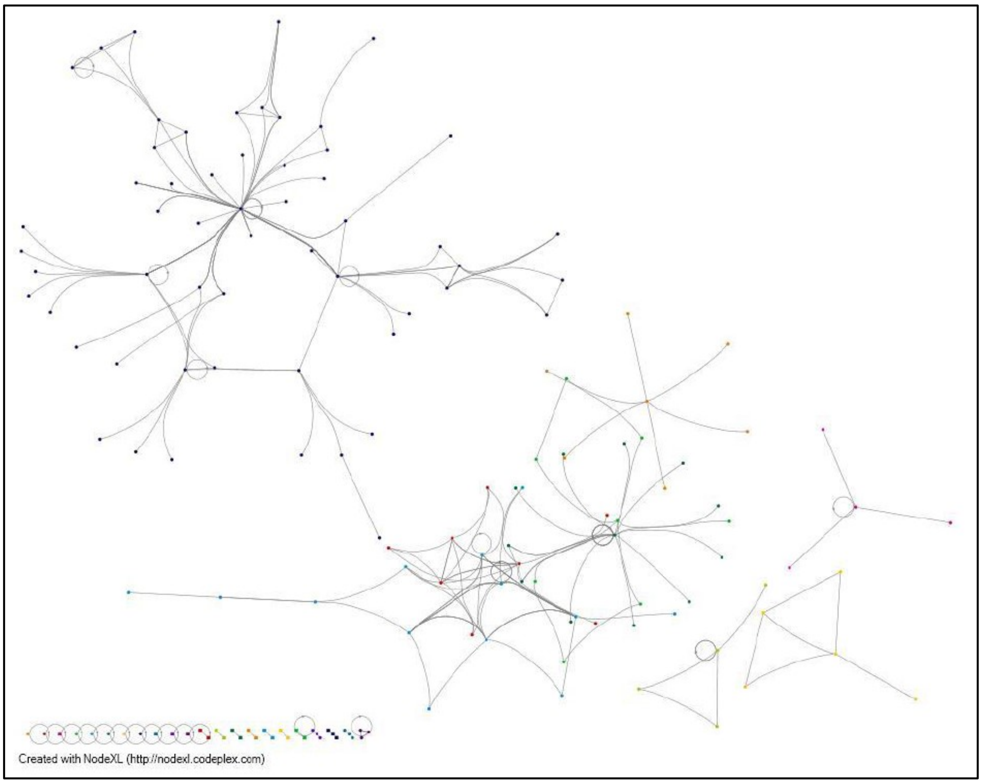


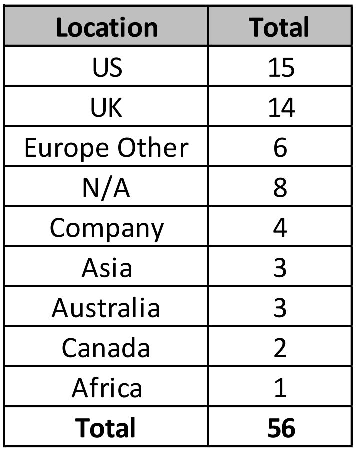
Figure 18 The #hack4good Network Grouped by Connected Component

Taking the group which comprised the most connected cluster within the #hack4good network, these were then examined in more detail. This group consisted of 56 actors in total. Within this group, 57% of actors were identified as male and 14% as female, as shown in Table.3. The remainder could not be categorised as they were either companies/organisations or did not state their gender.

Type	Total
Male	32
Company	12
Female	8
Not stated	4
Total	**56**

Table 3 Classification of highly-connected #hack4good members

Members were geographically quite distributed which is to be expected from these types of events, although the majority gave their location as the USA or UK (Table.4). Interestingly, interviews with #hack4good members suggested that these individuals had not met in real life. This is common to many online communities and is a feature of hacker communities based on my previous fieldwork (Chapter 5). As I will discuss later (Section 6.3.4), shared interest in hacking and technology may provide a commonality which holds these online groups together where real world relationships do not.



Location	**Total**
US	15
UK	14
Europe Other	6
N/A	8
Company	4
Asia	3
Australia	3
Canada	2
Africa	1
Total	**56**

Table 4 Geographical Distribution of highly-connected #hack4good members

Having selected this group, I then excluded companies and organisations to focus in on individual members. I used Twitter initially to Tweet and then Direct Message ('DM') these individuals by way of an approach, and to gain an email address at which further correspondence could be carried out. A DM can only be sent if someone is following you on Twitter. For those who replied, I then used email to ask them a range of more detailed questions in order to 'flesh out' my SNA data. 'Tweet' requests were sent to 39 individuals, and of these 17 replied with an email address. I then sent questions to 15 individuals, and of these 9 responded, giving an overall response rate of 23%.

My questions were intended to tie in with my previous interviews at the RHoK event (Chapter 5) and with Civic Hackers (Chapter 4) in order to triangulate my findings and included the following. These also allowed me to address the research questions described in Section 6.1.1;

- What was their involvement in the event?
- What did they see as the purpose of the event?
- Had they taken part in similar previous events?
- How long had they been involved in these kinds of events?
- Would they describe themselves as hackers?

The responses were collated and manually, coded to identify themes and commonalities in line with my research aims. The results are as follows;

- The respondents were aged between 21 and 45 years old, with no particular peak age range;
- The predominant occupation was in IT/software design/programming;
- They were geographically distributed - Europe, Zambia, USA, Australia;
- There were 3 females and 6 males;
- There were 3 organisers of events, the rest were members. Three were involved in coding/developing but the rest were more involved in coordinating the activity and facilitation.

Members used the following terms when describing their motivations for taking part in the #hack4good event, which could be classified into three primary themes;

- Theme One: Social aspects
- Theme Two: Desire to do social good
- Theme Three: An interest in technology

Theme 1 was the most popular motivation (56%) and the responses in this theme could be further subdivided into seven secondary themes (Table.5) which have some relationship to the social aspects of the event;

		Theme 1: Social Aspects	**Mentions**
Secondary Theme	**1**	Being part of a community	1
	2	Meeting new people	1
	3	Other social aspects of the event	2
	4	Working in a team	2
	5	Participation in activities	2
	6	Like the event organisers	2
	7	Being part of an important social movement	1

Table 5. Secondary Themes for Motivation

Members used the following terms when describing the purpose of the event, which again can be grouped under three primary themes;

- Theme One: Social aspects
- Theme Two: Desire to do social good

- Theme Three: Solving problems

Again, the social or community aspects of participation was emphasised (44%) in terms of purpose, and responses in this theme could be subdivided into six secondary themes (Table 6);

		Theme 1: Social Aspects	Mentions
Secondary Theme	1	Being part of a community	2
	2	Being inclusive	1
	3	Networking with others	1
	4	Being globally connected to others	1
	5	Collaborating with others	4
	6	Involvement regardless of skills	1

Table 6 Secondary Themes for Purpose

This finding was interesting as the idea of collaboration within a group of likeminded individuals was also a finding which I observed at the RHoK event where I concluded that this was often more of a motivation for taking part than the ‘social good’ aspect.

In addition, the following information was obtained from the respondents;

- 8 out of the 9 respondents had been involved in a previous similar event. It was also apparent that projects tended to be carried on beyond the actual hackathon;
- Respondents had been involved in this activity for between 1 and 3 years;

- The question of whether they would describe themselves as hackers produced some interesting responses. The majority (56%) said yes although, as expected from my previous research (Chapter 5), the answers were not straightforward and involved a great deal of self-debate and definition regarding the meaning of the term. I found from responses that in this setting they might be described as hackers although not in their day to day lives:

> *"...The word has been redefined a lot. A hacker is an enthusiastic and skilful computer programmer, a hacker is a problem-solver, a hacker is someone who thinks outside of the box, who disregards the rules. All these definitions describe me. So yes, I would describe myself as a hacker..."*
>
> *[Hack4good 2014 Member]*

6.2.7 Exploring the Ties between Actors

I then explored the types of ties (edges) which connected the #hack4good members in more depth, in order to establish what their content was and what they might reveal about the group. I was interested to go beyond the overall structure of the group but to assign some value to the ties themselves. After all, while a tweet may imply some kind of relationship between two members, it tells us relatively little about the nature of that relationship, or what kind of communication is taking place – for example, the sharing of information or a narrative. It also does not tell us whether this connection is positive or negative, or the direction of commodity flow.

Being well connected on Twitter does not necessarily require any 'effort' or reciprocation in a social sense, since anyone can reference anyone else without needing their approval. Reciprocation on the other hand, for example replying to tweets, may imply some level of relationship. However, this tie would need to be explored in detail in order to gain some insight into its nature e.g. positive or negative. The strength of a tie could also be inferred through its duration or the frequency of communication.

In order to narrow my focus, I looked for the days on which the greatest volume of tweets was generated (Fig.19). The two peak days for tweet activity were the 22/02/14 and 24/02/14, with 62 and 60 tweets respectively. These values were significantly higher than on the seven other days in my sample. I was interested to explore this peak activity in more detail to see what it was related to as it seemed likely that an increase in activity might represent some topic or area of significance for the members.

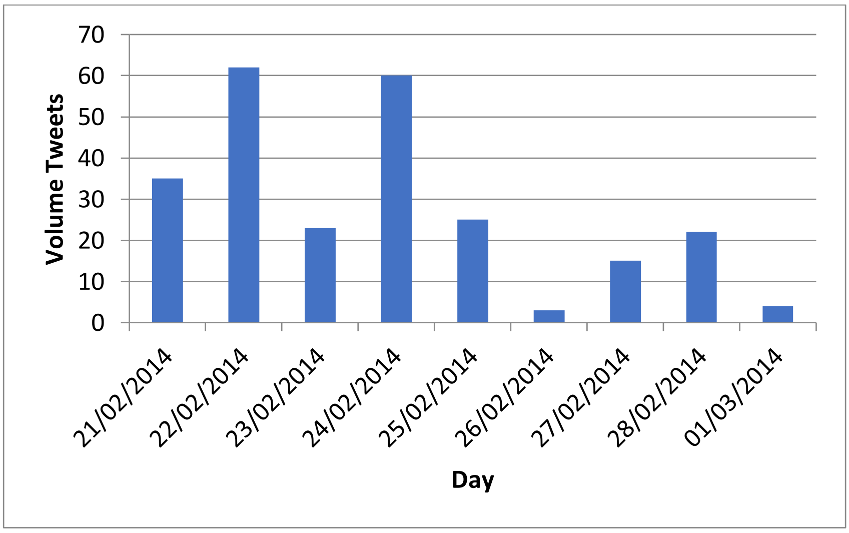
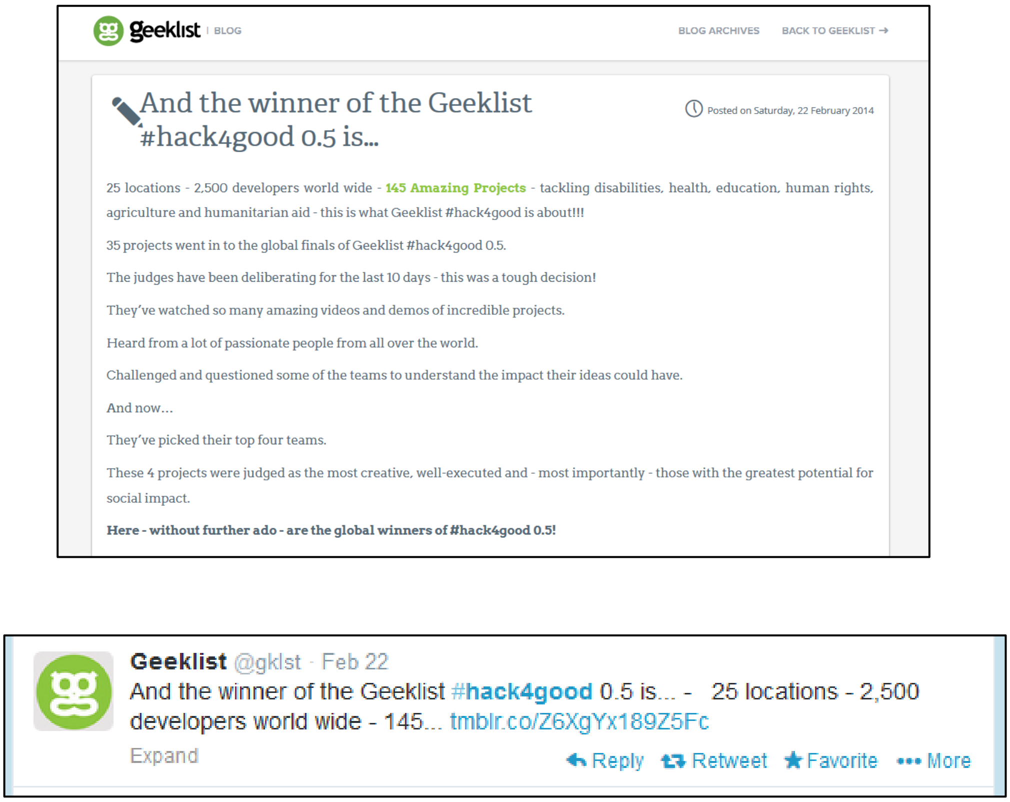


Figure 19 Volume of Tweets per Day Relating to #hack4good

The first peak day, 22nd February 2014, was the announcement of the winners of the Geeklist #hack4good event. The increased volume of tweets on this day all related to a website in which the event organisers made this announcement. This announcement was heavily retweeted by members (Fig.20).



And the winner of the Geeklist #hack4good 0.5 is...

Posted on Saturday, 22 February 2014

25 locations - 2,500 developers world wide - **145 Amazing Projects** - tackling disabilities, health, education, human rights, agriculture and humanitarian aid - this is what Geeklist #hack4good is about!!!

35 projects went in to the global finals of Geeklist #hack4good 0.5.

The judges have been deliberating for the last 10 days - this was a tough decision!

They've watched so many amazing videos and demos of incredible projects.

Heard from a lot of passionate people from all over the world.

Challenged and questioned some of the teams to understand the impact their ideas could have.

And now...

They've picked their top four teams.

These 4 projects were judged as the most creative, well-executed and - most importantly - those with the greatest potential for social impact.

Here - without further ado - are the global winners of #hack4good 0.5!

Geeklist @gklst · Feb 22
And the winner of the Geeklist #hack4good 0.5 is... - 25 locations - 2,500 developers world wide - 145... tmblr.co/Z6XgYx189Z5Fc

Figure 20 A 'Peak Day' #hack4good Tweet

The second peak day, 24th February 2014, comprised a number of tweets which related to the #hack4good. The tweets on 24/02/2014 can be classified into three main themes. The first set of tweets originated with organisations such as charities. They were generally links to websites and blogs and were heavily retweeted by other members in the event. The second set are related to a member who won the event which has been retweeted by other members. This is a tweet in which he thanks the organisers and members for their recognition. The remaining tweets are links to articles related to Civic Hacking and the posting of a hackathon project.

6.3 Discussion

6.3.1 Structure of the Group: Decentralisation and Semi-Autonomy

Based upon the findings described above, my first analytical consideration was that of the overall structure of the #hack4good Twitter network. This addressed my research question 'what types of communities are formed by Civic Hackers?'. In particular, I was interested in whether any thematic communities or divisions might emerge within this network which might contribute towards addressing my research aims. Below I will use social network data from #hack4good to triangulate findings from my previous research (Chapters 4 and 5) which suggested that these groups are relatively decentralised and semi-autonomous. I will also explore these findings in relation to previous theoretical frameworks of hacker communities (Chapter 2).

By social network analysis, the #hack4good network was comprised of several hubs of network members centred on the event organisers. These hubs were heavily connected to a number of inbound 'spokes' from members, who were themselves quite disconnected. Such inward spokes were created as the hackathon event organisers were mentioned, replied to or retweeted. However, a number of separate, smaller groups did appear which were quite well connected internally.

The #hack4good network would aligned with the 'Broadcast Network' model based on the definition provided in Section 3.2. In the hack4good network, the actor @gklst featured frequently as a hub with a large number of incoming ties, unsurprisingly since it was the Twitter page for the organisation, Geeklist, who were hosting the event.

I chose to exclude this as a 'false positive' as it may have skewed the data when I studied the event members in terms of factors such as their motivations. However, with the intention of analysing the overall network structure, it is still worth some consideration at this stage. Within this Twitter network, the prominence of the event organiser initially suggested quite a centralised structure, which differs from existing notions of hacker groups as *decentralised*.

One possible explanation for this might be that these corporately-sponsored Civic Hacking events do not really represent a type of hacking in its true sense but that the sponsors were re-appropriating hacker culture as a means to gain legitimacy (Section 2.2.2). Therefore, it might be argued that they do not truly represent a dispersal of the Hacker Ethics into wider society.

On the other hand, the apparently centralised structure may have had more to do with the inherent ways in which Twitter groups are structured. It was possible that the way in which this Twitter network was constructed tended towards centralisation since it was primarily used by the hackathon organisers to promote the event.

The event organisers did not seem to engage with their followers to a significant extent. For example, as described above, the majority of ties originated with the event organisers. However, these were not usually directed at the members themselves and there was little direct interaction with them. The event organisers rarely tweeted with the intention of directing or managing the members in any way. Instead, actors formed clusters and communicated between themselves, often displaying spontaneous discussion outside the official forums. Frequently, I noticed that these discussions were focused around key individuals who acted as 'teachers', offering advice and information (discussed further below). The event organiser's role was not seen as an 'organiser' as such, rather this was delegated and decentralised to various members of the group. There was a sense that members were 'in it together', that they had a shared sense of common purpose and were tied together by an interest in hacking rather than by any central authority. This interaction with a community of shared interest was a common feature of such events. Themes of participation, interaction and team work were common themes among my respondents. As one person told me:

> *"…It is a great opportunity to meet new and like-minded people and contribute to the community…" [Hack4good 2014 Member]*

This lack of centralised authority, even a mild sense of anti-authoritarianism, was also a key feature of the RHoK event I explored previously (Chapter 5). In the case of RHoK, the events passed by with relatively little interference from RHoK itself or even, to some extent, the local organisers. Teams formed and carried out their tasks in a semi-autonomous manner and often worked outside the officially suggested boundaries and structures of the day. I also noted a certain degree of distrust about the official event organisers in some of the narratives of members. For example, on several occasions, people described how the official forums and Skype links did not work properly. It was apparent that groups often preferred to use their own methods and forums. This seemed interesting given an event which is focused on creating local, appropriate technological responses rather than centrally imposed ones. Similar features can be observed in the #hack4good twitter network, in which members often found their own ways of working, outside the official channels. In fact, I noticed that discussions which started on the #hack4good network often migrated in quite a spontaneous way, eventually being continued within the Twitter feed of an individual.

This may be indicative of a decentralised and semi-autonomous group as has been described in other hacker communities and events (Section 3.1.2). The spontaneous Twitter discussions which took place outside the official #hack4good channel were in some ways reminiscent of the ‘Birds of Feathers’ gatherings described at hacker conferences, and which are now a common feature of more mainstream conferences. In fact, it is relatively common for such Twitter discussions to run parallel to these real-world events.

It was interesting to note that online, as in real world hackathons, members were sceptical of centralised authority. It was possible that these members were conscious, if not openly critical of, what could be viewed as the appropriation of hacker culture by big business and charity. Although there was a level of awareness that this sponsorship may be a necessity it did not seem to be something which they actively engaged with based upon my findings.

6.3.2 Types of Ties: Sharing, Support, and 'hobbyism'

I next began to explore the various types of ties within the hack4good network in terms of their direction (the flow of activity) and the values assigned to their content in order to address the research question regarding type of community this network reflected and the extent to which a shared set of Hacker Ethics, as described in Chapter 2, played a role in this. Although Social Network Analysis provided me with a starting point from which to highlight particular ties, I was most concerned with the 'thicker' qualitative detail based upon interviews and observation which could make sense of these ties.

Outbound connections were dominant within the #hack4good Twitter network, with almost 40% of actors having no inward connections. These can be attributed to a relatively small number of actors including the event organiser. During this period, 20% of inbound tweets were directed towards the Twitter page of the main event organiser, @gklst, and the rest were connecting towards individuals who had won the hackathon event as a form of kudos.

As discussed in Section 6.2, the inbound ties often took the form of congratulation and praise for winning the event and comprised of a kind of kudos. Outgoing ties for one highly scoring member, on the other hand, represented the act of thanking others for this kudos. This is indicative of a community in which success in these events, these tests of technical skill, are highly valued and rewarded. Interestingly, the peak temporal activity for tweets also centred on the announcement of event winners.

I also found evidence that this was a group in which quite a supportive spirit could be seen. As with the real world RHoK hackathon, people were valued and rewarded for choosing to use their spare time in this way. There was not a strong sense of competition between the different teams but rather a desire to help each other out and feel part of a community. It was not the 'competition' aspect of the event, imposed by the event organisers, which held significance for the members but rather being part of something. It provided them with a forum in which they could act out and perform, their *'lifeworld'* (Section 3.1.2).

It is interesting to note that all of my respondents described themselves as IT professionals of some sort, yet they were choosing to spend their spare time engaging in an activity which was not dissimilar to their 'work'. As with the members at the RHoK event, it was apparent that there was a lack of distinction between work and leisure time. Among this group there was a hobbyist aspect to the act of hacking and being part of a hacker group which drew people to spend their spare time engaging in an activity which was so close to their working lives. Many of those I interviewed explained this as resulting from their passion for technology, something which they acted out both in their profession and in their spare time whether through hackathons, blogs or communities:

> *"…I like organising events, love technology and networking with other technologists…" [Hack4good 2014 Member]*

This lack of distinction between work and leisure time has been described previously within hacker groups. As in the RHoK event (Chapter 5), the #hack4good network was a clear example of the abandonment of a work/leisure duality described in Section 2.2.2. It was also, I would argue, evidence for the 'hobbyism' described in other studies of hacker communities (Section 2.2.2) as motivations for taking part. This 'passion' in hacking as an activity seems to form an important part of such events and is significant to the communities involved. As I suggested in Chapter Four, these aspects of the Hacker Ethic may have had some influence upon working practices beyond the hacker community. The working practices of hackers may have been shaped by changes within the 'Network Society' (Section 2.3.2), but have also themselves shaped this society. Features such as informationalism, decentralisation and knowledge based working practices are all also central aspects of the Hacker Ethic. If hacking as an act is about working outside mainstream technological practices, it is also about subverting cultural frameworks. A central facet of the Hacker Ethic is the idea of finding better ways of working; not being constrained by rules and centralised structures. It should therefore not be surprising to find working practices within #hack4good following the same path.

The Betweeness ties, the bridges between different parts of this network, featured discussions of technology and science, themes which I have found across this community. Such discussions seem to hold a shared interest among the Civic Hackers involved in #hack4good. It is one of the commonalities around which these groups gather when they otherwise might come from different places, backgrounds and jobs.

From my observations and interviews within the group, the motivations of those taking part were primarily related to being part of a community focused around technology than 'doing social good':

> *"…..I chose to participate because of my passion for Technology…" [Hack4good 2014 Member]*

When asked about their motivations, the majority of my respondents placed most emphasis on their interest in technology, solving problems and engaging with a group of like-minded people rather than the humanitarian aspects of the event. When describing their involvement, members tended to focus on the technologies they created, on the methodologies they used and how they went about solving problems rather than the problems themselves. Members indicated that they could have been working on any project, regardless of its nature, and still have been motivated if given an interesting technical challenge and the opportunity to work with a group of people who shared their passion.

This is not to say that the humanitarian aspect was irrelevant. In fact, the majority of members stated that it was important to use their skills for good. From the members I spoke with, it did not seem to be their central motivation but rather acted as a kind of bonus. This may go some way to explaining the range of different projects which most of those involved had taken part in. These projects or problems are often set by organisers, charities or certain members of the event while members are content to lend their technological skill wherever it is needed, and to focus on the solution.

I also found that links to articles and discussion about the politics of such events were popular postings in the hack4good Twitter community. As with real world events, the members in this event were highly self-analytical regarding their community and the issues involved. They were in a constant state of discussion regarding the wider meaning of such events and what it meant to be involved. Interestingly, this has also been noted previously within other hacker groups (Section 2.2.2).

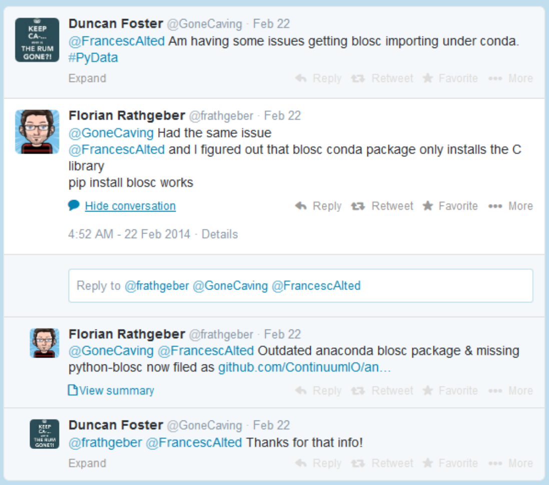
In terms of addressing my research question, I found that the ties identified among this network was reflective of the Hacker Ethics identified in Chapter 2 and that this was a group which reflected those shared ethics.

6.3.3 Seeking Advice and Teaching: Where does influence lie?

I next explored the extent to which influence within this network was reflective of the Hacker Ethics and to what extent this shaped the community which this group formed (see Chapter 2). When exploring who were the influential members of this online network, unsurprisingly the event organisers (such as @gklst) formed a central hub around which the external structure of the network formed. A large number of the tweets produced by members referred back to the event organisers in one way or another, placing them at the centre of connectivity, while, according to this data at least, members were relatively unconnected to each other. This initially implied a network which was formed around the official event organisers and in which they held a certain amount of influence. However, I found that the organisers did not generate a high volume of tweets themselves, and nor did they interact with members to a significant extent. Despite what was at first suggested by SNA, my interviews raised the idea that the event organisers were not necessarily the most important or influential members of this network. It became apparent that a range of different interactions were taking place which might not have been so easily detected. Again, Social Network Analysis provided a starting point, but many of these more subtle interactions became more apparent through interviews and observation.

As discussed above, a form of kudos was acquired by those who won the #hack4good event. The event organisers placed some emphasis on this and it was a popular topic for tweets in my Twitter sample. However, through my interviews and observations, I found that winning the ‘competition’ at #hack4good was not considered of central importance to the event, despite what first appeared to be the case. I also noted that the members saw themselves as relatively decentralised from the official organisers and often formed their own relationships and ties outside this network. This led me to question whether influence in the community was really derived from this kind of outwardly imposed ‘kudos’. The influential actors had something in common based on my Social Network Analysis. I found that several of the members who featured as influential within this network were all involved in tweets related to teaching, advising and sharing knowledge with other members. I therefore looked to explore further through interview and observation the ways in which members sought advice from certain network members, and how this ‘teaching’ was distributed. It is apparent that advice is sought from particular members of this network, however, in order to identify this there was a need to ‘go beyond’ this relatively limited hashtag network which serves a specific purpose. I changed my research focus towards areas outside the official #hack4good event Twitter feed where these kinds of interactions were taking place (see Section 3.4.4).

I selected the member @frathgeber for further discussion. As discussed previously, @frathgeber featured highly in terms of in-degree, or members referencing him in tweets, but was not an official organiser or sponsor. Interestingly, this member was also strongly linked to a number of the members from my RHoK fieldwork and played an important role in this community. Moving beyond the official #hack4good network, it became apparent from his other Twitter discussions that he was involved in advising and assisting other members of the Civic Hacker community with technical problems, as well as acting as an organiser and co-ordinator (Fig.21). It was clear from my observations of his interactions with other members of the group that this individual had a degree of influence and respect within this community which resulted from his willingness to help others and to share his knowledge. @frathgeber was involved in sharing code but also in sharing information. He was indicative of where power lay within a group which placed great importance on an open-source approach in every aspect.



Duncan Foster @GoneCaving · Feb 22
@FrancescAlted Am having some issues getting blosc importing under conda. #PyData

Florian Rathgeber @frathgeber · Feb 22
@GoneCaving Had the same issue
@FrancescAlted and I figured out that blosc conda package only installs the C library
pip install blosc works

4:52 AM - 22 Feb 2014 · Details

Reply to @frathgeber @GoneCaving @FrancescAlted

Florian Rathgeber @frathgeber · Feb 22
@GoneCaving @FrancescAlted Outdated anaconda blosc package & missing python-blosc now filed as github.com/ContinuumIO/an...

Duncan Foster @GoneCaving · Feb 22
@frathgeber @FrancescAlted Thanks for that info!

Figure 21 Tweets Relating to a Key Member, @frathgeber

Influence within this community came from a willingness to share with others. As code was shared in an open-source manner within the group, so was information and knowledge. This approach could also be seen in the interest of this community in open data. The Hacker Ethics were built into the fabric of these groups; they shaped how the group was structured and where influence existed. They shaped the way code was produced, but they also shaped the social *code* of those involved. In Chapter 4, Section 5.1.4 I argued that the sharing of power cables at the RHoK event could be seen as a metaphor for the fact that power and influence among this group was tied to the Hacker Ethics of sharing, openness and collaboration (Section 2.2.2). It was apparent that to be disconnected from this power within a Network Society based around informational networks was to be disengaged, and a core purpose of Civic Hacking is to give that engagement back (Section 2.3.2). Similarly, I would argue that these ethics were what made an individual such as @frathgeber so influential within this community. I have interviewed several members of this community whom I believe occupied a similar role. Individuals such as this volunteered a relatively large amount of time and effort to assisting other members of the community without appearing to receive anything immediate or obvious in return.

But I was also interested to know why individuals such as @frathgeber chose to help others. What they got out of it and whether it was for some kind of kudos or an expectation of future reciprocation, which has been described as 'the gift' (Section 2.2.2). It was clear from my interviews that a primary motivation for taking part in these events was an altruistic passion, joy and interest for hacking itself rather than any promise of reciprocal reward. But those who went further and assisted others, such as @frathgeber, gained a degree of reputation within this group in return for their willingness to help others. @frathgeber was also an interesting member of this group since he definitively described himself as a hacker.

He described to me his motivations for helping others with technical problems:

> *"...I think this is an integral part of the open source software development culture and it's only fair that I contribute my share to it. For projects that I develop or maintain, any form of user feedback is vital for finding and fixing bugs, missing or unclear documentation etc. As a user of other projects I'm trying to provide this exact feedback to the developers and maintainers...."*

@frathgeber explained that he took an open-source approach to sharing knowledge and helping others:

> *"...This is certainly what I'm trying to do. It's very much the case that you get out what you put in and knowledge shared is so much more valuable than it being only in my head. Sharing is also an incentive to formulate and articulate more clearly, which ultimately helps to better understand and remember things yourself....."*

Discussing what motivated him to be involved in the Civic Hacker movement generally, he provided some insight into this:

> *"...One motivation is the realisation that there is such great potential to use technology to help make the world a little bit better and with experience comes the*

> *responsibility to use it in that capacity I think. Another motivation is all the positive response and excitement we get in return for this work and of course the feeling of achievement....."*

This was evidence for the fact that certain members of this group were indeed motivated by the perceived value placed upon collaboration and free information sharing. These are core aspects of the Hacker Ethic and therefore suggests that these ethics were a fundamental part of this group. I also found that the network emphasised ideas of democratisation through its open and sharing nature.

6.3.4 A Community of Ethics

One of my research questions was to explore what type of community might best be used to describe the #hack4good network. There have been a number of previous attempts to model the various types of online communities, and even open-source hacker communities specifically. However, few of these studies are evidenced by first-hand empirical data (Section 3.1.3). An aim of my research has therefore been to test these theories against my data.

As discussed in Section 2.2.2, hacker communities have been described through a variety of theoretical frameworks including 'gift societies', 'virtual communities', 'Imagined Communities' 'Communities of Interest', 'Communities of Knowledge' and 'Communities of Practice'. In terms of overall concept, a virtual or imagined community seems relevant to the #hack4good network. It is a community in which members have often never met in person and transcend physical boundaries. It is also a group of individuals who are drawn together by a common set of shared interests. In particular, the concept of Communities of Interest seems appropriate since I have demonstrated that shared interests in technology and the Hacker Ethics are what ties together members of this group.

However, while the theoretical frameworks noted above may be generally applicable to online communities, they are not specific to hacker communities online. They do not explain what makes them 'hacker' communities *specifically,* whether a shared interest in the Hacker Ethics, the culture of hacking, as well as hacking as a practice. I was interested to explore what kind of community #hack4good was in order to explore what motivated those taking part and what values were at their core. What was the social glue that bonded this community together? Joy, reputational kudos, sharing, teaching? The ties within the #hack4good Twitter network provided me with some understanding of what that glue might be. I hoped that this would also allow me to understand the wider Civic Hacker community.

There were certainly indications that the #hack4good network was a community held together by a set of shared interests. An interest in technology was at the centre of people's motivations for taking part. It also seemed to be an important part of drawing the members of this network together. It was a commonality which meant that, regardless of other perceived differences, members did feel some sense of shared purpose with the rest of the group. This was evidenced through the strong feeling among those whom I observed that a primary motivation for taking part was a desire to be part of a community of people with shared interests.

The members in #hack4good fit the 'Community of Interest' model (Section 2.2.2) in that they were hobbyists rather than practitioners. On the other hand, all of them were professional IT practitioners whose day to day work was closely aligned, at least in practical terms, to the activities which took place at the hackathon. There was also a clear lack of perceived distinction between work times and leisure time. However, they were generally used to 'working' in quite a different manner, in a more corporate way, rather than hacking. Events such as hack4good may have allowed them the opportunity to 'do IT' in a different way and to express the Hacker Ethics through these working practices.

I also found evidence that the #hack4good network displayed aspects of a 'Gift Society' of sorts (Section 2.2.2). It was a community in which information, whether code or advice, was freely shared and where reputation (and indeed influence) was gained through this sharing. It was also an example of the gift as a symbolic embodiment of the values of that community. This was an example of hacker events as an expression of hacker '*lifeworld*' (Section 2.2.2). By exchanging these 'gifts', members of the #hack4good network were expressing a symbol of their Hacker Ethics. As noted in Chapter Four, it was apparent that the technologies produced by such events were also symbolic embodiments of their ethics – that the Hacker Ethics were expressed through the code that they produced.

The members of this group did exhibit features of the Hacker Ethics described elsewhere (see Section 2.2.2). This was apparent in their emphasis of collaboration and decentralisation from official authority as evidenced through interviews, SNA and observations. This set of shared ethics and values seemed to be part of what held the community together. This led me to consider whether this might best be described as a 'community of ethics'. A community held together by a shared set of ethics, namely the Hacker Ethics described above.

From this perspective, one can see how it might be possible to position the #hack4good network, and the wider Civic Hacker community, as a 'Community of Interest' (Section 2.2.2). This is because, according to my data analysis, the community did not have a strongly unified intention but rather a set of shared interests, and would also not generally be described as 'highly cohesive' since members had often not met in person and did not have strong ties. It might be argued that the Hacker Ethics were in fact this shared *interest* held by members of the #hack4good community.

Of course, in reality a community is often a combination of different models – it may be part 'Community of Interest' and part 'Community of Practice'. It is important to consider where the emphasis lies within that group; what is their core purpose. Civic Hackers are in fact more closely aligned to a 'Moral Community' (Section 2.2.2).

This might include such formally bound communities as medical doctors and academics, for example, the former being connected through the Hippocratic Oath and the latter through ethical guidelines, departmental or of a professional body. A religious group would be another example, being bound by formal sets of moral codes. On the other hand, communities bound together by ethical codes sometimes include those groups who adhere to a less defined and unwritten set of ethics. Examples of such groups include criminal groups (for example the concept of *omerta* among Mafia groups), amateur sports people such as mountaineers, skateboarders and surfers and subcultures such as graffiti artists. Communities who abide by these kinds of informal and unwritten codes tend to be amateurs and those outside the mainstream.

Civic Hackers also had this in common with these kinds of communities. Although my data suggested that the outwardly imposed ethics of the event organisers, sponsors and charities were not a primary motivating factor, the members very much adhered to a set of informal Hacker Ethics with regards to sharing of information and collaboration. This was evident through their relationships and activities with respect to both the #hack4good and RHoK events. The above findings therefore suggested that the #hack4good network could be described as a community which formed around the Hacker Ethics described in Section 2.2.2.

6.4 Summary

One of my research questions was to explore the types of communities formed by Civic Hackers. In particular, I was interested in the extent to which those communities involved in Civic Hacking are reflective of the Hacker Ethics described in Chapter 2. As noted above, I found that this group exhibited aspects which one would expect from a group of hackers. This was based on previous framings of hacker culture within the Hacker Ethics of collaboration, openness and decentralisation. To an extent, members of this group also self-identified with the term hacker although this was not a straightforward identity. As I found previously, the term is deemed a difficult one due to use misuse and those involved in hacking tend to resist such outwardly imposed labelling. While hacker is a term of respect they might endow upon others, most tended to prefer to describe themselves in terms of the activity, hacking, rather than hacker. I also found that this network placed emphasis upon the idea of democratisation through its open and sharing nature.

Having determined that this group did indeed conform to expectations of the Hacker Ethics, I was interested to investigate whether the #hack4good Twitter network comprises a community and, if so, what type. Through exploring various models which have previously been used to describe online communities, I considered how we might describe this community. My findings concluded that #hack4good comprised a 'community of ethics' in which the bond between members was a common emphasis upon Hacker Ethics such as sharing, openness, collaboration and decentralisation. In addition, the community was motivated much more by the social aspects of taking part, working with others or meeting new people, and saw these as the primary purpose of the event as much as an interest in technological hacking or 'doing social good'.

Within these Civic Hacking narratives, I also intended to test previous inferences of a dispersal of the Hacker Ethics into wider society. In reality, this was probably too small a sample to form any wider inferences about whether the Hacker Ethics have influenced wider societal change. I would suggest, however, these events in themselves are indicative of a wider trend in which the ethics and culture associated with hacking is being appropriated within a number of fields beyond what would traditionally be described as hacking in its purest sense i.e. technological modification. I also explored whether the event organisers in this case, mainstream charities and IT corporations, are involved in appropriation of hacker culture in order to gain some legitimacy. There was not strong evidence from members that they felt this was the case or that this event represented merely the appropriation of hacker culture by official organisers or sponsors in an attempt to gain legitimacy. Instead, my research indicated that there was more of an unconscious anti-authoritarianism in which members largely ignored much of the centralised, official organisation in favour of 'doing their own thing'.

It is interesting to note that the #hack4good data did triangulate with my previous findings carried out in real world settings such as interviews and event participant observation (Chapters 4 and 5). For example, I was able to identify a semi-autonomous, decentralised group who sought to distance themselves from the official authority of organisers. I also found a sharing and collaborative group with an open-source approach not just to software but to their overall 'lifeworld'. They also seemed to be hobbyists, held together by a shared interest in technology and not primarily motivated by the 'social good'. There was a clear lack of distinction between work and leisure time.

Having analysed a specific group of Civic Hackers, I next sought to explore some of the wider narratives which could be identified through online multiple sources. By doing so, I hoped to build upon these findings and address research gaps regarding the extent to which Civic Hackers express a democratisation of technology and whether Civic Hacking is indicative of a proliferation of the Hacker Ethics into wider areas of society.

Chapter 7

Telling Stories of Good Hacks: Online Narratives of Civic Hacking

7.1. Introduction

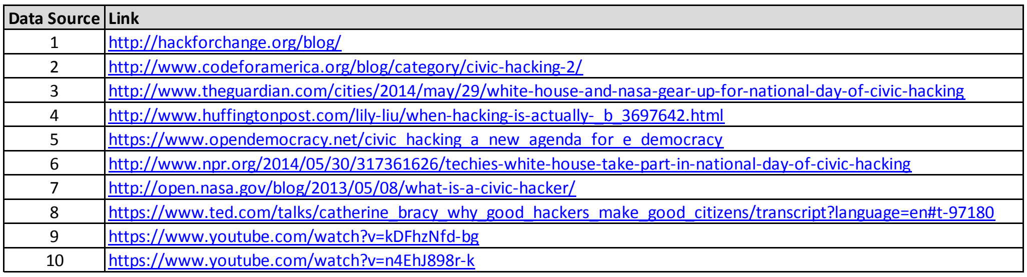
By 2014, when the #hack4good event took place, the term Civic Hacker had entered the online vocabulary. This fact signalled a change over the course of my research project (Section 2.3.4). When I started the project in 2010, groups involved in hacking for social good were rarely known outside their own communities and, where they were, tended to be linked to the wider ICT4D movement. Certainly, outside its own participants there was no recognised term Civic Hacking.

7.1.1 Research Aims

Within this chapter, and in line with my overall research questions, I intended to identify the commonly used themes and structures within the narratives produced by Civic Hackers online, to answer the research questions 'to what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?' and 'to what extent are Civic Hackers indicative of the proliferation of the Hacker Ethics into wider areas of society?'.

7.2. Research Findings

I will provide some description and context of these data sources and the main findings for each one in terms of narrative themes. The 10 data sources were:



Data Source	Link
1	http://hackforchange.org/blog/
2	http://www.codeforamerica.org/blog/category/civic-hacking-2/
3	http://www.theguardian.com/cities/2014/may/29/white-house-and-nasa-gear-up-for-national-day-of-civic-hacking
4	http://www.huffingtonpost.com/lily-liu/when-hacking-is-actually-_b_3697642.html
5	https://www.opendemocracy.net/civic_hacking_a_new_agenda_for_e_democracy
6	http://www.npr.org/2014/05/30/317361626/techies-white-house-take-part-in-national-day-of-civic-hacking
7	http://open.nasa.gov/blog/2013/05/08/what-is-a-civic-hacker/
8	https://www.ted.com/talks/catherine_bracy_why_good_hackers_make_good_citizens/transcript?language=en#t-97180
9	https://www.youtube.com/watch?v=kDFhzNfd-bg
10	https://www.youtube.com/watch?v=n4EhJ898r-k

Table 7. Data Sources Used for Civic Hacking Narrative Analysis

The selection process is described in Chapter 3, Section 3.4.5 (see also Appendix C). Based on this analysis;

- There were ten main narrative themes present in the data sources;
- These were all themes which I had previously identified among humanitarian hackers through interviews, hackathons or Twitter (link to chapters, sections);
- No data source contained all the themes;
- The themes were quite evenly dispersed across the websites with the exception of one (7.2.5);
- There was not a strong correlation between the type of data source (e.g. journalism, official sponsor) and the narratives found, although those which were described as journalistic articles tended to map much less

closely to the Hacker Ethics than sources produced by those directly involved in Civic Hacking;

- The most common theme was around collaboration, togetherness, commonality and sharing.

A graph visualising the themes in relation to these data sources is shown in Appendix A. I will provide some description and context of these data sources and the main findings for each one in terms of narrative themes;

7.2.1 Datasource #1: Hackforchange.org Blog

www.hackforchange.org/blog, last accessed 01/11/2016.

This source consisted of 46 posts between April 2014 and July 2014. Hackforchange.org is the official website for US-based National Day of Civic Hacking. These are regularly held international hackathons with the aim of solving local community problems. The events are co-ordinated by government and sponsored by Intel. Participants in these events work to create open-source tools, usually based upon open government data, for example an app called wasmycartowed.com which makes use of public data held by Chicago government and allows users to track their vehicle. Other examples are ‘Adopt a Siren’, an app which allows residents in tsunami zones to locate their local tsunami warning siren and volunteer to maintain it. My main research focus when analysing this website was the blog which is posted to by various individuals involved in the events, usually those involved in organising them. Although the content for this blog is provided by participants, it could also be viewed as an official media outlet since it is hosted, and presumably moderated to some degree, by the event organisers and sponsors.

I mapped the narrative themes within these posts against aspects of the Hacker Ethics which I had previously identified (Appendix A).

There was a close correlation between all of the previously identified Hacker Ethics and the narrative themes found on this blog. For example, the narrative themes described above, including collaboration and problem solving, could be directly mapped against Hacker Ethics.

- The most common narrative theme was focused around **finding solutions, the challenge of taking part and solving problems**. These narratives tended to describe the personal satisfaction which could be obtained from identifying a challenge or problem and then setting out to solve it through technical skill and Hacker Ethics such as collaboration. This narrative feature tended to form the beginning of the narrative structures described later. This was also indicative of one of the motivations for taking part which I have heard described by other parts of the Civic Hacking community (Chapters 4-6);
- The next most common narrative theme used in this series of blogs was **collaboration**, with a number of postings focusing on this topic. This tended to emphasise the importance of working together to solve the above described problems but also the enjoyment of hacking as a group. I have also found this narrative to be prevalent throughout the Civic Hacker community;

- After that, the most frequent narratives involved the idea that these events were **not just about technology**, a theme I also noted at the RHoK hackathon. These narratives took the form of attempts to involve non-tech participants, for example via an instructional video, and discussions of how the organisation teamed up with non-tech NGOs, government and other non-technological organisations;
- Closely linked to the themes of collaboration were narratives of **community** and also narratives of **contribution and participation**. Narratives of community emphasised the importance of a global network of participants with a set of shared interests and activities, often including the Hacker Ethics. Contribution and Participation tended to focus on the idea that hacking should not be a passive or theoretical activity but rather should involve 'hands-on' action.

Other themes also emerged, however, which although not strictly Hacker Ethics, were topics which I had noted within my previous research findings and which I have noted in other studies of hacking discussed in Section 2.2;

- Several discussions centred on open data and the promotion of an open-source ethic. One interesting aspect to this narrative theme was an attempt to link the democratisation of information to historical US philosophical and political ideals. This is similar to the ethnocentric notions described previously by authors when discussing the Hacker Ethic (Section 2.2). This is also despite the fact that the National Day of Civic Hacking is now an international event;

- The idea of the 'local vs the global' was also a common theme within this blog. These narratives described the ways in which local Civic Hacker projects, designed to deal with a specific issue, were then adopted more widely by the global community and applied to different geographical situations.

7.2.2 Datasource #2: Code for America Blog

http://www.codeforamerica.org/blog/category/civic-hacking-2, last accessed 01/11/2016.

This source consisted of 10 postings between May 2014 and October 2014. Code for America is a non-political organisation which was founded in 2009 with the aim of using open-source technology to solve local government issues. The organisation works through a number of channels; 'Brigades' of local participant hackers who regularly meet to build civic apps; a Fellowship programme which places developers into local government; an 'Accelerator' programme which provides funding and resources for start-ups; a 'Peer Network' for innovators in local government; and 'Code for All', which is a project intended to scale the programme internationally.

'Code for America' is a play on the term 'Teach for America' which is a non-profit organisation established in the 1980s to encourage top graduates to teach within low-income communities for short periods. This was later emulated in the UK through the 'Teach First' scheme. Interestingly, one of the early sponsors of this programme was Tim O'Reilly, an open-source evangelist and one of the 'creators' of the hackathon.

The list below shows the various narrative themes, many of which mapped broadly against the Hacker Ethics (see Appendix A).

- There were a number of mentions within the Code for America blog which emphasised the theme of **community**. These emphasised the importance of participants being part of a community, at both a local and global level. Participants were encouraged to form local 'brigades' which were then linked to a global community of similar groups. These narratives also discussed the importance of engaging with the wider community in the sense of government and residents;
- Narratives of **contribution** also featured within this blog. In particular, as described in the previous blog, the idea of action over words was emphasised. This theme was central to many of these blogs;
- The Hacker Ethic of inclusivity could be seen in the use of narrative theme that Civic Hacking is **not just about technology** and should involve those with non-technological skills;
- Finally, the narrative theme of **collaboration** was also present in 6 other sources described in this chapter.

A number of other narrative themes were also significant within this blog;

- Relationships with government, which tended to involve the idea that government did not always serve citizens due to a combination of poor technologies and undemocratic ways of working, and that Civic Hackers could provide a solution to this;

- The importance of conferences and events was often emphasised as being central to the Civic Hacking community;
- Again, as discussed in Section 7.2.1, the importance of the Local vs Global issues and the interrelationship between the two was often mentioned.

As with 4 of these 10 data sources, the Code for America blog incorporated aspects of US liberalism in its narratives. It made use of phrases such as "for the people, by the people" and linked these narratives to open-source ethics and hacker culture. There was not, however, inclusion of narratives from participants in their 'global events' outside the US and it would be interesting to know whether the narrative themes of these non-US individuals differed from those of US participants.

7.2.3 Datasource #3: Guardian Online Article

http://www.theguardian.com/cities/2014/may/29/white-house-and-nasa-gear-up-for-national-day-of-civic-hacking, last accessed 19/08/2017.

Although this source is a work of journalism, written for a Guardian newspaper article, the author in this case appears to be a Civic Hacker himself and heavily involved in the community. So, while at first, it may be argued that this source is not truly reflective of Civic Hacker narratives, it is still worth including for consideration. It is also worth noting that most of the Civic Hacker blogs feature a certain degree of their own bias since they are published on official websites and written by event organisers.

The article includes some of the narrative themes already identified above;

- For example, it discussed the relationship between **local** projects and a wider global community;
- It also mentioned the idea that Civic Hacking was **not just about technology** and described a variety of non-technological aspects, involving "…going beyond technology and involving activists, entrepreneurs and creative thinkers from all areas of society…".

However, as can be seen (Appendix A), this source mapped much less closely to the Hacker Ethics than the sources previously analysed in this chapter. This should not be seen as surprising since this source was written by a journalist rather than someone involved directly in Civic Hacking. This article used terms which did not feature elsewhere on Civic Hacker blogs nor in my other research samples (Chapters 4-6), including "Citizen Power" and "Innovation".

The author of this article did not present any downsides or criticism of Civic Hacking in his narrative. The narrative was a fairly utopian one. This differed from the narratives of Civic Hackers themselves who presented some of the challenges involved in making hacking technologies and hackathon events work in practice within their online material. There was a framing of Civic Hackers as in contrast to the 'bad hackers' described elsewhere in the media; a portrayal of them as heroic. The article also drew on clichéd hacker narratives, describing hacker events as "tech and pizza extravaganzas".

As with the narratives I observed within the #hack4good network (Chapter 5), this Guardian article described various important factors of Civic Hacking which were not directly related to the official purpose of the hacker event but were more about socialising and being part of a community, including working with “like minded individuals”.

The article described the roots of Civic Hacking in relation to the open source movement and positioned the participants in these events as hero type characters who volunteer their time and skills selflessly for good causes. Civic Hackers love to tell stories about great projects and, in common with other narratives I have observed, this article described a number of examples of Civic Hacking projects. In terms of structure, these stories consisted of around a paragraph explaining the name of the project, where it was located geographically, what was done and the outcome. These stories tended to emphasise collaboration between ‘the state’ and the Civic Hackers. They were also able to use a hyperlink which directed the reader to the ‘full story’ should they wish to find out more. I also found a commonality between stories in their description of Civic Hacking in terms of technological metaphors. In this case, the article described open data as the “oil that lubricates Civic Hacking”. Finally, there was also a strong link made between Civic Hacking and North American political ideals. There was an emphasis that public data should be transparent, owned by and available to citizens, and that Civic Hacking is an empowering and liberating opportunity

7.2.4. Datasource #4: Huffington Post Online Article

http://www.huffingtonpost.com/lily-liu/when-hacking-is-actually-_b_3697642.html, last accessed 19/08/2017.

This source also represents an online news article and therefore must be considered within its context as a work of journalism. However, the author of this article was also involved in technology and civic engagement so I would describe them as involved in the Civic Hacking community. As with the Guardian article described in Section 7.2.3, the narrative themes included in this article did not closely map to the Hacker Ethics. Similarly, this should not be considered surprising given the purpose of the writer of this source.

- As the title suggested, the central narrative theme of this article focused on the idea of '**good vs bad**' hacking. The author asks, "...to many of us the concept of "Civic Hacking" may seem like an oxymoron, for how can the word "civic," defined by its associations with municipal government and citizen concerns, be linked to the activity of hacking?";
- It also discussed the fact that participation in these groups and events were **not limited to technologists** by "....bringing together developers, designers, artists, urban planners and interested citizens.... residents and activists with no coding experience were able to submit their ideas as well.".

Again, as with the Guardian article, this source featured no negative discussion or critique of Civic Hacking. It suggested that Civic Hacking is a wholly 'good' form of hacking which can be separated from the negative forms of this activity. By attempting to position itself in opposition to these more traditional representations of hacking within the mainstream media, this source produced just another binary and inaccurate narrative of hacking.

The Huffington Post article told stories about Civic Hacking projects which took the form of setting the geographical location, the problem to be solved, and describing how the hackers went about finding solutions to this problem. Within this narrative, 'the state' was positioned as slow or ineffective and in need of help by the 'hero' hackers who were agile, collaborative and technologically skilled. The positive outcomes were described without any discussion of the complexities or problems involved.

Particular, local projects were also linked to other similar Civic Hacking projects happening throughout the USA and were thus contextualised within a much larger network or community of Civic Hacking. As found elsewhere within research into hacking (Chapter 2), these projects were both overtly and subtly linked to North American political ideals through descriptions of 'citizens' influencing government by using open data and collective action.

7.2.5. Datasource #5: Opendemocracy.net Website

https://www.opendemocracy.net/civic_hacking_a_new_agenda_for_e_democracy, last accessed 19/08/2017.

This website was interesting to me because it represented the earliest example I found of the use of the term Civic Hacking, being used in 2007. The author of this article was a journalist and a member of a US government think-tank but there was no indication of them being directly involved in Civic Hacking. It was also interesting to me in that it was the only media source I identified which made any critique of Civic Hacking. The article was set in the context of the UK's 'New Labour' government.

As the table at Appendix A shows, this article did not map at all against any of the Hacker Ethics identified in Chapter 2 (Section 2.2.2).

The main narrative theme of this blog was the relationship between Civic Hacking and democracy. It describes how the UK government suggested that the internet may be the answer to the problem of engaging young people. The article claimed that the government had misunderstood the real usefulness of the internet in this respect and that technology doesn't allow the means to collaborate with many people but rather provides "hip" electronic ways of engaging with the population. However, the article did then state that Civic Hacking had a significant role to play in engaging young people in politics and suggested that the government should provide funding to hackers to develop an "equivalent of Napster for government".

This article was produced prior to Civic Hacking becoming a self-aware and recognised movement. It provided a quite different view from my other data sources used in this chapter and did not reflect the same themes which I have found within them. The article was one of the few sources I selected not produced by a US organiser and so did not have a US focus in terms of political ideals and philosophy. The author was not directly involved in the Civic Hacking movement and did not follow the same narrative devices or structure as my other sources. For example, the article did not narrate stories about Civic Hacking projects. From this point of view, this article provided a useful insight into the narratives used by non-Civic Hackers to describe Civic Hacking.

7.2.6. Datasource #6: Npr.org Online Article

http://www.npr.org/2014/05/30/317361626/techies-white-house-take-part-in-national-day-of-civic-hacking, last accessed 19/08/2017.

This source was an online news article focusing on the National Day of Civic Hacking which took place in the US during May 2014. There was no indication as to the author of this blog although npr.org is an online news channel. The article was constructed from an interview carried out with an organiser of Civic Hacking events and his responses to a range of questions.

The following narratives were commonly used which map directly to several of the Hacker Ethics (Appendix A).

- **Collaboration** was a frequently discussed theme within the answers given by the respondent in this article. It was presented as a positive and important part of Civic Hacking by the author;

- The responses to interview questions described the enjoyment of **solving problems, coming up with solutions and challenges** of a technical nature;
- Descriptions of '**good vs bad**' hacking

In addition, the following narrative themes were used by the individual being interviewed within this article;

- The importance of open data, from both a practical point of view and as a philosophical concept linked to US democratic ideals;
- An emphasis on physical space and the geographical location within which this project took place. This was a recurring theme within these narratives;
- The importance of working together for the common good and sharing knowledge;
- The relationship between local and global hacking projects;
- There is also an aspect of pragmatism when discussing data access. At one point, the individual being interviewed states "of course it doesn't mean we should open up all data";
- The use of hacking as a non-technological description. For example, the interviewee uses the phrase "they hacked the day of hacking".

7.2.7. Datasource #7: NASA Blog

http://open.nasa.gov/blog/2013/05/08/what-is-a-civic-hacker, last accessed 19/08/2017.

This blog was from the NASA open data website and was created in relation to the National Day of Civic Hacking of which NASA was one of the main sponsors.

- This blog uses the theme of **collaboration** within narratives, in line with the Hacker Ethics;
- Themes within the narratives often involved the importance and pleasure of technological **challenges**. Again, this was in line with the Hacker Ethics identified previously;
- There was also mention of the fact that Civic Hacking is **not just about technology** and should include *"…technologists, civil servants, designers, entrepreneurs, engineers – anybody……anyone can participate to collaboratively create, build, and invent new solutions using publicly-released data, code and technology. You don't have to be an expert in technology, but you do have to care about your neighborhood and community to participate."*.

There were also a number of other themes which featured which were not directly linked to the Hacker Ethics;

- The relationship between global and local hacker projects
- The distinction between 'good' and 'bad' hackers

This blog placed particular emphasis on the history of technology, specifically within North America, and sought to position hackers in relation to World War Two. It used a historical narrative to demonstrate their view of Civic Hacking and is a story told by one participant in the National Day of Civic Hacking event which recounted their father’s experience in World War Two:

> *“Each night huge teams of mechanics would converge upon the wrecked planes and “hack” at them, removing the good parts from several and building a new plane over night from all the salvaged pieces. He told me they were referred to as the “hacker details.” That was because they had to use metal “hacksaws” as they cut away the damaged panels of the planes.”*

This interest in stories about the history of science and technology is a theme which I have identified frequently in previous interviews and observations among Civic Hackers (Chapter 5). There seemed to be a recurring desire to understand where Civic Hacking emerged from and to position it within a positive and relatively older history of technology, in contrast to previous framings as new or deviant (Section 2.2.3).

7.2.8. Datasource #8: TED Talk Video (Catherine Bracy)

https://www.ted.com/talks/catherine_bracy_why_good_hackers_make_good_citizens/transcript?language=en#t-97180, last accessed 19/08/2017.

This source was unique among my data sources in that it was an online video of a presentation made at a TED Talk event. The presenter was one of the organisers of Code for America, a Civic Hacking movement, and should therefore be considered a direct participant in Civic Hacking.

In this example, the narrator again began by describing a "team" last year in Honolulu. In this case, three people were asked by the government to rebuild a website. However, by collaborating, they determined that the website was too large and "clunky" so the task at hand would not be possible. Instead of following their government objective, they decided to build a new solution which was described as small and humble. It was designed for 'the people' and in addition to technological skill, they also instigated a form of 'crowed sourcing' to gather content through a "writathon". They used their skill, both technical and otherwise, to overcome this problem and created a new way for citizens to participate in government. The narrator then concluded with their local solution being adopted by another local group and repeated globally.

In this narrative, the presenter described how the government in Mexico City needed a new app to assist with tracking legislation. At the beginning, she stated that they were going to pay a huge amount of money to a corporation to build this for them. However, through collaboration on social media, Civic Hackers found out about this fact and expressed their anger at both the perceived waste of money and lack of civic engagement. They again used communities of open collaboration such as social media and issued a challenge to the wider group to devise a solution to this problem. The narrator showed how these developers expressed the Hacker Ethics to solve the problem and that was adopted much more widely.

The narrator described how Benjamin Franklin realised that the government of Philadelphia were not able to cope with fires and so formed the first fire brigade. This narrative contained a number of the previously identified themes including the idea that hacking is not just about technology, as well as a link to a US-centric history of technology and democratic ideals.

Many of the narrative themes which I have identified within other sources in this chapter are present within this talk which align with the Hacker Ethics (Section 2.2.2);

- The presenter described **problem solving** as a key aspect of Civic Hacking and presented a number of examples;
- An emphasis was placed upon **participation** with discussion of practical activity and action within various hacker projects rather than focusing on the theoretical aspects. From a purely empirical point of view, participation was the dominant narrative theme expressed within this ten-minute presentation, with five mentions;
- **Collaboration** was frequently used as the speaker focused on the importance of this ethic within Civic Hacker projects;
- **Inclusivity** was also stressed as an important factor with the speaker keen to embed the notion that Civic Hackers do not have to be computer programmers.

There were a number of other narrative themes within this source which did not align with the Hacker Ethics;

- This speaker begins her presentation with a discussion of 'Good vs Bad' hackers in an attempt to dispel popular framings of hackers;
- A central focus of the presentation was on the history of technology and innovation. This was described as amateur innovation on existing systems and these individuals were referred to a 'tinkerers';
- The discussions of these historical hackers were closely linked by the narrator to democratisation. There was a discussion of US patriotism and history with an emphasis on the idea that Civic Hackers were following in a long line of North American democracy activists. Democracy was strongly linked through these narratives to a set of North American ideals in a relatively ethnocentric manner;
- However, the presenter did also mention that Civic Hacking is not just a North American phenomenon and briefly referenced the fact that it was happening in other countries, such as Mexico;
- The idea of democracy was also closely linked by the presenter to the internet as an open and decentralised model.

7.2.9. Datasource #9: Sunlight Foundation Online Video

https://www.youtube.com/watch?v=kDFhzNfd-bg, last accessed 19/08/2017.

This source was an online video produced by The Sunlight Foundation, an organisation which describes itself as:

"...a nonpartisan non-profit that advocates for open government globally and uses technology to make government more accountable to all."

I identified the main narrative themes within this video as being;

- The importance of and joy which can be obtained through **solving problems**;
- The importance of **community** to Civic Hacking;
- A discussion of Civic Hacking in relation to **Good and Bad** hacking.

These are all closely related to the Hacker Ethics. In addition, there were also a number of other themes, many of which I had identified previously;

- An emphasis upon democracy, particularly in relation to data access. The idea that data and information should be openly available;
- The idea of practical interaction at this project and of being actively involved in making things.

7.2.10. Datasource #10: TED Talk Video (Jennifer Pahlka)

https://www.youtube.com/watch?v=n4EhJ898r-k, last accessed 19/08/2017.

The presenter of this TED Talk is one of the organisers of 'Code for America' and is therefore a participant and organiser of Civic Hacking events. The narrator set the scene as February in Boston with the city covered in large amounts of snow. One individual (the protagonist) noticed that citizens are shovelling snow on pavements but not uncovering fire hydrants. This individual did “what all good developers do” and created an application (‘app’) which allowed users to share and to track information regarding this. It was described as a small and modest invention, contrasted against the government (who we then assume to be the opposite of small and modest). This individual collaborated as a group and did something the government could not do by working in an open and democratic way, displaying their technological skill. The app went ‘viral’ when another Civic Hacker in Honolulu, again a lone protagonist contrasted against the state, used the same model. Again, they collaborated through the Hacker Ethics to create an app where residents could ‘adopt’ tsunami alarms to prevent people stealing their batteries. The narrator then went on to list other cities which used the same model. In each case, the government was described as slow, cumbersome while the hackers were “organic”, “frictionless” and “natural”. The presenter described the “problem” of government and used the term “we the people” to directly frame this activity within terms which a US centric audience would understand. The culmination of this narrative was that, through expressing these Hacker Ethics, the protagonists were able to solve the problem at hand and also contributed to much wider issues. It was also interesting that the narrator described things in metaphors of technology. She talked about the “machinery of government”, government as a “platform”, government as like the “internet”, “architect the system”, “fix government”.

- A central narrative in this presentation was that of **collaboration**. The presenter frequently told stories in which hackers worked together.
- **Participation** in terms of practical involvement in hacking was emphasised. The speaker summed up her presentation by asking "*are we just going to be a crowd of voices, or are we going to be a crowd of hands?*" This phrase is also closely linked to the to the pragmatic 'maker' aspect of hacking which emphasises action over theory;
- Civic Hacking was framed as forming a **Community** (or series of interlinked communities) which are essential to making these technologies work.

A number of narrative devices were also employed which were not directly related to the Hacker Ethics but which I have previously noted elsewhere among Civic Hackers (see Chapters 4-6);

- This source also relied heavily upon the narrative of North American libertarianism. For example, the presenter associated Civic Hackers with various North American historical figures or events which express democratic and libertarian ideals;
- The government was described as a 'platform' for helping others, 'platform' being an almost technical choice of phrase. In fact, more parallels were drawn between the machinery of state and technology as she argued that government should be "*more like the internet*".

7.3 Discussion

7.3.1 Narrative Structures

The Civic Hackers I focused on in this chapter enjoyed recounting stories about clever or imaginative hacking projects. They shared these as one of the main sources of content for blogs and websites. Below are common narrative structures which I identified within the sources I explored above. These went some way to addressing my research question 'to what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?'. The formats of narrative within these sources were similar to those I had noted among the RHoK hackathon (Chapter 5) and among the #hack4good Twitter network (Chapter 6). Below I set out a common structure which I have distilled from these narratives:

- A protagonist or small group, exemplified by a humbleness and different way of approaching situations;
- The protagonist(s) is contrasted against the state who are described as large, cumbersome and undemocratic;
- The protagonist(s) notice a problem and decide to solve it on their own terms. This problem can take the form of technological or non-technological issues but are usually confined to something locally bounded;

- The protagonist(s) share and collaborate and express a range of the Hacker Ethics in order to solve this problem;
- By doing this, they find a clever solution and solve the problem;
- This solution is then picked up by others and spreads to wider geographical areas.

The chart at Fig.22 shows some of the main themes within these narrative structures.

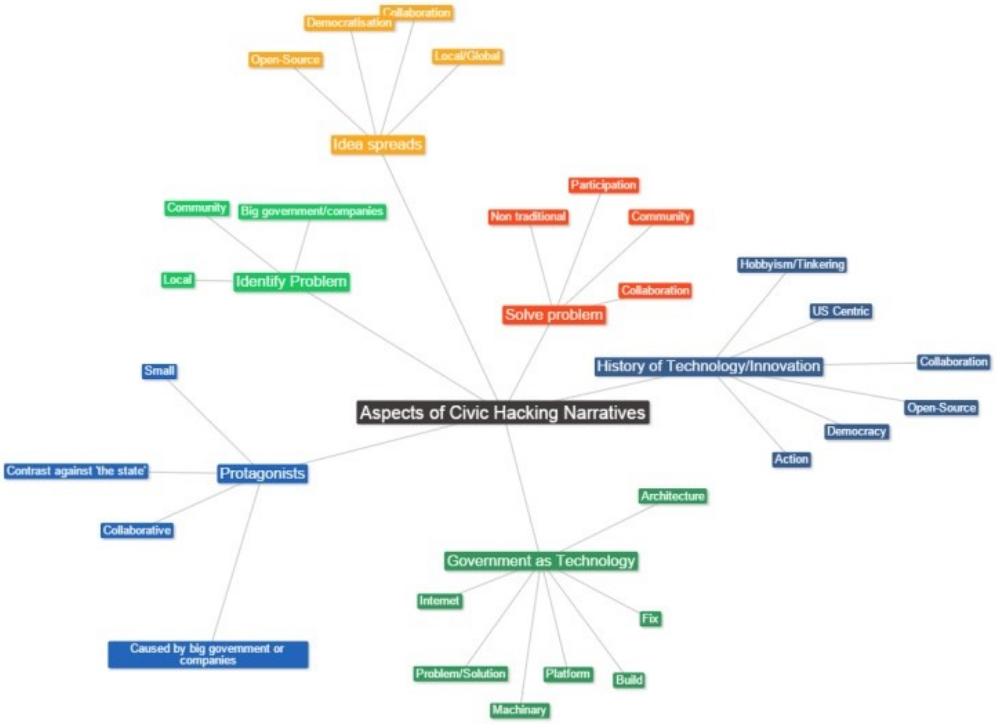


Figure 22 Civic Hacking Narrative Themes

The above findings suggested that the narratives told by Civic Hackers did express a positive attitude towards the democratisation of technology. The idea that information technology should be open and accessible to all was certainly presented as an ideal within these narratives. As with previous findings in

Chapters 4-6, this view on democratisation of technology is related to aspects of the Hacker Ethics identified in Section 2.2.2, which featured strongly within these narratives. This can be seen through the common themes within these narrative structures. An emphasis on the democratisation of information and technology was clear. This allowed me to conclude that the narratives told by these Civic Hackers did indeed express a democratisation of technology.

It is also possible, however, that the presence of these Hacker Ethics among Civic Hackers is evidence of the *appropriation* of hacker culture by the organisers of these events who tend to be relatively 'mainstream' corporate or governmental bodies. There is evidence to suggest that the appropriation of subculture is a commonly used tactic by these kinds of actors in order to gain some form of legitimacy (Section 2.2.3). One need only examine a handful of examples of conferences and articles to see how the term 'hacking', as well as hacker imagery and language, is now frequently applied in order to 'cash in on' the growing public interest in hacking (see Chapter 2). So, are these Civic Hackers narratives really 'hacker' narratives at all and how would we determine this? After all, the organisers and sponsors of these events and groups are relatively mainstream corporations and governmental organisations we would not typically associate with hacking. Should we judge their 'hackerness' based on their use of open-source technologies, their ethics, their self-identification as hackers?

In order to test this, I applied the identified Hacker Ethics to the narratives being expressed by these groups, and associated narratives, online. I concluded that there is a sense in which Civic Hacking is both indicative of the 'true' Hacker

Ethics *and also* appropriated hacker culture. The organisers and sponsors of these events are generally speaking not hackers, and there are certainly some groups and events who, although they may use the terminology and culture, are not involved in hacking in any sense. However, that does not categorically mean that those who participate in Civic Hacking do not possess the Hacker Ethics. In order to explore this further, I conducted comparative analysis against the narratives used by the media when discussing Civic Hacking.

7.3.2 Media Narratives

The external narratives used to describe these groups contrasted quite significantly with those used by the Civic Hacker participants themselves, despite the fact that the majority of these journalist narrators were themselves involved in Civic Hacking. The motivations behind these narratives led to a thematic differentiation. In general terms, the Hacker Ethics were not observed within these narratives, although they sometimes touched upon some of these themes. There was a clear emphasis upon the theme of Civic Hackers as 'good' contrasted against 'bad'. There was an implication that Civic Hackers can do no wrong and this is implicitly contrasted therefore against so-called bad hackers. In actuality, this is not how the Civic Hackers identify themselves within their own narratives. Although they do frequently use the theme of good vs bad, they use it in quite a different way from the news articles. During my previous interviews and observations (Chapters 4-6), I also found that Civic Hackers were keen to disassociate themselves with the idea of hackers as good or bad but rather saw it as an activity or set of social practices which were neither good nor bad. It did not form a significant part of their own identity, and was rarely discussed within these groups. Any such discussions tended to only occur when explaining their activities to outside observers.

Externally imposed media narratives also reveal an interesting set of themes. As explored within my literature review (Chapter 2), traditional portrayals of hackers, both within the media and academia, have framed them as deviant or heroic. It would appear that this 'binary' framing of hackers is supported in the case of Civic Hacking. Within the online media presentation of Civic Hacking, I found that the main narrative themes were almost the opposite of the traditional media/popular narrative of hackers as 'bad/criminal/deviant'. These narratives portrayed these Civic Hackers as almost heroically good, seeking to frame them in contrast with 'bad hackers'. Interestingly, these positive narratives might be viewed in the context of recent popular interest in 'heroic hackers' and 'hackers turned billionaires' (Section 2.2.2).

Although the Civic Hackers themselves sometimes made reference to this good/bad hacker binary, it was typically within a different context. As with the other groups I have observed, the association of hacking with something deviant or criminal within the popular imagination was ever present and inescapable. It was something which had to be confronted head on and dealt with, even if these Civic Hackers themselves did not associate with that narrative and often appeared bored by its constant re-emergence. Therefore, when it was mentioned, it was to clear up the subject 'once and for all', before moving on to discussing 'real' hacking or core issues. It was dealt with using the same 'hacker pragmatism' described in Chapter 2 (Section 2.3.2) which argues that hacking can not only be part of mainstream culture but should even influence it.

7.3.3 Discussion of Narrative Types

Broadly speaking, the types of narratives which emerged within these data sources were the same ones which I had identified in previous chapters. A number of the narrative types employed by Civic Hackers in their online sources correlated with those I had seen on the #hack4good Twitter network (Chapter 6) and at the RHoK hackathon in Southampton (Chapter 5).

The type of narrative most used was a description of a hacker project which took the form of a linear story involving protagonists (hackers), a problem which was identified and then an explanation of how they solved this problem through a combination of Hacker Ethics including collaboration, openness and participation as well as their technical skill.

In this way, these narratives can be viewed as clear expressions of the Hacker Ethics, particularly democratisation. Their narratives emphasise the fact that, by acting out the ethics of inclusivity, collaboration and openness, the participants were able not only to solve that particular technological problem but also to solve a local social issue and in doing so build a different, more ‘hacker’ type of government. One based upon these ethics. By hacking technology, they were also seen to be hacking government. Thus, these narratives emphasised the move from local to global and how a single, local hack could proliferate through an open network out into other similar projects.

Narrative Type #1: History of Technology and the USA

A significant number of the Civic Hacking narratives featured some link to the history of technology, and specifically to the relationship between technology and the democratic ideals of North America. For example, they frequently mentioned historical 'hackers' such as Benjamin Franklin and WW2 aircraft engineers in ways which associated this historical hacking with ideals of freedom and democracy. I also noted the use of this narrative theme among the RHoK participants I observed who frequently told stories about the history of science and technology.

I would argue that such narratives express a number of ideas associated with the Hacker Ethics. For example, they emphasise the idea that hacking is not a purely computer, or even technology, specific practice but rather a particular 'worldview'. They also tend to associate this 'historical hacking' with ethics such as openness and collaboration.

It was interesting to note that, despite being seen as such a contemporary group, those involved in Civic Hacking were quite concerned with situating themselves historically. For such a newly emerging group, narratives of this type expressed a desire to understand their identity and place in history. It was also possible that they are an attempt to legitimise, even justify, what might otherwise be considered a subversive act. It was clear that popular imagination had tied hacking closely to its criminal past, as framed by previous theory (Section 2.2.3). By linking themselves to positive and somewhat patriotic stories of heroes, at least within a US context, these Civic Hackers were attempting to portray themselves in contrast to these criminal hackers.

Narrative Type #2: Civic Hacker Narratives as Ethnocentric

As previously noted, studies of hackers have tended to focus on those within the North Atlantic therefore excluding other cultural viewpoints of this activity. Interestingly, despite the fact that Civic Hacking now takes place in a number of other countries outside of the North Atlantic, a fact emphasised by several of the above narratives, there were no online narratives encompassing such viewpoints. The narratives I observed, even when discussing the involvement of other regions, were almost exclusively from the point of view of North Americans.

This therefore makes for an ethnocentric description of Civic Hacking and must be taken into consideration when attempting to gain a fuller understanding of hacking as a whole. It is likely that different cultural, historical and political contexts would result in quite different ways of framing this activity. For example, while those in the US and northern Europe view Civic Hacking in terms of heroic libertarians from these regions, contrasting it against the deviant criminal hackers of the past, it is quite possible that those in other geographical locations might frame it in terms of, say, southern European political activism or state control over technology in North Africa (see Section 2.2).

At present there is not, however, the empirical data required to explore this further. An interesting area for future research would therefore be to study first-hand the narratives of Civic Hackers outside the North Atlantic.

Narrative Type #3: Narratives of Government as Technology

One of my research aims was to explore to extent to which the Hacker Ethics and also a democratisation of technology was expressed among Civic Hackers. While exploring online narratives of Civic Hacking, I observed a number of occasions where the government was referred to in terms of technology or computing. Within the above narratives, the government was referred to as "machinery", a "platform" and as like the "internet", while hackers were urged to "architect the system", "fix" and "build" government.

This was a new narrative device which I had not previously noted and I consider it to be significant for a number of reasons. These narratives reveal something about the worldview of the Civic Hackers, one which is informed by hacking as a technological activity and as a set of ethics. The ways in which they seek to understand government and to relate to it on their own terms could be seen as indicative of the worldview which underpins this group. By referring to government as a technology which can be hacked, I would argue that these groups are expressing the fact that they view hacking as something which goes beyond technology.

More widely, however, the term ‘hack’ has increasingly come to be used outside technology, typically when referring to ways of working more collaboratively, openly and innovatively in a non-mainstream way as described in Section 2.2.2. The format of the hackathon has also become commonplace, often replacing conferences within corporate environments as an apparently more collaborative and less structured way of working.

However, it would be difficult to argue that events and groups such as this should really be described as hacking or that their participants are, for the most part at least, hackers. Such factors should not be seen as indicators that hacking has proliferated into wider areas of society. It seems more likely that they are involved in appropriating the language and imagery of hacking in order to gain some form of legitimacy or ‘cool’ factor (Section 2.2.3). This is particularly likely given the current popular interest in computer hacking.

7.4 Summary

I set out to explore the narratives of those involved in Civic Hacking, the official organisers of Civic Hacking groups and events and also media interpretations of Civic Hacking. In particular, to explore the extent to which Civic Hackers value the democratisation of technology. I observed across these online sources to see whether there were any differences in the narrative themes expressed by participants compared with those of the organisers. Many of the same themes did occur across these sources, while I noted some difference in the media sources. Despite my interpretation of previous research at hackathon events (Chapter 5) and within a Twitter network (Chapter 6) which found a degree of conflict between the grass-roots participants in Civic Hacking and the official organisers and sponsors, there was not any overt acknowledgement of this issue within any of the Civic Hacking narratives I explored. This could be interpreted as due to the fact that the Civic Hacking digital sources were, generally speaking, either official channels or journalism. On the other hand, this finding might indicate that this conflict is not really present in any real sense.

I found that the journalistic media narratives of Civic Hacking are all quite positive in nature. In my view, they portray Civic Hacking in binary opposition to the stereotype of 'bad' or deviant hacking with the Civic Hackers cast as hero figures (Section 2.2.3). It was interesting to note that these media narratives did not tend to map against the Hacker Ethics, for which I found strong evidence within the narratives of Civic Hackers themselves. This is not surprising, however, it does also provide empirical evidence for the inference that these ethics are unique to those involved in this activity rather than any wider groups and builds upon my conceptual framework, hackathons (Chapter 5) and social media (Chapter 6) that external representations of hackers tend to differ from the ways in which they self-identify.

I examined whether the online narratives used by Civic Hackers indicate aspects of the Hacker Ethics and explored whether previous ethical themes identified in Chapters 4-6 can be identified within these online narratives. The narratives previously described did seem to be present within these online narratives and they were, in general, closely linked to the Hacker Ethics. For example, narrative themes frequently included an interest in technology, openness and sharing, anti-authoritarianism and the history of science and technology. In Chapter Eight, I will discuss whether the presence of these ethics represents an adoption of the Hacker Ethics in wider areas of society or, as indicated previously, whether the official sponsors/organisers have appropriated hacker culture in order to gain some form of legitimacy. Within this chapter, I did find some evidence for this within narratives of government.

At the beginning of this chapter, I identified the aims for researching online Civic Hacking narratives as exploring whether there is some focus on the democratisation of technology within the narratives of this community. This idea was identified within my conceptual framework as closely related to the Hacker Ethics. In exploring these themes, I addressed the wider research questions of my thesis, namely, is the emergence of Civic Hacking in any way indicative of the proliferation of Hacker Ethics into wider society beyond hacker culture. Or, rather, should they be interpreted instead as the appropriation of hacker culture by the official sponsors and organisers of these events. This will be discussed in more detail in Chapter 8.

Chapter 8

Conclusions

8.1 Introduction

At the beginning of this thesis, I presented the following research questions as the focus of my research into Civic Hacking which sought to build upon the conceptual framework described in Chapter 2;

1. What are the different types of groups involved in hacking for social good and how are they situated within the wider history of hacking as a culture and practice?
2. In what ways are the technological artefacts produced by Civic Hackers shaped by the ethics of these groups and wider social factors?
3. To what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?
4. To what extent are Civic Hackers indicative of the proliferation of the Hacker Ethic into wider areas of society?
5. What types of communities are formed by Civic Hacker groups?

In this chapter I discuss my overall findings in relation to these questions, to draw conclusions and demonstrate my contribution to existing work. I will also highlight the scope for future work in this area.

8.2 Defining Civic Hacking

The following discussion examines my first research question, 'What are the different types of groups involved in hacking for social good and how are they situated within the wider history of hacking as a culture and practice?'.

Through an analysis of the existing literature on hacking, my research project has contributed a definition of Civic Hacking which is situated within the wider history of hacking as a culture and practice. My literature review identified that at some point during the mid-1980s, the public in North America and Europe began to be aware of computer hacking as a practice and a culture. It was a time when the popular narratives of hacking were being formed which positioned it as dangerous, criminal and malicious. While the majority of people had no understanding of the practices involved, they saw what was presented to them in the form of destruction and anarchy. In the USA, law enforcement agencies presented hackers as a new threat to society and the media reinforced this through what would become stereotypical depictions of these 'villains'. Meanwhile, in film, literature and music, technology was becoming associated with the violence of a dystopian future in which angry, lone adolescents had all the power. I have shown that these portrayals of hacking, both in popular culture and academia, become quite simplistic and often do not reflected the true complexity of this practice or its practitioners.

From my research, I concluded that the development of this view of hacking coincided with the increasing importance of computing technology within society. It was also the same point at which computing technology had started to become intrinsically linked to the economy. The proliferation of personal computing into corporate North America and Europe meant that, not only the military, but business now also relied upon these technologies. Global stock markets were predicated upon computer infrastructure and companies had become hugely powerful. The public's everyday lives were also touched by personal technologies such as the Sony Walkman and calculators, video games and VHS. A new professional 'class' had emerged, with the IT entrepreneurs typified by Bill Gates and Steve Jobs, and for the first time, computing was starting to become networked. It is out of this social and economic context in which computers gained real and symbolic importance that the popular imaginings of hacking emerged. The view that is today still associated with hacking and hackers was formed during that period and is, I argue, indicative of the fact that, as computing became increasingly important to western societies, the perceived threat posed by hackers also increased. Since hackers had the ability to subvert computer systems, and therefore the power structures behind them, they became symbolically threatening to those in power. Yet, at the same time, advocates of hacking presented an almost utopian view of their activities and the potential for social change, largely driven by technological determinism. Neither of these framings seemed to represent the pragmatic and diverse reality of hacking.

But in order to provide a more accurate definition of hacking and to situate it within a wider context, I explained where the practice and culture of hacking emerged from. This occurred much earlier than the 1980s and reveals a more positive and, in fact, non-technologically specific, reality. It is accepted that the early computer labs of the Massachusetts Institute of Technology (MIT) during the 1950s were highly influential in the development of computer hacking as a notion (although the origins of the term itself are disputed). Within MIT, students were beginning to push the boundaries of this new technology through innovative workarounds and a type of working which emphasised collaboration, kudos and 'hobbyism' (Bender, 2011). This emerged alongside a culture of humour, elaborate pranks and anti-authoritarian rule breaking.

I demonstrate that hacking as a wider concept, however, could in fact be viewed as much older than this. The idea of technological innovation and rule-breaking carried out by amateurs working outside the boundaries of power structures has been in existence for some time, and these practices have frequently been presented as threatening by those in power. Examples of this can be seen in the early printing presses, used to democratise religious knowledge to the masses, or the work of amateur doctors prior to the formalisation of the profession during the 18th Century (Foucault, 2003).

Thus, from exploring the historical development of hacking within existing literature, I situate Civic Hacking within a wider set of activities which exist as both non-technologically specific practices and also as an associated culture. This practice and culture, however, almost exclusively emerged from the USA so it is perhaps unsurprising to find that it was influenced by this particular context. Most hacking is reflective of North American culture in its 'frontier narratives' (Healey, 1996) and places emphasis upon informational freedom (Coleman and Golub, 2008). Early in my research, however, I note that there are almost no studies of hacking in cultures outside the North Atlantic (North America and Northern Europe). My own research, while not overtly focused on hacking within specific cultures, engaged with a wide range of hackers who form a global community and therefore include a range of different backgrounds and world views. I find that, while Civic Hacking is a highly globalised community, it is still deeply informed by these original hacker influences from the North Atlantic. There is certainly clear opportunity for future research into hacking in countries outside this region and which have not been as strongly influenced by the USA.

My research also engages with hacking outside the North Atlantic in another less obvious way. Civic Hacking can be traced to an increase in technological innovation within the Global South. Often, this type of activity is not directly referred to as hacking, but I argue that it shares many features such as innovation, an open source approach, democratisation and collaboration. It would be almost impossible, and not particularly useful, to attempt to distinguish this hacking from that elsewhere since hacking appears to take place within such a globalised community. I find that hacking within Africa and Asia, for example, is highly intertwined with the practice in Europe or the USA, and that a degree of back and forth sharing takes place. However, I also found that hacking within the Global South regions does not appear to identify with traditional hacker culture to the same extent as in the North Atlantic.

In exploring the development of Civic Hacking during the 1990s, it became apparent to me that a relationship exists between hacking and the ICT4D (Information Communication Technology for Development) movement, a relationship which had not been identified previously. I identified a number of projects which brought together traditional humanitarian development with the open-source hacking community. Often, these groups were associated with new technological entrepreneurs and had some level of government support. Importantly, they associated with a number of hacking practices and with hacker culture. Various humanitarian and environmental disasters (the Haitian earthquake, Hurricane Katrina, Indian Ocean tsunami) also demonstrate the role which could be played by social media and mobile technologies in raising global awareness and support. Many of the most prominent ICT4D organisations result from African technology hubs, and in particular the rise of mobile technologies in Africa. There is a clear debate between corporate and governmental development policy makers on a global level and grassroots activists seeking to implement appropriate solutions. It is at the fault line between such approaches that Civic Hackers make both their practical and ideological interventions.

I have shown that this kind of 'hacking for good' is important since it can be situated within theories of Network Societies. Regardless of which way you choose to define it, modern society has been shaped by the dominance of informational networks. Within this type of society, the ability to control these informational networks brings a degree of power. Following on from my earlier point regarding the criminalisation of hackers, it makes sense from this perspective that governments during the 1980s might begin to fear those who could subvert and manipulate these networks. Conversely, I suggest that those without access to such networks are left powerless. The aim of those involved in ICT4D, and Civic Hacking, can therefore be viewed as an attempt to address these inequalities. This can be both a practical, pragmatic approach and also an ethical stance which closely resembles the Hacker Ethics described below.

Viewed in this way, therefore, Civic Hacking can be seen as a significant movement and an important research gap in terms of understanding hacking and its relationship to Network Society theory. If we accept that our society is based upon informational networks, then hackers should be seen as highly influential actors.

The importance of carrying out such an in-depth exploration of what hacking means, and tracing its origins, was that it allowed me to form a critical typology of hacking (and Civic Hacking in particular), one based upon a realistic view of hacking within context and based upon valid data. This then provided a basis for my research based upon the complex reality of hacking in contemporary life. This differs from previous studies of hacking which often begin with a number of assumptions about what hacking means and the characteristics of those involved.

8.3 The Hacker Ethics

This section addresses my third research question, ‘to what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?’.

A core aspect of my research built upon a concept referred to as the Hacker Ethic. The original MIT hackers were defined by a number of key ethics including sharing, openness, decentralisation, freedom of access to technology and world improvement. However, there are also a number of less easily defined ethics such as an approach towards work and 'hobbyism', anti-authoritarianism, practicality and a sense of community. Within my own research, these ethics provided me with a means to verify whether the Civic Hacking groups I was engaging with could be described as hackers and in what ways. I found that, for the most part, the Civic Hacking community does indeed adhere to these Hacker Ethics, as I will describe below. I had already identified a distinct lack of empirical research into the Hacker Ethics among wider groups so felt that this focus addressed a significant gap.

More recently, Kelty (2008) built on these ideas to suggest that the ethics of open source hacking have influenced practices within a range of other fields beyond computing. It is acknowledged that a fork had occurred between hackers who opposed mainstream IT and those who were more willing to embrace corporate IT and felt that open source could become a viable business model. In this way, the Hacker Ethics, and the wider practices and culture of hacking, have changed the nature of corporate business. For example, companies such as Microsoft and Apple were influenced by North American hacker communities, and open source technology is now the basis for a large part of the internet.

This argument had perhaps the most relevance to my own research and I was keen to develop this concept. I found that Civic Hacking is in fact indicative of the ways in which the Hacker Ethics, and hacking more generally, are influencing wider areas of society. It became apparent that many aspects of Civic Hacking might not be described as 'hacking' in the traditional sense of technological modification. In addition, those involved often did not overtly identify themselves with hacking or hacker culture. However, their ethics, as expressed through various practices, strongly align with the Hacker Ethics and I noted a number of similarities in terms of culture and approaches. From this relatively small 'slice', I was therefore able to form some wider interpretations about the ways in which the Hacker Ethics might be influencing areas beyond technology.

I refer to this concept as Hacker Ethics in the plural, since I argue that they in fact comprise a number of different, constantly shifting ideals. Rather than attempting to define these ethics as a static and inflexible set of rules, I looked at the ways in which Civic Hackers approached various situations and expressed these ethics through their practices. I found through my research that Civic Hackers clearly do exhibit the Hacker Ethics and, through my data analysis, I was able to evidence this argument. For example, by interpreting hacking narratives, events and artefacts, I identified aspects which are clearly expressions of these ethics.

I was initially surprised by the degree of socialisation among Civic Hackers, but with hindsight, perhaps I should not have been. After all, the Hacker Ethics are largely defined by interactions with others, and despite popular preconceptions of 'geeks' and hackers as working in isolation, in fact the opposite is the case. Civic Hackers are usually part of a wide network of interconnected groups both online and offline. For example, the RHoK event I attended was part of a global social movement and I found that many of the same actors moved between different groups. In all areas, I found Civic Hacking to be typified by collaboration and the importance of community, something which is expressed through both the narratives and artefacts crafted by this community. This is a clear manifestation of the Hacker Ethics.

Civic Hacker events and communities seem to take place in a semi-autonomous manner, which I have seen described among hackers elsewhere. Again, I witnessed the expression of a Hacker Ethic through this decentralisation and a mistrust of authority through their events. Yet Civic Hackers are able to galvanise quickly and effectively around a particular issue and often collaborate along with corporations and government when they choose to do so. There is a democratic aspect to their approach in choosing what problems to work on and in how they judge success.

I noted a lack of competition among Civic Hacker groups despite the apparently competitive nature of the events they participate in. Collaboration within a community is a central aspect of their practices and access to information is viewed as particularly important. I also saw frequent examples of a desire to help each other as well as address the wider problems they were trying to solve. Whether giving advice on Twitter or sharing internet connectivity at hackathons, collaboration is a key thread running through my research findings.

It was also interesting to observe a lack of distinction between leisure time and work time among Civic Hackers. There is a high degree of 'hobbyism' among Civic Hackers, many of whom have other professions and volunteer their time. This correlates with the work of Castells and Himanen who argue that Network Societies feature a shift in working practices away from formal, weekday jobs and towards a blurring between ‘hobbyism’ and the “Fridayisation of Sunday” (Himanen, 2001).

Interestingly, despite the fact that theories of the Hacker Ethic have been in existence for over thirty years, there is little in the way of empirical research to explore this. Part of my intention was therefore to use empirical data to test these theories. In doing so, I found that these theories are largely accurate. The ethics do appear to be present among the groups I was exploring. In addition, I also noted features such as approach towards work and community which align to these concepts. It was also clear that, despite some hackers who refuse to engage with mainstream ICT, those that I encountered are influencing wider areas of society beyond technology and changing the ways in which it is conducted. These findings represent an important contribution to the study of hacking as a social practice since they provide evidence for previously untested theories and appear to validate a number of them. This includes the ability to form some generalisation regarding the significance of hacking to wider society.

8.4 The Ethic of the Code

This section addresses my second research question, ‘In what ways are the technological artefacts produced by Civic Hackers shaped by the ethics of these groups and wider social factors?’

The social sciences have, for a long time, carried out analysis of objects as a method for gaining insight into the views of the groups that produce them. This has involved everything from the study of everyday objects (Turkle, 2007) to the anthropological interpretation of ethnographic artefacts, the masks, instruments and clothing of 'the other'. More recently, technologies have been interpreted in terms of the ways they are shaped by social and cultural factors. This interpretation acknowledges that society and technology are intertwined in a two-way relationship which shapes one and the other. This approach has been in part a response to technological determinism, which views technology as a driving force, shaping society while ignoring the impacts society has on technology.

I was interested in the kinds of technological artefacts which are produced by Civic Hackers and how they are shaped by the social context of these groups, as I knew that this had not been addressed before. In particular, I was keen to examine whether the Hacker Ethics I had identified are expressed through these artefacts. As a researcher, the study of the objects produced by these communities is one way of gaining an insight into the views and beliefs of those involved. In the case of my research, the artefacts my research subjects produced largely took the form of computer code. Despite its seemingly binary nature, this code has the ability to carry meaning beyond the practical. As Cox (2013) has argued, code can have a poetic, performative quality and can give voice to its author.

The technologies they produce, the end products, are the group's cultural artefacts. As well as being just practical tools, they are expressions of that group and its values. A particular technology may have a set of affordances which determines some of the ways in which it turns out, but they are also socially constructed. They are shaped, for example, by the collaborative nature of the group or an emphasis on decentralisation, the values which the members of that group hold close. There is a very clear process by which members of the group consciously select or are given the problem they are going to work on, and then go through a process of designing and developing their technology.

During my research, I deconstructed and examined the process by which Civic Hackers produce technological artefacts. I did this by shadowing particular groups and 'following' these objects throughout their lifecycle. This allowed me to identify various aspects of their creation which reveal something about the wider context in which they were constructed. The process of developing a technology begins long before any code is written or wires soldered. It involves a complex interaction between participants, technology and the wider community in which they interact. This is a creative, iterative and non-linear process in which the Hacker Ethics are expressed first in speech, then on paper and finally in code.

The code is an expression of the Hacker Ethics and so are the technologies these Civic Hackers produce. Their artefacts tend to be collaborative and decentralised in nature, similar to the processes by which they are made. There is a strong tendency towards simple, mobile applications which can be used in low income communities where access to expensive technology may not be available. Civic Hackers also frequently produce hardware hacks, re-appropriating and making use of cheap and available kit to build prototypes.

More recent creations tend to harness Web 2.0 technologies and social media to 'crowd source' from their audience. They are very much 'end user' driven (Von Hippel, 2005). Open data is a central feature of Civic Hacking and they always rely upon open-source software. Finally, I found that Civic Hacking emphasises a relationship between the global and the local in terms of problems and solutions. A technological solution might start small, attempting to solve a specific problem in a specific community, but they are frequently scaled up and applied to various global issues, often quite different in nature.

Hackathons in themselves proved to be insightful in terms of events in which Civic Hackers expressed their ethics and values, and had also not been the focus of previous research. Borrowing from previous studies of conferences, I found aspects in which they form an expression of hacker 'life world' (Coleman, 2010) and also act as spaces within which this relatively new community can come together and form its identity. Within this context, the technological artefacts are shaped by, and also themselves shape, what it means to be a Civic Hacker. Hackathons are, in this way, a performance of the Hacker Ethics and the act of producing a technology is an aspect of this performance.

I also found that these physical events are strongly tied to online space and that participants inhabit both the offline and online hackathon simultaneously. In this way, they are able to transcend geographical location as well as time zones. For example, there is a great deal of discussion taking place on social media platforms and chatrooms which helps shape the events and the technologies produced. Since the hackathon took place globally, there were a number of links to the events which were going on elsewhere including live video links. It was therefore important within my own research to ensure that I accurately captured this online interaction.

By focusing upon these events themselves, as situations in which this group expressed and shaped its values, I was able to gain insights into the relationship between Civic Hacking and the Hacker Ethics. As with my analysis of artefacts, these findings largely substantiate the idea that the Hacker Ethics described previously are central to this community. The ways in which the events themselves were organised, and the activity of those involved, provided numerous examples to support this. It was also interesting to note that 'hackathon' type events are increasingly becoming popular in fields beyond hacking and, as I will describe later, this suggests that Kelty's arguments about the influence of hacking in wider society may carry some weight.

8.5 A Community of Ethics

This section explores my findings with respect to my fifth research question, 'What types of communities are formed by Civic Hacker groups?'

It became clear during the early stages of my fieldwork that Civic Hackers produce some form of a community. I was dealing with a group of individuals who were drawn together by some commonality to attend events and take part in shared practices. It was also interesting to note that several of my informants featured in different Civic Hacker groups and referenced each other independently. I also found, however, that the boundaries of this community are not clearly defined by geography or demographics. Those involved often meet only online and are drawn from a range of quite different backgrounds. Therefore, one of my research objectives was to explore what kind of community this might be and what that reveals about Civic Hacking.

I approached this issue by first exploring some previous theories of communities with the aim of establishing whether any of these might be applicable to Civic Hackers. Understanding what it is that binds a community together can provide insights into what that group considers important and increases understanding of their practices. In particular, I was keen to establish what motivates Civic Hackers to take part in this practice. Is it, for example, primarily enjoyment of hacking or humanitarianism? There are a number of previous interpretations of hacker communities which are relatively untested in terms of first-hand data therefore this seemed to be a relatively novel area for research.

I gathered and analysed data by applying a combination of Social Network Analysis (SNA) from an online setting in which Civic Hacking interaction took place, a Twitter hashtag which surrounded a hackathon event. This allowed me to explore the types of links and themes which might reveal something of what it is that draws this community together. I was also able to validate my findings against offline data gathered through participant observation and interviews.

I noted a high degree of decentralisation and semi-autonomy within this group, something which has previously been observed among hackers. I was interested to know whether there might be any sense of conflict between the participants and event organisers. After all, the idea of a centralised organiser, particularly involving sponsorship by mainstream IT companies and government, seems at odds with the Hacker Ethics of decentralisation and anti-authoritarianism. Both in this setting and at the RHoK event, I did find evidence for such conflict and also that participants moved away from the official corporate websites and blogs in order to interact on their own terms. However, there was no indication of this conflict within the online narratives I examined.

I also noted that ties between participants emphasised sharing, support and a hobbyist approach. These features of the Hacker Ethics were frequently present and provided one form of commonality between members of the community. In terms of what endows influence upon members of the community, there was a focus upon the seeking of advice and teaching of other community members. Participants placed great value upon those within the group who had knowledge and were willing to share this knowledge.

The anthropological concept of 'Gift Societies' has been applied to hackers previously (Raymond, 2000b). Open-source hacking takes place within a community predicated upon sharing of code, data and information. I found that Civic Hacking does comprise some sort of 'gift community' in which the symbolic currencies which members value (code, but often also ideas or knowledge) are shared freely in the belief that it will be reciprocated by any member of the group in the future. However, I was not convinced that this is what differentiates Civic Hackers from other communities. My fieldwork indicated that there is something else central to this group which goes beyond just the sharing of code. After all, the participants could just take part in coding but instead they choose to focus their activity towards 'doing good'.

The group clearly comprises a type of 'Virtual Community' (Rheingold, 1993). The majority of participants do not meet in person but it appears that they must be bound together by *some* kind of commonality. They are to some extent engaged in a common set of practices, holding common interests and knowledge. However, these concepts do not seem to fully address what it is that holds them together. Rather, it was apparent that this community is highly heterogeneous in terms of the way it works, the motivations of those involved and their backgrounds. Even in terms of their activities within Civic Hacking, there is immense variety in their contribution. Some are professional software developers so they design projects, others with no technical skill organise the people involved or the events.

I concluded that the concept of 'Moral Community' (Moon, 1993) might be well suited to interpreting Civic Hacking. Unlike formally bound communities, medical doctors and academics, for example, who are connected by a set of rules imposed by an outward, central governing body, Civic Hackers appear to centre upon a loose adherence to a less defined and unwritten set of ethics which are self-governing. Communities who abide by these kinds of informal and unwritten codes tend to be amateurs and those outside the mainstream. These morals could be best defined as the Hacker Ethics which I had identified previously. The Hacker Ethics appear to be a common factor which brings together a range of different people to take part in quite different activities and who do not share a common location and have often never met in person.

8.6 What Stories do Civic Hackers Tell?

This section addresses my third research question, 'to what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?'.

The narratives which are told both *by* and *about* a group can reveal interesting insights into what they hold important and what motivates them. There has been almost no empirical research into hacker narratives and what exists tends to focus on external narratives, the media and state portrayals of criminal 'crackers' or 'geeks turned billionaires' (Alleyne, 2015). In contrast, there have been few studies of what stories hackers, or indeed Civic Hackers, *themselves* tell. This struck me as a significant research gap which could be addressed through my project and would contribute to the wider study of hacking within the Social Sciences.

I first encountered Civic Hacking narratives while interviewing subjects for my portraits of hacking. I found that these individuals tend to tell similar stories about what hacking means to them. While participating in the RHoK event, I decided to capture some of these narrative themes in more detail. This provided me with a basis to explore whether the same narrative themes can be found in online settings such as Twitter, blogs, websites and other sources and, if so, what they reveal about Civic Hacking as a practice and the community involved. Having identified a number of narrative themes, closely aligned to the Hacker Ethics, I was able to observe for these traits within the online narratives and use this to carry out further analysis.

I was able to identify clear examples of the Hacker Ethics within narratives of Civic Hacking in addition to a number of new themes and structures. For example, themes discussed elsewhere including inclusion, community and collaboration were present within the narrative content of blogs, websites and online videos produced by the Civic Hacking community. This was significant in that it demonstrates empirically that the Hacker Ethics exist within this group and suggests that these ethics are central to the narratives of Civic Hackers. This would appear to suggest that Civic Hackers have some relationship to the wider social practice of hacking.

There was a common structure to many of the Civic Hacker narratives I examined which generally involves a humble protagonist who is trying to do things differently. This protagonist is contrasted against the state which is viewed as large, cumbersome and undemocratic. The protagonist notices a local problem, technical or otherwise, and decides to solve it. The protagonist shares, collaborates and expresses a range of the Hacker Ethics in order to solve this problem. By doing this, they find a clever solution and solve the problem. This solution is then picked up by others and spreads to wider geographical areas. This finding was important since it revealed a commonality between Civic

Hacking narratives which are related through use of the Hacker Ethics as positive virtues. This demonstrates that these are viewed as important values to this group and therefore form a central part of their narratives.

I also noted some similar themes within online Civic Hacking narratives which I had observed during offline fieldwork. For example, Civic Hackers frequently discuss the history of technology, use USA centric analogies, and describe government as a form of technology. This allows me to validate those findings and gives credibility to the inference that these groups all form a wider Civic Hacking community. Examining these narrative themes also provided me with some insight into the values of Civic Hackers.

Within my literature review, I have identified the fact that media narratives of hackers often portray them in a negative context. They are typically cast as criminals and outlaws in contrast to mainstream society. I was therefore interested to explore the ways in which media-produced narratives of Civic Hacking differ from those produced by Civic Hackers themselves. I have been surprised to discover that the media narratives tend to depict Civic Hackers in an overly positive manner. Almost as a reaction to previous stereotyping of hackers, media narratives emphasise the virtuous acts carried out by Civic Hackers. I conclude that these narratives of 'good hackers' are just as inaccurate as those of 'bad hackers'. This still represents a binary framing of 'good vs bad' which is in fact seldom used by Civic Hackers when producing their own narratives of hacking. Identifying this disparity between external narratives of Civic Hacking has allowed me to situate Civic Hacking alongside wider representations of hackers in popular media and reveal something of the complex reality of these groups.

These external representations of Civic Hacking through narratives provided interesting insights into the extent to which the practices of this group can be described as hacking. I have addressed whether the 'hacking' in this case is merely the appropriation of this term by event organisers and sponsors. These organisers tended to be associated more with mainstream corporate IT, government or development than hacking, and their practices certainly did not appear to be expressions of the Hacker Ethics. Assuming that to be the case, as I will discuss later, I was interested to know whether these organisers were merely appropriating hacker culture in order to gain some form of legitimacy. Therefore, I aimed to establish whether there was any conflict between 'grass roots' participants, those practicing Civic Hacking, and organisers. This was something which had been indicated during my initial fieldwork. Within my Social Network Analysis of the #hack4good Twitter community and at the RHoK event, I did find evidence for this conflict. I was surprised to note, however, that this does not seem to be present within these online narratives. This could be interpreted as because the Civic Hacking digital sources are, generally speaking, either official channels or journalism. There is scope for future research to explore this issue further using a wider sample of online narratives.

Finally, I again noted that the online narratives of Civic Hackers within my study tended to be ethnocentric in nature. There was a clear emphasis upon USA focused narratives, including topics such as Benjamin Franklin, and mechanical 'hacking' during WW2. It would be interesting to analyse narratives which do not follow this pattern, however, I was unable to identify any narratives which were produced outside this cultural boundary. There is therefore scope for future research into narratives outside of the USA and Northern Europe. This also ties into a wider research gap into hacking as a practice outside the North Atlantic which I identified through my literature review.

8.7 Hacking is Going Viral: The Proliferation of Hacker Ethics into Wider Society

This section addresses my fourth research question, 'To what extent are Civic Hackers indicative of the proliferation of the Hacker Ethic into wider areas of society?' and also my third research question, 'to what extent do Civic Hackers express the Hacker Ethics and a democratisation of technologies?'.

One of my key research aims built upon Kelty's argument that hacking has influenced wider areas of society beyond technology, and that the ethics, culture and practices of hacking have informed fields such as art, science and academia. By exploring Civic Hacking, I hoped to address this question by discussing whether it is indicative of the proliferation of Hacker Ethics into wider society, and whether Civic Hacking is an example of the influence of computer hacking on existing humanitarian development. Through my research, I would conclude that there is a strong body of evidence to suggest that Civic Hacking does indeed represent the influence of hacking, and in particular the Hacker Ethics, on wider areas of society. These ethics can be found in many areas of this field, as can a number of the practices and cultural traits associated with hacking. This influence can be seen in the events held, artefacts produced, narratives told and ways of working which all appear to express the Hacker Ethics which developed from those involved in computer hacking.

As my research project developed, however, I began to consider whether computer hacking itself is perhaps also one early example of a wider societal shift. I questioned whether it is accurate to infer that computer hacking was the practice which was influencing this change. I would argue that it is not just that computer hacking has influenced society, but that computer hacking itself is indicative of a wider societal change. Other recent examples of social movements which I would argue correlate with the Hacker Ethics include alternative media; CrossFit, a fitness movement which might be described as 'open source'; the Clean Web which uses crowd sourced, open-source technology and culture to address climate change; and movements such as Arab Spring, Anonymous or Occupy which emphasise collaboration, informational freedom and democratisation. Rather than viewing these wider changes as technologically determined by computer hacking, instigated by the invention and influence of computing, perhaps it might be better to view them as socially constructed changes. Those involved in early computing developed a set of ethics which can, I would argue, best be explained by situating them within theories of Network Societies (Castells, 2012).

Castells argues that power is based upon controlling various types of information networks and their connections to other networks through 'switches'. Increasing inequality and crisis of legitimacy eventually meet with an emotional trigger such as a violent event. Outrage against injustice and hope for change creates resistance to the dominant power in the form of social movements which reprogram and disrupt dominant switches. These kinds of social movements are based upon mass self-communication which is autonomous from state or corporate control, forms of communication which used to be completely under state control but are no longer, facilitated by new technologies such as the internet:

> *"The combination of a degradation of the material conditions of life and of a crisis of legitimacy of the rulers in charge of the conduct of public affairs induces people to take matters into their own hands, engaging in collective action outside the prescribed institutional channels, to defend their demands and, eventually, to change the rulers, and even the rules shaping their lives." (Castells, 2012, p.219)*

While collective anger is the trigger for these movements, fear is the repressor since the state still ultimately has power over force and even violence. This fear, however, can be overcome through collective action and a sense of community.

The technological artefacts, narratives and networks produced by Civic Hackers are expressions of contest against these power structures and reflect a wider move towards democratisation seen in various movements. Civic Hackers resist corporate power and the traditional dominance of development work through collaborating on hacks to producing locally appropriate solutions. Their artefacts and narratives provide insights into this attempt to re-negotiate the power relationships embedded in the technology and redistribute information to the many.

Key ideals which are closely related to the Hacker Ethics include the democratisation of information and decentralisation would appear to be key components of these social movements. However, while certain technologies such as personal computers, the internet, open-source code or social media, may have intertwined with and facilitated hacking as a set of ethics, we should not view them as the determining factors but rather as expressions of social changes.

It is worth reflecting upon the origins of computer hacking in 1960s North America and Northern Europe. This is a period in which post-war liberalism, counterculture and the democratisation of information networks were taking place which were not tied to a specific technological change or group (BBC, 25 Jan. 2011b). It seems likely, therefore, that hacking was also influenced by this wider social change – what are referred to as the Hacker Ethics. I would argue that, in the past decade, movements such as those described above, and indeed Civic Hacking, can be viewed as expressions of these changes and an increasing desire by the general population for greater democratisation of information. In cases where this has clashed with state control of that information this has caused conflict and resistance in the form of protest, criminalisation of hackers, or legal debates over copyright.

The increasing significance of what has been termed Hacker Ethics were expressed in one way through modification of computing technology but also through a number of other channels, for example, music, science and business. Yet it is the culture and practices of computer hacking which have had a direct influence upon the groups I have engaged with.

It is important to note that, during the course of my research, the public interest and awareness in what might be described as hackers such as Alan Turing, Steve Jobs and Mark Zuckerberg as well as the broader history of 'hacking' as unorthodox innovation through individuals such as Babbage or Da Vinci, began to intensify. The use of the term hacking and hacking culture in mainstream life became commonplace in fields from corporate human resources to music to academia. Hacking has now, I would argue, gained a degree of positive legitimacy within the public attention. It has become 'cool' to associate a product or event with the imagery, lexicon or culture of hacking (Heath and Potter, 2006).

On the other hand, as my research progressed, I began to question whether certain activities involved in Civic Hacking can in fact truly be described as hacking. Are the practices and culture of hacking simply being re-appropriated by mainstream industries in order to commoditise the credibility it appears to hold within certain areas of society? Being a hacker within a Network Society appears to be both a powerful position and also brings marketability due to the growing interest in the history of positive hacking. My interpretation of research findings among Civic Hackers, at least, suggests that for those involved in Civic Hacking at grassroots level this does not appear to be the case and that they strongly associate with the Hacker Ethics. Perhaps, however, for corporate organisers of these events and for those in other fields this re-appropriation may be a factor.

Finally, I believe I have made a contribution to the wider social study of technologies through my methodological approaches. By combining interviews and participant observation with other methods, including Social Network Analysis and Narrative Analysis, I was able to gain a more holistic insight into the groups I was studying. I also combined online and offline data to increase my understanding which is important when studying practices which take place across multi-sited and temporally fluid boundaries. I was required to develop the use of innovative techniques which I would argue have applications across a range of modern fieldwork.

8.8 Scope for Future Research

One of my research aims was to address the ethnocentric nature of previous research into hacking by exploring the practice of groups outside of the USA and Northern Europe. To some extent I was able to achieve this by observing groups comprised of global participants and some of the activities of ICT4D. However, this remains a significant gap which could be explored through future research.

There is still a substantial amount of understanding to be gained regarding hacking by examining its practice as related to specific cultures and societies. Based on my experience, there are likely to be challenges in terms of data collection which would need to be addressed. For example, identifying civic hacking groups outside the US and Europe can itself be problematic and gaining first-hand access to them would require some degree of integration. Relying upon online data sources only clearly has its own in-built bias.

In addition, I was not able to explore in detail some of the other groups which I suggested express Hacker Ethics through their practices. A future area for research would be to test some of my inferences against wider groups such as open data projects, Clean Web advocates and so on. My question regarding the shaping of technological artefacts was limited to a relatively small number of projects therefore future research could certainly be aimed towards a wider range of these objects.

As identified in Chapter 2, there are gender aspects to hacking, and indeed technology more generally, which are relatively unexplored. I identified civic hacking groups with a focus on addressing gender inequality both in the focus of their activities and the nature of the groups themselves. While these were not the primary focus of my own research project, they do provide opportunities for future research and also to address imbalances in current research. This may also apply to less documented class and race dimensions to civic hacking.

There is also scope for gaining more insight into the unofficial social media channels and forums used by civic hackers. Due to the challenges of gaining access to these data sources, there were limitations within my own research in this respect. Therefore, there is potential for future research focusing on these parallel channels. This might also extend to more data gained from long term immersion with grassroots activist and hacking participants. This would allow for more first-hand data collection among those involved in civic hacking.

8.9 Hack the Planet - Final Remarks

To return to the question posed at the beginning of this thesis; ‘what is hacking?’. At a purely practical level, it might involve diverse practices of disruption and intervention, technological or otherwise – the manipulation of code. In a sense, those things encompass what hacking *does*. But what does it really *mean*? This is an important question since it has wider implications for the societies in which we live.

The meaning of hacking is assigned both by its participants and observers. Whether writing code or reading media articles, we all contribute to our shared understanding of hacking. One might question whether any of us are really just passive observers or whether we are all in fact involved in hacking - whether we realise it or not. Hacking, being hacked, demonising or mythologizing hackers. We are all complicit in defining what hacking means. It is a reflection of the world around it, a world which is increasingly defined by a tension between those who control informational networks and those who seek to democratise them.

And, conversely, hacking has also shaped the world around it. Despite the romanticism of some commentators, it is undeniable that our society is defined by hacking in many more pragmatic ways. This can be seen in the friction between the hierarchical black-box of consumer technology and the desire by individuals to take control over their own destiny.

Civic Hackers play an important role in addressing this meaning of hacking. They can help us to understand something about the ways in which ethic, code in another less literal sense of the word, is so central to this meaning. In this way, they provide an important counterbalance to the often dystopian folklore of hacking. I have found that hacking is not defined by terms such as 'good' or 'bad'. It is instead about renegotiation, resistance and contest between those whose interests lie in containing information and those who seek to extend its boundaries.

Bibliography

Abbott, H. (2008) *The Cambridge Introduction to Narrative*, Cambridge: Cambridge University Press.

Adam, A. (1998) *Artificial Knowing: Gender and the Thinking Machine*, London: Routledge.

Adam, A. (2001) ‘Gender and Computer Ethics', in R. Spinello and H. Tavani (eds.) *Readings in CyberEthics*, Sudbury MA: Jones and Bartlett, 63-76.

Adam, A. (2003) ‘Hacking into Hacking: Gender and the Hacker Phenomenon’, *ACM SIGAS Computers and Society*, 33(4), 3.

Agar, (1996) *The Professional Stranger: An Information Introduction to Ethnography*, Bingley: Emerald Group Publishing Limited.

Alberts, G. and Oldenziel, R. (2014) *Hacking Europe: From Computer Cultures to Demoscenes*, London: Springer.

Alleyne, B. (2015) *Narrative Networks: Storied Approaches in the Digital Age*, London: SAGE.

Alleyne, B. (2016) *Geek, Hacker and Gamer Stories: Challenging Code*, London: Palgrave.

Altorki, S. (2014) *Arab Women in the Field: Studying Your Own Society*, New York: Syracuse University Press.

Amit, V. (2007) *Constructing the Field: Ethnographic Fieldwork in the Contemporary World*, London: Routledge.

Amsden, A. and Clark, J. (1999) ‘Software Entrepreneurship among the Urban Poor: Could Bill Gates Have Succeeded if He Were Black?...Or Impoverished?’, in

Schon, D., Sanyal, B. and Mitchell, W. (eds.) (1999) *High Technology and Low-Income Communities*, Cambridge, MA: MIT Press. 213.

Anderson, B. (2006) *Imagined Communities*, London: Verso.

Anonymous (2013) *Anonymous by Anonymous*, London: Imaginary Book Co.

Aspers, P. and Darr, A. (2011) 'Trade Shows and the Creation of Market and Industry', *The Sociological Review,* 59(4), 758-778.

Assange, J. (2012) *Cypherpunks: Freedom and the Future of the Internet*, London: OR Books.

Assange, J. and Dreyfus, S. (2011) *Underground: Tales of Hacking, Madness and Obsession on the Electronic Frontier*, Edinburgh: Canongate.

Atkinson, P. and Hammersley, M. (1994) 'Ethnography and Participant Observation', in N.K. Denzin and Y.S. Lincoln (eds.) *Handbook of Qualitative Research*, Thousand Oaks: SAGE Publications, 248-261.

Attewell, P. (2001) 'The First and Second Digital Divide', *Sociology of Education,* 74(3), 252-259.

Attride-Stirling, J. (2001) 'Thematic Networks: An Analytical Tool for Qualitative Research', *Qualitative Research, 1(3),* 385-405.

Bar, F., Weber, M. and Pisani, F. (2007) *Mobile Technology Appropriation in a Distant Mirror: Baroque Infiltration, Creolization and Cannibalism*. Available: http://www.researchgate.net/publication/253284230_Mobile_technology_appropriation_in_a_distant_mirror_baroque_infiltration_creolization_and_cannibalism. [Last Accessed 8th October 2015].

Barbrook, R. (2005) 'The Hi-Tech Gift Economy', *First Monday,* 3(12).

Barbrook, R. and Cameron, A. (1995) 'The Californian Ideology', *Science as Culture*, 6(1), 44-72.

Barker, J. and Downing, H. (1980) 'Word Processing and the Transformation of Patriarchal Relations of Control in the Office', *Capital and Class*, 10.

Barnard, A. (2000) *History and Theory in Anthropology*, Cambridge: Cambridge University Press.

Barter, C. and Renold, E. (1999) *The Use of Vignettes in Qualitative Research*. Available: ru.soc.surrey.ac.uk/SRU25.html. [Last Accessed 21st August 2017].

BBC news (2010) 'Wikileaks' Julian Assange Tells of 'Smear Campaign'', *BBC News*, 17 Dec. 2010. Web. Available: http://www.bbc.co.uk/news/uk-12015140. [Last Accessed: 7th October 2015].

BBC (2011a) 'Panorama: WikiLeaks: The Secret Story', *BBC Television*, 14 February.

BBC news (2011b) 'Hackers and Hippies: The Origins of Social Networking', *BBC News*, 25 Jan. 2011. Web. Available: http://www.bbc.co.uk/news/technology-12224588. [Last Accessed 7th October 2015].

BBC news (2011c) 'Anonymous Defends the use of Web Attacks', *BBC News*, 28 Jan. 2010. Available: http://www.bbc.co.uk/news/technology-12307802. [Last Accessed 7th October 2015].

Beaulieu, A. (2004) 'Mediating Ethnography: Objectivity and the Making of Ethnographies of the Internet', *Social Epistemology*, 18(2), 139-163.

Becker, H. (1963) *Outsiders*, New York: The Free Press.

Bell, D. (1973) *The Coming of Post Industrial Society*, New York: Basic Books.

Ben-Yehuda, N. (1990) 'Positive and Negative Deviance: More Fuel for Controversy', *Deviant Behaviour*, 11(3): 221-243.

Bender, E. (2011) *Nightwork: A History of Hacks and Pranks at MIT*, Cambridge MA: The MIT Press.

Benkler, Y. (2006) *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven: Yale University Press.

Benkler, Y. (2011) *The Penguin and the Leviathan: The Triumph of Cooperation Over Self-Interest*, New York: Crown Publishing.

Berg, S. (1988) 'Snowball Sampling', in S. Kotz and N.L. Johnson (eds), *Encyclopaedia of Statistical Sciences Vol8*, New York: Wiley.

Berg, S. (2009) *Qualitative Research Methods for the Social Sciences*, Harlow: Pearson Education Limited.

Boas, (2004) *Global Institutions and Development: Framing the World?*, New York: Routledge.

Boellstorff, T. (2008) *Coming of Age in Second Life*, Princeton: Princeton University Press.

Bornstein, D. and Davis, S. (2010) *Social Entrepreneurship: What Everyone Needs to Know*, Oxford: Oxford University Press.

Borsook, P. (2000) *Cyberselfish: A Critical Romp Through the Terribly Libertarian Culture of High Tech*, New York: PublicAffairs.

Bourdieu, P. (1991) *Language and Symbolic Power*, Cambridge MA: Harvard University Press.

Bowker, G. and Star, S. (2000) *Sorting Things Out: Classification and Its Consequences*, Cambridge MA: MIT Press.

Brail, S. (1996) 'The Price of Admission: Harassment and Free Speech in the Wild, Wild West', in L. Cherny. and E. Wise (eds.), *Wired Women: Gender and New Realities in Cyberspace*, Seattle, WA: Seal Press, 141-57.

Bryman, A. (2008) *Social Research Methods*, Oxford: Oxford University Press.

Buchanan, T. (2000) 'Internet Research: Self-Monitoring and Judgments of Attractiveness', *Behaviour Research Methods, Instruments and Computers*, 32(4): 521-527.

Bunge, M. (1977) 'Towards a Technoethics', *The Monist*, 60(1), 96-107.

Burrell, J. (2010) 'Evaluating Shared Access: Social Equality and the Circulation of Mobile Phones in Rural Uganda', *Journal of Computer-Mediated Communication*, 15(2), 230–250.

Busch, O. and Palmas, K. (2006) *Abstract Hacktivism: The Making of a Hacker Culture*, London: Open Mute.

Caltagirone, S. (No Date) *A Practical Ethical Assessment of Hacktivism*, Available: www.classstudio.com/papers/grad_papers/comp.../hacktivism_ethics.doc [Last Accessed 6th October 2015].

Candea, M. (2007) 'Arbitrary Locations: In Defence of the Bounded Field-Site', *Journal of the Royal Anthropological Institute*, 13(1), 167-184.

Castells, M. (1999) 'The Informational City is a Dual City: Can it be Reversed?', in Schon, D., Sanyal, B. and Mitchell, W. (eds.) (1999) *High Technology and Low-Income Communities*, Cambridge, MA: MIT Press. 213.

Castells, M. (2000) *The Rise of the Network Society*, London: Blackwell Publishers.

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

Castells, M. (2012) *Networks of Outrage and Hope*, Cambridge: Polity Press.

Castells, M., Fernandez-Ardevol, M., Qiu, J. and Sey, A.. (2007) *Mobile Communication and Society: A Global Perspective*, Cambridge MA: MIT Press.

Chadwick, A. (2006) *Internet Politics: States, Citizens and New Communication Technologies*, Oxford: Oxford University Press.

Chambers, R. (1997) *Whose Reality Counts: Putting the First Last*, London: ITDG Publishing.

Chan, A. (2004) 'Coding Free Software, Coding Free States: Free Software Legislation and the Politics of Code in Peru', *Anthropological Quarterly* 77(3), 531-545.

Chandler, A. (1996) 'The Changing Definition and Image of Hackers', *International Journal of the Sociology of Law,* 24, 229–251.

Christensen, H. S. (2011) 'Political activities on the Internet: Slacktivism or political participation by other means?', *First Monday,* 16(2).

May, C. (2002) *The Information Society: A Sceptical View*, Cambridge: Polity Press.

Chun, W. (2011) *Programmed Visions: Software and Memory*, Cambridge MA: MIT Press.

Clifford, J. and Marcus, G. (1986) *Writing Culture: The Poetics and Politics of Ethnography*, California: University of California.

Code for America. (2015) *About Code for America*. Available: http://www.codeforamerica.org/about/. [Last Accessed: 7th October 2015].

Cohen, S. (1972) *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, New York: Routledge.

Coleman, G. (2004) 'The Political Agnosticism of Free and Open Source Software and the Inadvertent Politics of Contrast', *Anthropological Quarterly,* 77(3), 507-519.

Coleman, G. (2009) *Anonymous: From the Lulz to Collective Action. The New Everyday*. Available: http://mediacommons.futureofthebook.org/tne/pieces/anonymous-lulz-collective-action. [Last Accessed 5th October 2015].

Coleman, G. (2010) 'The Hacker Conference', *Anthropological Quarterly*, 83(1), 47–72.

Coleman, G. (2013) *Coding Freedom: The Ethics and Aesthetics of Hacking*, New Jersey: Princeton University Press.

Coleman, G. (2014) *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, London: Verso.

Coleman, E. G. and Golub, A. (2008) 'Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism', *Anthropological Theory,* 8(3), 255-277.

Coleman, S. and Blumler, J.G. (2009) *The Internet and Democratic Citizenship: Theory, Practice and Policy*, Cambridge: Cambridge University Press.

Cooper, J. R. (2000) 'The CyberFrontier and America at the Turn of the 21st Century: Reopening Frederick Jackson Turner's Frontier', *First Monday,* 5(7).

Cormode, G., Krishnamurthy, B. and Willinger, W. (2011) 'A Manifesto for Modelling and Measurement in Social Media', *First Monday,* 15(9).

Cova, B. (2007) *Consumer Tribes*, Oxford: Butterworth-Heinemann.

Cox, G. (2013) *Speaking Code: Coding as Aesthetic and Political Expression*, Cambridge MA: The MIT Press.

Critical Art Ensemble (1994) *The Electronic Disturbance*, New York: Autonomedia.

Critical Art Ensemble (1996) *Electronic Civil Disobedience and Other Unpopular Ideas*, New York: Autonomedia.

Cudd, A. (2001) 'Objectivity and Ethno-Feminist Critiques of Science', in K. Ashman and P. Baringer (eds.) *After the Science Wars*, New York: Routledge, 80-97.

Czarniawska, B. (2007) *Shadowing and Other Techniques for Doing Fieldwork in Modern Societies*, Copenhagen: CBS Press.

Hackers (1996) [DVD] Directed by Iain Softley. USA: MGM.

Davies, A. (2011) *Measuring the mood of the world.* PhD. Thesis. University of Cambridge.

Dean, J., Anderson, J.W. and Lovink, G. (2006) *Reformatting Politics: Information Technology and Global Civil Society*, New York: Routledge.

Delamont, S. (2004) 'Ethnography and Participant Observation', in Seale, C. et al (eds.) *Qualitative Research Practice*, London: SAGE.

DeMars, W.E. (2005) *NGOs and Transnational Networks: Wild Cards in World Politics*, London: Pluto Press.

Dickson, D. (1984) *The New Politics of Science*, New York: Pantheon.

Dizard, W.P. (1981) 'The Coming of the Information Age', *The Information Society*, 2, 91-112.

Dodge, M. and Kitchen, R. (2006) 'Exposing the Secret City: Urban Exploration as 'Space Hacking" [PowerPoint Presentation]. *AAG Annual Meeting, 11 March 2006, Chicago*. Available: http://www.casa.ucl.ac.uk/martin/aag_space_hacking.pdf [Last Accessed: 23rd August 2017].

Donner, J. (2007) 'The Rules of Beeping: Exchanging Messages Via Intentional "Missed Calls" on Mobile Phones', *Journal of Computer-Mediated Communication,* 31(1), 1-22.

Donner, J. (2009a) 'Blurring Livelihoods and Lives: The Social Uses of Mobile Phones and Socioeconomic Development', *Innovations: Technology, Governance, Globalization,* 4(1), 91-101.

Donner, J. (2009b) *Mobile-Based Livelihood Services in Africa: Pilots and Early Deployments*. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.205.2894. [Last Accessed 8th October 2015].

Dr. K. (2004) *Hackers' Tales: Stories from the Electronic Front Line*, London: Carlton Books.

Drucker, P. (1968) *The Age of Discontinuity: Guidelines to Our Changing Society*, New York: Routledge.

Dyer, R. (1997) *White: Essays on Race and Culture*, New York: Routledge.

Dyson, E. (1997) *Release 2.0: A Design for Living in the Digital Age*, London: Viking.

Eberle, T. and Maeder, C. (2011) 'Organisational Ethnography', in D. Silverman (ed.) *Qualitative Research,* London, SAGE.

Economic and Social Research Council. (2015) *ESRC Framework for Research Ethics 2015*. Available: http://www.esrc.ac.uk/funding/guidance-for-applicants/research-ethics/. [Last Accessed: 24th November 2015].

The Economist (2012) *Smart Policies to Close the Digital Divide*. Available: http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan049753.pdf [Last Accessed 23rd August 2017].

Edwards, P. (1996) *The Closed World: Computers and the Politics of Discourse in Cold War America*, Cambridge MA: MIT Press.

Ekine, S., Ed. (2010) *SMS Uprising: Mobile Activism in Africa*, Cape Town: Pambazuka Press.

Eliot, A., Norum, R. and Salazar, N. (eds.) (2017) *Methodologies of Mobility: Ethnography and Experiment*, New York: Berghahn.

Eriksen, T. (2001) *Small Places, Large Issues: An Introduction to Social and Cultural Anthropology*, London: Pluto Press.

Ewick, P. and Silbey, S. (2003) 'Narrating Social Structure: Stories of Resistance to Legal Authority', *American Journal of Sociology*, 108(6): 1328-72.

Fafinski, S. (2009) *Computer Misuse: Response, Regulation and the Law*, New York: Routledge.

Falzon, M. (2009) *Multi-Sited Ethnography: Theory, Praxis and Locality in Contemporary Research*, New York: Routledge.

Fardon, R., Van Binsbergen, W. and Van Dijk, R. (eds.) (1999) *Modernity on a Shoestring: Dimensions of Globalisation, Consumption and Development in Africa and Beyond*, London: EIDOS.

Feather, J. (2008) *The Information Society: A Study of Continuity and Change*, London: Facet Publishing.

Feenberg, A. (1999) *Questioning Technology,* New York: Routledge.

Fereday, J. and Muir-Cochrane, E. (2006) 'Demonstrating Rigor Using Thematic Analysis: A Hybrid Approach of Inductive and Deductive Coding and Theme Development', *International Journal of Qualitative Methods*, *5*(1).

Fernandez-Ardevol, M. *and Ros, A.* (2009) *Communication Technologies in Latin America and Africa: A Multidisciplinary Perspective*, Barcelona: Universitat Oberta de Catalunya.

Findeli, A. (1994) 'Ethics, Aesthetics and Design', *Design Issues*, 10(2), 49-68.

Flowers, S. (2008) 'Harnessing the hackers: The Emergence and Exploitation of Outlaw Innovation', *Research Policy* 37(2), 177-193.

Forsey, M. (2010) 'Ethnography and the Myth of Participant Observation', in S. Hillyard, *Studies in Qualitative Methodology*, Bingley: Emerald Group Publishing, 65-79.

Foucault, M. (2003) *The Birth of the Clinic*, New York: Routledge.

Frank, T. (1997) *The Conquest of Cool*, Chicago: University of Chicago Press.

Franklin, M. (2007) 'NGOs and the "Information Society": Grassroots Advocacy in the UN – Cautionary Tale', *Review of Policy Research*, 24(4), 309-330.

Franklin, M. (2012) *Understanding Research: Coping with the Quantitative-Qualitative Divide,* New York: Routledge.

Franklin, M. (2014) 'Slacktivism', *OUPBlog, 19th November 2014*. Accessed: https://blog.oup.com/2014/11/slacktivism-clicktivism-real-social-change/. [Last Accessesd 23rd August 2017].

FrontlineSMS (2010). *FrontlineSMS*. Available: http://www.frontlinesms.com. [Last Accessed: 4th December 2010].

Fuchs, C. (2011) 'New Media, Web 2.0 and Surveillance', *Sociology Compass*, 5(2), 134-147.

Fuchs, C. (2014) *Social Media: A Critical Introduction*, New York: SAGE.

Fuller, M. (2003) *Behind the Blip: Essays on the Culture of Software*, Brooklyn: Autonomedia.

Fuller, M. (2005) *Media Ecologies: Materialist Energies in Art and Technocultures*, Cambridge MA: MIT Press.

Fuller, M. (2008) *Software Studies: A Lexicon*, Cambridge MA: MIT Press.

Fuller, M. (2017) *How to Be a Geek: Essays on the Culture of Software*, Cambridge: Polity Press.

Galvan, J. (2003) 'On Technoethics', *IEE-RAS Magazine*, 10, 58-63.

Garfinkle, H. (1967) *Studies in Ethnomethodology*, Cambridge: Polity Press.

Garfinkle, H. (1996) 'Ethnomethodology's Program', *Social Psychology Quarterly,* 59(1), 5-21.

Garrett, B. (2011) 'Assaying History: Creating Temporal Junctions Through Urban Exploration', *Environment and Planning,* 29, 1048-1067.

Garrett, B. (2012) *Place Hacking: Tales of Urban Exploration*. PhD. Thesis. Royal Holloway, University of London.

Garud, R. (2008) 'Conferences as Venues for the Configuration of Emerging Organizational Fields: The Case of Cochlear Implants', *Journal of Management Studies,* 45(6), 1061-1088.

Gatignon, H., Gotteland, D., and Haon, C. (2015) *Making Innovation Last: Volume 2*, London: Palgrave MacMillan.

Gee, J. (2013) *The Routledge Handbook of Discourse Analysis*, New York: Routledge.

Geertz, C. (1973) *The Interpretation of Cultures*, New York: Basic Books.

Girls Who Code (2017) Girls Who Code Website. Available: https://girlswhocode.com. [Last Accessed 23rd August 2017].

Gitau, S. and Donner, J. (2010) 'After Access: Challenges Facing Mobile-Only Internet Users in the Developing World', in *Proceedings of the 28th International Conference on Human Factors in Computing Systems*. CHI2010, April 2010, Atlanta. New York: ACM. Pp.2603-2606.

Glenny, M. (2011) *DarkMarket: CyberThieves, CyberCops and You*, London: Bodley Head.

Glough, P. (1993) *Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers and Keyboard Criminals*, London: Random House.

Goliama, C. (2011) *Where are you Africa? Church and Society in the Mobile Phone Age*, Bamenda: Langaa RPCIG.

Golumbia, D. (2013) *Cyberlibertarianism: The Extremist Foundations of 'Digital Freedom'*. 5th September 2013, Clemson University. Available: http://www.uncomputing.org/?p=276. [Last Accessed: 6th October 2015].

Goode, L. (2015) 'Anonymous and the Political Ethos of Hacktivism', *Popular Communication*, 13(1), 74-86.

Gouldner, A. (1979) *The Future of Intellectuals and the Rise of the New Class*, London: Palgrave

Gozukele, I. (2006) *Free and Open Source Software Hackers in Turkey*. Available: https://www.linux.org.tr/wp-content/uploads/2010/04/Gozukeles-WorkingPaper.pdf (Last Accessed: 6th October 2015).

Gupta, A. and Ferguson, J. (1992) 'Beyond "Culture": Space, Identity and the Politics of Difference', *Cultural Anthropology*, 7(1): 6-23.

Granovetter, M. (1973) 'The Strength of Weak Ties', *American Journal of Sociology,* 78(6), 1360-1380.

Gray, D. E. (2013) *Doing Research in the Real World*, London: SAGE.

Gurstein, M. (2003). 'Effective use: A Community Informatics Strategy Beyond the Digital Divide'. *First Monday* 8(12).

Gustavson, L. and Cytrynbaum, J. (2003) 'Illuminating Spaces: Relational Spaces, Complicity and Multisited Ethnography', *Field Methods*, 15(3), 252-270.

Gurumurthy, A. (2003) A Gender Perspective to ICTs and Development: Reflections Towards Tunis. Available: http://www.worldsummit2003.de/en/web/71.htm. [Last Accessed: 24th October 2017]

Hack4Good. (2014). *Hack4Good Website*. Available: http://hack4good.io/. [Last Accessed: 7th October 2015].

Haddon, L. (1992) 'Explaining ICT Consumption: The Case of the Home Computer', in R. Silverstone and E. Hirsch (eds.), *Consuming Technologies: Media and Information in Domestic Spaces*, London: Routledge, 82-96.

Hage, G. (2005) 'A Not-So Multi-Sited Ethnography of a Not-So Imagined Community', *Anthropological Theory,* 5(4), 463-75.

Hamelink, C. (1986) 'Is There Life After the Information Revolution?', in M. Traber (ed.), *The Myth of the Information Revolution*, London: Sage, 7-20.

Hannerz, U. (2003) 'Diversity is Our Business', *American Anthropologist*, 112(4), 539-551.

Hansen, D. (2011) 'Exploring Social Media Relationships', *On the Horizon*, 19(1), 43-51.

Hansen, D., Rotman, D., Bonsignore, E., Milić-Frayling, N., Rodrigues, E., Smith, M., Shneiderman, B. and Capone, T. (2012) 'Do You Know the Way to SNA?: A Process Model for Analyzing and Visualizing Social Media Data', in *Proceedings of the 2012 International Conference on Social Informatics, December 2012, Washington DC*. Washington DC, IEEE Computer Society. pp. 304-313.

Haywood, D. (2013) 'The Ethic of the Code: An Ethnography of a Humanitarian Hacking Community', *Journal of Peer Production, Issue #3.*

Healy, D. (1996) *Cyberspace and Place: The Internet as Middle Landscape on the Electronic Frontier*, New York: Routledge.

Heath, J. and Potter, A. (2006) *The Rebel Sell*, Chichester: Capstone Publishing.

Heckert, D. (1989) 'The Relativity of Positive Deviance: The Case of the French Impressionists', *Deviant Behaviour*, 10(2): 131-144.

Heeks, R. (2008) 'ICT4D 2.0: The Next Phase of Applying ICT for International Development', *Computer*, 41(6), 26-33.

Henri, F. and Pudelko, B. (2003) 'Understanding and Analysing Activity and Learning in Virtual Communities', *Journal of Computer Assisted Learning*, 19(4): 474-487.

Henwood, F. (1993) Gender Perspectives on Information Technology: Problems, Issues and Opportunities', in E. Green, J. Owen and D. Pain (eds.), *Gendered by Design? Information Technology and Office Systems*, London: Taylor and Francis, 31-49.

Herring, S. (1996) 'Posting in a Different Voice: Gender and Ethics in CMC', in C. Ess (eds.) *Philosophical Perspectives on Computer-Mediated Communication*, Albany : State University of New York Press, 115-45.

Hersman, E. (2015) *AfriGadget Website*. Available: www.AfriGadget.com. [Last Accessed: 7th October 2015].

Hill, K. A. (1998) *Cyberpolitics: Citizen Activism in the Age of the Internet*, Lanham: Rowman & Littlefield Publishers.

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

Himanen, P. (2009) *The Hacker Ethic: A Radical Approach to the Philosophy of Business*, London: Random House.

Hindman, M. (2009) *The Myth of Digital Democracy*, Oxford: Princeton University Press.

Hine, C. (2000) *Virtual Ethnography*, London: SAGE.

Hine, C. (2015) *Ethnography for the Internet*, London: Bloomsbury.

Horst, H. (2006) 'The Blessings and Burdens of Communication: Cellphones in Jamaican Transnational Social Fields', *Global Networks*, 6(2): 143–159.

Horst, H. and Miller, D. (2006) *The Cell Phone: An Anthropology of Communication*, New York: Berg Publishers.

Illia, L. (2002) 'Passage to Cyberactivism: How dynamics of Activism Change', *Journal of Public Affairs,* 3(4), 326-337.

Isaacson, W. (2014) *The Innovators*, London: Simon & Schuster.

Jacobson, A. (2013) 'Vignettes of Interviews to Enhance an Ethnographic Account', *Ethnography and Education*, 9(1), 35-50.

Jargon File (2007) *The Meaning of 'Hack'.* Available: http://www.catb.org/jargon/html/meaning-of-hack.html, [Last Accessed: 6th October 2015].

Jesiek, B. K. (2003) 'Democratizing software: Open Source, The Hacker Ethic and Beyond', *First Monday,* 8(10).

Johnson, D. (1985) *Computer Ethics,* NJ: Prentice-Hall.

Johnson, S. (1997) *Interface Culture: How New Technology Transforms the Way We Create and Communicate,* San Francisco: Harper.

Jordan, T. (2001) 'Mapping Hacktivism: Mass Virtual Direct Action (MVDA), Individual Virtual Direct Action (IVDA) and Cyber Wars', *Computer Fraud and Security*, 2001(4), 8-11.

Jordan, T. (2002) *Activism! Direct Action, Hacktivism and the Future of Society*, London: Reaktion Books.

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

Jordan, T. (2009) 'Hacking and Power: Social and Technological Determinism in the Digital Age', *First Monday,* 14(7).

Jordan, T. and Taylor, P. (1998) 'A Sociology of Hackers', *The Sociological Review,* 46(4), 757-780.

Jordan, T. and Taylor, P. (2004) *Hacktivism and Cyberwars: Rebels with a Cause*, London: Routledge.

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

Kember, S. (2003) *Cyberfeminism and Artificial Life*, London: Routledge.

Kidder, T. (2011) *The Soul of a New Machine*, New York: Back Bay.

Kitchin, R. and Dodge, M. (2011) *Code/Space*, Cambridge MA: MIT Press.

Kleinknecht, S. W. (2003) *Hacking Hackers: Ethnographic Insights into the Hacker Subculture-Definition, Ideology and Argot.* M.A. Thesis. Ontario McMaster University.

Kloet, J. D. (2002*)* 'Digitisation and Its Asian Discontents: The Internet, Politics and Hacking in China and Indonesia', *First Monday,* 7(9).

We Are Legion: The Story of the Hacktivists (2012) Luminant Media

Kollock, P. (1999) *Communities in Cyberspace*, London: Routledge.

Korupp, S. and Szydlik, M. (2005) 'Causes and Trends of the Digital Divide', *European Sociological Review,* 21(4), 409-422.

Kozinets, R. (2010) *Netnography: Doing Ethnographic Research Online*, London: SAGE Publications.

Kozinets, R. (2015) *Netnography: Refined*, London: SAGE Publications.

Kramer, J. and Kramarae, C. (1997) 'Gendered Ethics on the Internet', in J. Makau and R. Arnett (eds.) *Communication Ethics in an Age of Diversity*, Chicago: University of Illinois Press, 226-43.

Larsson, S. (2008) *The Girl with the Dragon Tattoo*, London: McLehose Press.

Lash, S. (2002) *Critique of Information*, London: SAGE.

Latour, B. (1999) *Pandora's Hope: Essays on the Reality of Science Studie*s, Cambridge, MA: Harvard University Press.

Latour, B. (2005) *Reassembling the Social: An Introduction to Actor-Network Theory*, Oxford: Oxford University Press.

Leadbetter, C. (1999) *Living on Thin Air: The New Economy*, London: Penguin.

Leonard, K. (2009) 'Changing Places: The Advantages of Multi-Sited Ethnography', in M. Falzon (ed.) *Multi-Sited Ethnography: Theory, Praxis and Locality in Contemporary Research*, New York: Routledge, 165-180.

Lessig, L. (2001) *The Future of Ideas: The Fate of the Commons in a Connected World*, New York: Random House.

Lessig, L. (2004) *Free Culture: The Nature and Future of Creativity, London*: Penguin Books.

Lévi-Strauss, C. (1966) *The Savage Mind*, Chicago, IL: University of Chicago Press.

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

Lewis-Beck, M., Bryman, A. and Liao, T. (2004) *The SAGE Encyclopedia of Social Science Research Methods*, London: SAGE.

Li, N. and Kirkup, G. (2002) 'The Internet: Producing or Transforming Culture and Gender', *Electronic Journal of Communication*, 12(3-4): 1066-1080.

Lin, Y. and Beer, D. (2005) 'Is Hacking Illegal?', in *Sarai Reader, Bare Acts,* New York: Autonomedia, 205-214. Available: http://archive.sarai.net/files/original/41bc414cbdcd812480f41d8bc14154e8.pdf. [Last Accessed: 23rd August 2017].

Lovink, G. (2003) *Dark Fiber*, Cambridge, MA: MIT Press.

Lovink, G. (2008) *Zero Comments: Blogging and Critical Internet Culture*, London: Routledge.

Lovink, G. (2011) *Networks Without a Cause: A Critique of Social Media*, Cambridge: Polity Press.

Lovink, G. (2016) *Social Media Abyss: Critical Internet Cultures and the Force of Negation*, Cambridge: Polity Press.

Lovink, G. (2017) '"Developing Dissident Knowledges": Interview with Geert Lovink', *Net Critique. Available*: http://networkcultures.org/geert [Last Accessed 23rd August 2017].

Lu, Y., Luo, X., Polgar, M. and Cao, Y. (2010) 'Social Network Analysis of a Criminal Hacker Community', *Journal of Computer Information Systems*, 51(2), 31.

Lueg, C. (2001) 'Newsgroups as Virtual Communities of Practice', *European Conference on Computer Supported Cooperative Work, 16-20 September.* Bonn, Germany.

Luppicini, R. (2008) 'The Emerging Field of Technoethics', in R. Luppicini and R. Adell (eds.) *Handbook of Research on Technoethics*, Hershey: Idea Group Publishing.

Lupton, D. (2015) *Digital Sociology*, Oxon: Routledge.

Luyt, B. (2004) 'Who Benefits from the Digital Divide?', *First Monday*, 9(8).

Machlup, F. (1962) *The Production and Distribution of Knowledge in the United States*, Princeton: Princeton University Press.

MacKenzie, A. (2006) *Cutting Code*, New York: Peter Lang.

MacKenzie, A. (2010) *Wirelessness*, Cambridge MA: MIT Press.

MacKenzie, D. and Wajcman, J. (eds.) (1999) The Social Shaping of Technology, Maidenhead: Open University Press.

Malinowski, B. (2014) *Argonauts of the Western Pacific*, Oxon: Routledge.

Manovich, L. (2013) *Software Takes Command*, London: Bloomsbury.

Marcus, G. (1995) 'Ethnography in/of the World System: The Emergence of Multi-Sited Ethnography', *Annual Review of Anthropology,* 24, 95-117.

Markham, A. (1998) *Life Online: Researching Real Experience in Virtual Space*, Lanham: AltaMira Press.

Marres, N. and Rogers, R. (2005) 'Recipe For Tracing the Fate of Issues and Their Publics on the Web', in B. Latour and P. Weibel (eds.) *Making Things Public: Atmospheres of Democracy,* Cambridge MA: MIT Press, 922-935.

Marx, L. (1989) *The Pilot and the Passenger: Essays on Literature, Technology, and Culture in the United States*, Oxford: Oxford University Press.

Marx, L. (2010) *The Machine in the Garden: Technology and the Pastoral Ideal in America*, Oxford: Oxford University Press.

Mason, J. (1996) *Qualitative Researching*, London: SAGE.

Mathaba. (2011) *Hacktivism: From Here to There*. Available: http://www.mathaba.net/news/?x=625772. [Last Accessed: 7th October 2015].

Mauss, M. (1954) *The Gift*. Available: https://libcom.org/files/Mauss%20-%20The%20Gift.pdf. [Last Accessed: 7th October 2015].

May, C. (2002) *The Information Society: A Sceptical View*, Cambridge: Polity Press.

McCormick, E. and Sanders, M. (1982) *Human Factors in Engineering and Design*, New York: McGraw-Hill.

McDermott, S. (2010) ‘White's Three Disciplines and Relative Valuation Order: Countering the Social Ignorance of Automated Data Collection and Analysis’, *2010 International Conference on Advances in Social Networks Analysis and Mining.* Odense, Denmark 9-11 August.

McDonald, S. and Simpson, B. (eds.) (2014) ‘Shadowing Research in Organisations: The Methodological Debates’, *Qualitative Research in Organisations and Management*, 9(10), 3-20.

McKemey, K., Kimbobo, R., Scott, N., Souter, D., Afullo, T., and Sakyi-Dawson, O. *(*2003*) Innovative Demand Models for Telecommunications Services: Final Technical Report.* Department for International Development.

McQuillan, D. (2012) *Anonymous and the Digital Antinomians*. Available: http://mediasocialchange.net/2012/01/21/anonymous-and-the-digital-antinomians [Last Accessed: 6th October 2015].

Meikle, G. (2002) *Future Active: Media Activism and the Internet*, London: Routledge.

Melhuss., Mitchell, J., and Wulff, H. (eds.) (2011) *Ethnographic Practice in the Present*, New York: Berghahn.

Merton, R. (1968) ‘The Matthew Effect in Science’, *Science*, 159(3810): 56-63.

Mezrich, B. (2009) *The Accidental Billionaires: The Founding of Facebook: a Tale of Sex, Money, Genius and Betrayal*, New York: Doubleday.

Mikkonen, T., Vaden, T., and Vainio, N. (2007) ‘The Protestant Ethic Strikes Back: Open Source Developers and the Ethic of Capitalism’, *First Monday,* 12(2).

Miller, D. (2008) *The Comfort of Things*, Cambridge: Polity Press.

Miller, D. (2011) *Tales from Facebook*, Cambridge: Polity Press.

Miller, D. and Slater, D. (2000) *The Internet: An Ethnographic Approach*, Oxford: Berg.

Miller L. (1995) 'Women and Children First: Gender and the Settling of the Electronic Frontier', in J. Brooks and I. Boal (eds.), *Resisting the Virtual Life: The Culture and Politics of Information* (eds.), San Francisco: City Lights, 49-57.

Mills, C. W. (1959) *The Sociological Imagination*, Oxford: Oxford University Press.

Mitnick, K. (2012) *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker,* New York: Little, Brown and Company.

Mizrach, S. (2009) *Is There a Hacker Ethic for 90s Hackers?* Available: http://www2.fiu.edu/~mizrachs/hackethic.html. [Last Accessed: 6th October 2015].

Moody, G. (2002) *Rebel Code: Linux and the Open Source Revolution*, New York: Basic Books.

Moon, J. (1993) *Constructing Community: Moral Pluralism and Tragic Conflicts*, Princeton: Princeton University Press.

Moor, J. H. (1985) 'What is Computer Ethics', in T.W. Bynum (ed.), *Computers and Ethics,* Basil: Blackwell, 266-275.

Morozov, E. (2009) *The Brave New World of Slacktivism*. Available http://www.npr.org/templates/story/story.php?storyId=104302141 [Last Accessed 23rd August 2017].

Murthy, D. (2008) 'Digital Ethnography: An Examination of the Use of New Technologies for Social Research', *Sociology*, 42(5): 837-855.

Murthy, D. (2013) *Twitter: Social Communication in the Twitter Age*, Cambridge: Polity Press.

Nadai, E. & Maeder, C. (2005). 'Fuzzy Fields: Multi-Sited Ethnography in Sociological Research', *Qualitative Social Research*, 6(3).

Nadai, E. and Maeder, C. (2009) 'Contours of the Field(s): Multi-Sited Ethnography as a Theory-Driven Research Strategy for Sociology', in M. Falzon (ed.), *Multi-Sited Ethnography: Theory, Praxis and Locality in Contemporary Research*, New York: Routledge, 233-250.

Natriello, G. (2001) 'Bridging the Second Digital Divide: What Can Sociologists of Education Contribute?', *Sociology of Education,* 74 (3), 260-265.

Nelson, D. M. (1996) 'Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala', *Cultural Anthropology,* 11(3), 287-308.

Nycyk, M. (2010) 'Computer Hackers in Virtual Community Forums: Identity Shaping and Dominating Other Hackers', *Online Conference on Networks and Communities: Debating Communities and Networks.* Perth, Australia, 26 April-16 May. Perth WA: Department of Internet Studies, Curtin University of Technology.

Olsen, P. (2013) *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous and the Global Cyber Insurgency*, New York: Back Bay Books.

O'Neill, P. (2003) 'The "Poor Man's Mobile Telephone": Access Versus Possession to Control the Information Gap in India, *Contemporary South Asia,* 12(1), 85-102.

O'Neil, M. (2006) 'Rebels for the System? Virus Writers, General Intellect, Cyberpunk and Criminal Capitalism', *Continuum: Journal of Media & Cultural Studies,* 20(2), 225-241.

Open Knowledge International (2017) *Open Data Handbook*, Available at: http://opendatahandbook.org [Last Accessed: 8th October 2015].

Papa W.H. and Papa M.J. (1992) 'Communication Network Patterns and the Re-invention of New Technology', *Journal of Business Communication*, 29(1), 41–61.

Park, H.W. and Thelwall, M. (2003) 'Hyperlink Analysis of the World Wide Web: A Review', *Journal of Computer-Mediated Communication,* 8(4).

Paulus, P. and Nijstad, B. (eds.) (2003) *Group Creativity: Innovation Through Collaboration*, Oxford: Oxford University Press.

Pawluch, Dorothy, Shaffir, William and Miall, Charlene (2005) *Doing Ethnography: Studying Everyday Life*, Toronto: Canadian Scholars Press Inc.

Perkin, H. (1989) *The Rise of the Professional Society: England Since 1880*, London: Routledge.

Pfaffenberger, B. (1988) 'The Social Meaning of the Personal Computer: Or, Why the Personal Computer Revolution was No Revolution', *Anthropological Quarterly,* 61(1), 39-47.

Pick, J. and Sarkar, A. (2015) *The Global Digital Divides: Explaining Change*, London: Springer Heidelberg.

Pink, S. (2015) *Doing Sensory Ethnography*, London: SAGE.

Polkinhorne, D. (1988) *Narrative Knowing and the Human Sciences*, Albany: State University of New York Press.

Porat, M. (1978) 'Global Implications of the Information Society', *Journal of Communication*, 28(1), 70-80.

Porter, G., Hampshire, K., Abane, A., Muthali, A., Robson, E., Mashiri, M. and Tanle, A. (2012) 'Youth, Mobility and Mobile Phones in Africa: Findings from a Threat-Country Study', *Information Technology for Development*, 18(2), 145-162.

Poster, M. (1990) *The Mode of Information*, Cambridge: Polity Press.

Prahalad, C. (2006) *The Fortune at the Bottom of the Pyramid*, Upper Saddle River, NJ: Wharton School Publishing.

Prensky, M. (2012) *From Digital Natives to Digital Wisdom: Hopeful Essays for 21st Century Learning*, London: SAGE.

Prell, C. (2011) *Social Network Analysis: History, Theory and Methodology*, London: SAGE.

Rabinow, P. (ed.) (1984) *The Foucault Reader*, London: Penguin Books.

Rahman, H. (2009) *Selected Readings on Global Information Technology: Contemporary Applications*, London: Information Science Reference.

Random Hacks of Kindness. (2010) *Random Hacks of Kindness Website*. Available: http://www.rhok.org/ [Last Accessed: 4th December 2010].

Raymond, E. (1999) *The Cathedral and the Bazaar*. Available: http://www.catb.org/esr/writings/cathedral-bazaar/. [Last Accessed: 6th October 2015].

Raymond, E. (2000a) *How to Become a Hacker*. Available: http://www.tuxedo.org/~esr/faqs/hacker-howto.html. [Last Accessed: 6th October 2015].

Raymond, E. (2000b) *Homesteading the Noosphere*. Available: http://www.catb.org/esr/writings/homesteading/homesteading/. [Last Accessed: 6th October 2015].

Raynes-Goldie, K. (2010) 'To Catch a Predator: The MySpace Moral Panic'. *First Monday,* 15(1-4).

Rheingold, H. (1993) *The Virtual Community: Homesteading on the Electronic Frontier*. Available: http://www.rheingold.com/vc/book/. [Last Accessed: 6th October 2015].

Richardson, P. and Boyd, R. (2004) *Not By Genes Alone: How Culture Transformed Human Evolution*, Chicago: University of Chicago Press.

Richterich, A. (2017) 'Hacking Events: Project Development Practices and Technology use at Hackathons', *Convergence*, 1-27.

Ricoeur, P. (1980) 'Narrative Time', *Critical Inquiry*, 7(1), 169-190.

Riessman, C. (1993) *Narrative Analysis*, London: SAGE Publications.

Riessman, C. (2008) *Narrative Methods for the Human Sciences*, London: SAGE Publications.

Rogers, R. (2009) *The End of the Virtual: Digital Methods*, Amsterdam: Amsterdam University Press.

Rogers, R. (2013) *Digital Methods*, Cambridge MA: The MIT Press.

Rosenberg, S. (2008) *Dreaming in Code: Three Years, 4,732 Bugs and One Quest for Transcendent Software*, New York: Three Rivers Press.

Ruffin, O. (2000) *Client-Side Distributed-Denial-of-Service: Valid Campaign Tactic or Terrorist Act*. Available: http://www.fraw.org.uk/electrohippies/archive/op-01.html. [Last Accessed 02 May 2017].

Samuel, A. (2001) 'Decoding Hacktivism: Purpose, Method and Identity in a New Social Movement', *Innovations for an e-Society Congress*. Germany, October 2001. PS: Political Science and Politics.

Samuel, A. (2004) *Hacktivism and the Future of Political Participation*. PhD. Thesis. Harvard University.

Sandiford, P. J. (2015) 'Participant Observation as Ethnography or Ethnography as Participant Observation in Organizational Research', K.D. Strang (ed.) *The Palgrave Handbook of Research Design in Business and Management*, 411-446.

Sauter, Molly (2014) *The Coming Swarm*, London: Bloomsbury.

Schiller, H. (1996) *Information Inequality: The Deepening Social Crisis in America*, New York: Routledge.

Schiller, H. (2000) *Living in the Number One Country: Reflections from a Critic of American Empire*, New York: Seven Stories Press.

Schon, D., Sanyal, B. and Mitchell, W. (eds.) (1999) *High Technology and Low-Income Communities*, Cambridge, MA: MIT Press.

Scott, J. (2000) *Social Network Analysis: A Handbook*, London: SAGE.

Scott-Jones, J. and Watt, S. (2010) *Ethnography in Social Science Practice*, New York: Routledge.

Segan, S. (2000a) *Female of the Spacies: Hacker Women are Few but Strong*. Available: http://www.dvara.net/hk/fewbutstrong.asp [Last Accessed 23rd August 2017].

Segan, S. (2000b) *Female Hackers Battle Sexism to Get Ahead*. Available: http://www.mujeresenred.net/spip.php?article1543 [Last Accessed 23rd August 2017].

Seymour-Smith, C. (ed.) (1986) *MacMillan Dictionary of Anthropology*, London: Palgrave MacMillan

Shah, S. (1999) 'Sources and Patterns of Innovation in a Consumer Products Field: Innovations in Sporting Equipment', *MIT Sloan School of Management Working Paper,* #410.

Shen, C. and Monge, P. (2011) 'Who connects with whom? A Social Network Analysis of an Online Open Source Software Community', *First Monday,* 16(6).

Sherry, T. (2005) *The Second Self: Computers and the Human Spirit,* Cambridge, MA: MIT Press.

Shimomura, T. and Markoff, J. (1996) *Take-Down: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw – By the Man Who Did It*, New York: Hyperion.

Shirky, C. (2002) *Half the World*. Available: http://shirky.com/writings/herecomeseverybody/half_the_world_old.html [Last Accessed: 23rd August 2017].

Shirky, C. (2008) *Here Comes Everybody*, London: Penguin.

Shulman, S.W. (2005) 'The Internet Still Might (But Probably Won't) Change Everything: Stakeholder Views on the Future of Electronic Rulemaking', *I/S: A Journal of Law and Policy for the Information Society*, 1(1), 111–145.

Shy, O. (2001) *The Economics of Networked Industries*, Cambridge: Cambridge University Press.

Silverman, D. (2013) *Doing Qualitative Research*, London: SAGE.

Silverstone, R. and Morley, D. (1990) 'Families and their Technologies: Two Ethnographic Portraits, in T. Putnam and C. Newton (eds.) *Household Choices*, London: Futures Publications.

Slater, D. (2002) 'Making Things Real: Ethics and Order on the Internet', *Theory Culture Society* 19(5/6), 227–245.

Smith, A. G. (1999) 'The Impact of Websites: A Comparison Between Australasia and Latin America', *INFO '99 Congreso Internacional de Informacion. Havana, 4-8 October.*

Smith, C.B. (2005) *Politics and Process at The United Nations: The Global Dance*, Boulder: Lynne Rienner.

Smith, M. and Kollock, P. (eds.) (2001) *Communities in Cyberspace*, New York: Routledge.

Smith, M., Rainie, L., Shneiderman, B. and Himelboim, I. (2014) *Mapping Twitter Topic Networks: From Polarised Crowds to Community Clusters*. Available: http://www.pewinternet.org/files/2014/02/PIP_Mapping-Twitter-networks_022014.pdf. [Last Accessed: 7th October 2015].

Smith, M., Shneiderman, B. and Hansen, D. (2009) *Analyzing (Social Media) Networks with NodeXL*. Available: http://hcil2.cs.umd.edu/trs/2009-11/2009-11.pdf. [Last Accessed: 6th October 2015].

Soderberg, J. (2007) *Hacking Capitalism: The Free and Open Source Software Movement*, London: Routledge.

Sokefeld, M. (1999) 'Debating Self, Identity and Culture in Anthropology', *Current Anthropology,* 40(4), 417-448.

Sollfrank, C. (1999) *Not Every Hacker is a Woman*. Available: http://www.obn.org/reading_room/writings/html/notevery.html [Last Accessed 23rd August 2017].

Sollfrank, C. (2002) *Women Hackers*. Available: http://www.obn.org/hackers/text1.htm [Last Accessed 23rd August 2017].

Stallman, R. (2002) *Free Software, Free Society.* Available: https://www.gnu.org/doc/fsfs3-hardcover.pdf [Last Accessed 23rd August 2017].

Sterling, B. (1992) *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, New York: Bantam Books.

Still, B. (2005) 'Hacking for a Cause', *First Monday*, 10(9).

Sun, Y., Ding, X., Lindtner, S. and Gu, N. (2015) 'Reliving the Past and Making a Harmonious Society Today: A Study of Elderly Electronic Hackers in China', 18th ACM *Conference on Computer Supported Cooperative Work and Social Computing.* Vancouver, Canada, 14-18 March.

Surowiecki, J. (2004) *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*, New York: Anchor Books.

Tapscott, D. and Williams, A. (2006) *Wikinomics: How Mass Collaboration Changes Everything*, London: Atlantic Books.

Tarrow, S. (2005) *The New Transnational Activism*, Cambridge: Cambridge University Press.

Taussig, M. (2011) *I Swear I Saw This: Drawings in Fieldwork Notebooks, Namely My Own*, Chicago: University of Chicago Press.

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

Taylor, P. A. (2001) ‘Editorial: Hacktivism’, *The Semiotic Review of Books,* 12(1).

Taylor, P. A. (2005) ‘From Hackers to Hacktivists: Speed Bumps on the Global Superhighway?’, *New Media & Society,* 7(5), 625-646.

The Mentor (1986) *The Conscience of a Hacker*. Available: http://phrack.org/issues/7/3.html. [Last Accessed 23rd August 2017].

Thomas, D. (2005) ‘Hacking the Body: Code, Performance and Corporeality’, *New Media & Society,* 7(5), 647-662.

Thomas, J. (2001) *Ethics of Hacktivism*. Available: http://www.dvara.net/hk/Ethics-Hacktivism.asp. [Last Accessed: 6th October 2015].

Thomas, J. (2005) ‘The Moral Ambiguity of Social Control in Cyberspace: A Retro-Assessment of the 'Golden Age' of Hacking’, *New Media & Society,* 7(5), 599-624.

Toffler, A. (1980) *The Third Wave,* London: Collins.

Torvalds, L. and Diamond, D. (2011) *Just for Fun: The Story of an Accidental Revolutionary,* New York: HarperCollins.

Toyama, K. and Dias, B. (2008) ‘Information and Computer Technologies for Development’, *Computer,* 41(6).

Tuomi, I. (2003) *Networks of Innovation: Change and Meaning in the Age of the Internet,* Oxford: Oxford University Press.

Turgeman-Goldschmidt, O. (2008) ‘Meanings that Hackers Assign to their being a Hacker’, *International Journal of Cyber Criminology,* 2(2), 382–396.

Turkle, S. (1997) *Life on the Screen: Identity in the Age of the Internet,* New York: Touchstone.

Turkle, S. (2005) *The Second Self: Computers and the Human Spirit*, Cambridge, MA: MIT Press.

Turkle, S. (2007) *Evocative Objects*, Cambridge MA: MIT Press.

Turner, F. (2006) 'How Digital Technology Found Utopian Ideology: Lessons From the First Hackers' Conference', in D. Silver and A. Massanari, *Critical Cyberculture Studies*, 257-269.

Van Maanen, J. (1995) *Representation in Ethnography*, London: SAGE.

Van Maanen, J. (2011) *Tales of the Field: On Writing Ethnography*, Chicago: University of Chicago Press.

Van Dijk, J. (2005) *The Deepening Divide: Inequality in the Information Society*, London: SAGE.

Van Dijk, J. (2006) *The Network Society*, London: SAGE Publications.

Vegh, S. (2002) 'Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking', *First Monday*, 7 (10).

Vegh, S. (2005) 'The Media's Portrayal of Hacking, Hackers, and Hacktivism Before and After September 11', *First Monday,* 10(2).

Venkatesh V., Thong J. and Xu X. (2012) 'Consumer Acceptance and use of Information Technology: Extending the Unified Theory of Acceptance and use of Technology', *MIS Quarterly*, 36(1), 157–178.

Vergeer, M., Hermans, L. and Sams, S. (2011*)* 'Is the voter only a tweet away? Micro blogging during the 2009 European Parliament election campaign in the Netherlands', *First Monday,* 16(8).

Von Busch, O. and Palmas, K. (2006) *Abstract Hacktivism: The Making of Hacker Culture*, London and Istanbul: Open Mute.

Von Hippel, E. (2005) *Democratising Innovation*, Cambridge MA: The MIT Press.

Von Hippel, E. (2007) 'Horizontal Innovation Networks – By and For Users', *Industrial and Corporate Change*, 16(2).

Walton, M. and Donner, J. (2011) 'Read-Write-Erase: Mobile-mediated Publics in South Africa's 2009 Elections', in J. Katz (ed.) *Mobile Communication: Dimensions of Social Policy*, New Brunswick, NJ: Transaction Publishers, 117-132.

Wardrip-Fruin, N. (2009) *Expressive Processing: Digital Fictions, Computer Games, and Software Studies*, Cambridge MA: MIT Press.

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

Warschauer, Mark. (2002) 'Reconceptualizing the Digital Divide', *First Monday*, 7(7-1).

Webb, S. (2001) 'Avatarculture: Narrative, Power and Identity in Virtual World Environments', *Information, Communication & Society,* 4(4), 560-594.

Weber, M. (2001) *The Protestant Ethic and the Spirit of Capitalism*. Available: http://www.d.umn.edu/cla/faculty/jhamlin/1095/The%20Protestant%20Ethic%20and%20the%20Spirit%20of%20Capitalism.pdf, [Last Accessed: 20th November 2015].

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

Webster, F. (2006) *Theories of the Information Society*, London, Routledge.

Webster, L. and Mertova, P. (2007) *Using Narrative Inquiry as a Research Method: An Introduction to Using Critical Event Narrative Analysis in Research on Learning and Teaching*, New York: Routledge.

Wetherell, M., Taylor, S. and Yates, S. (2001) *Discourse as Data: A Guide for Analysis*, London: SAGE.

Wiles, R., Taylor, S. and Yates, S. (2004) 'Researching Researchers: Lessons for Research Ethics', *Qualitative Research,* 6(3), 283-299.

Wiener, N. (1988) *The Human Use of Human Beings: Cybernetics and Society*, Boston: DaCapo Press.

Williams, R. and Edge, D. (1996) 'The Social Shaping of Technology', *Research Policy*, 25(6), 865-899.

Willis, K. (2005) *Theories and Practices of Development*, London: Routledge.

Winston, B. (1998) *Media Technology and Society: A History: From the Telegraph to the Internet*, London: Routledge.

Wittel, A. (2000) 'Ethnography on the Move: From Field to Net to Internet', *Forum: Qualitative Social Research*, 1(1).

Wohn, Y. and Na, E. (2011) 'Tweeting About TV: Sharing Television Viewing Experiences via Social Media Message Streams', *First Monday*, 16(3).

World Summit on the Information Society (2017). Available: http://www.itu.int/net/wsis/basic/why.html [Last Accessed 23rd August 2017].

Wray, S. (1998) 'Electronic Civil Disobedience and the World Wide Web of Hacktivism', *Switch,* 4(2).

Yar, M. (2005) 'Computer Hacking: Just Another Case of Juvenile Delinquency?', *The Howard Journal,* 44(4), 387-399.

Yee, D. (1999) 'Development, Ethical Trading and Free Software', *First Monday,* 4(12).

Zachary, G. P. (2004) ‘Black star: Ghana, information technology and development in Africa’, *First Monday,* 9(3).

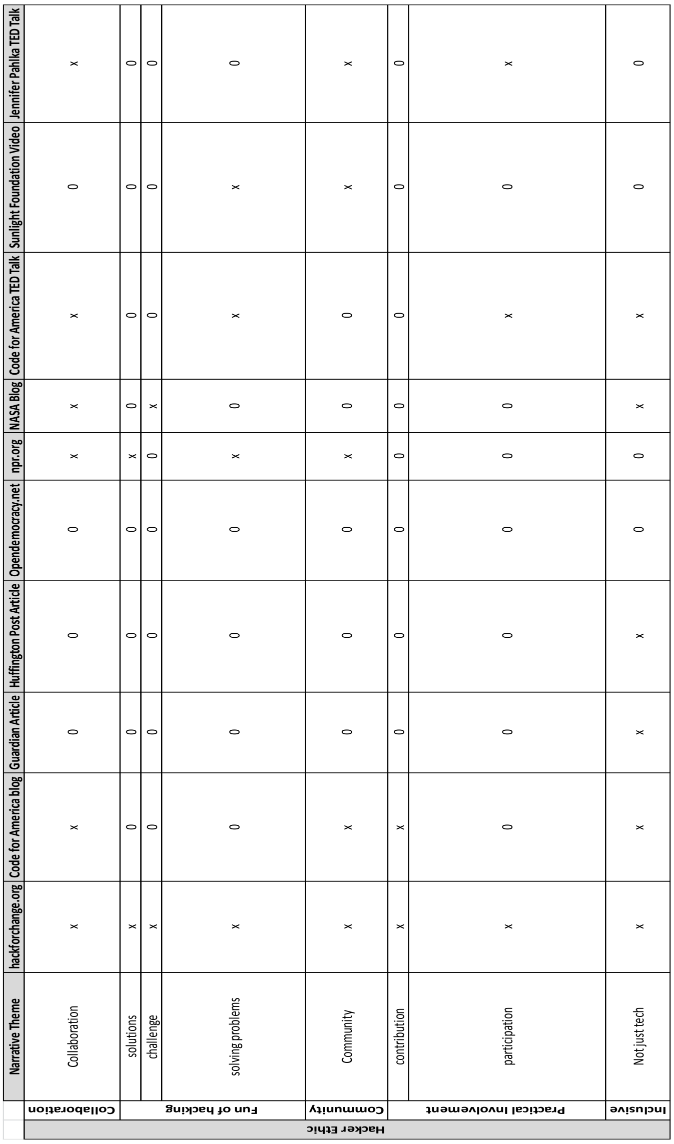
Zainudeen, A., Samarajiva, R. and Abeysuriya, A. (2006). *Telecom Use on a Shoestring: Strategic Use of Telecom Services by the Financially Constrained in South Asia*. Available at: http://www.lirneasia.net/wp-content/uploads/2006/03/Zainudeen%20Samarajiva%20Abeysuriya%202006%20teleuse%20strategies.pdf. [Last Accessed: 8th October 2015].

Zdenek, S. (1999) ‘Rising up from the MUD: Inscribing gender in software design’, *Discourse & Society,* 10(3), 379-409.

Ziegler, H. (2002), ‘The Digital Outlaws: Hackers as Imagined Communities’, *Journal of New Media and Culture,* 1(2).

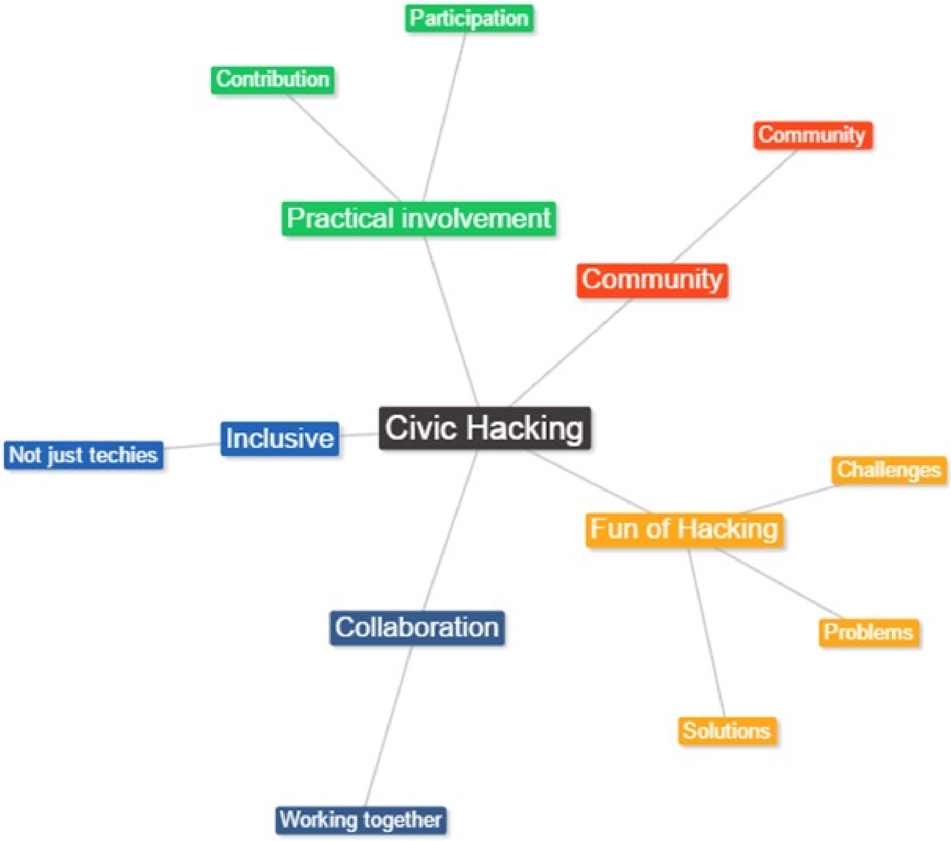
Appendices

Appendix A – Narrative Themes Mapped Against the Hacker Ethics



Hacker Ethic		Narrative Theme	hackforchange.org	Code for America blog	Guardian Article	Huffington Post Article	Opendemocracy.net	npr.org	NASA Blog	Code for America TED Talk	Sunlight Foundation Video	Jennifer Pahlka TED Talk
	Collaboration	Collaboration	x	x	0	0	0	x	x	x	0	x
	Fun of hacking	solutions	x	0	0	0	0	x	0	0	0	0
		challenge	x	0	0	0	0	0	x	0	0	0
		solving problems	x	0	0	0	0	x	0	x	x	0
	Community	Community	x	x	0	0	0	x	0	0	x	x
	Practical Involvement	contribution	x	x	0	0	0	0	0	0	0	0
		participation	x	0	0	0	0	0	0	x	0	x
	Inclusive	Not just tech	x	x	x	x	0	0	x	x	0	0

Appendix B – Hacking Narrative Themes



Appendix C – Online Narrative Data Sources

Mapped Against Themes

		Narrative Theme									
Ref	Link	bad vs good' hacking	challenges/problems/solutions	Action/pragmatism/activity/contribute	North American ideals	Democracy	Local vs global	Not just about tech/inclusion	History of technology (tech)	Support for government and sponsors	Community/together/common/collaboration/share
1	http://hackforchange.org/blog/		X	X	X		X	X		X	X
2	http://www.codeforamerica.org/blog/category/civic-hacking-2/			X	X		X	X		X	X
3	http://www.theguardian.com/cities/2014/may/29/white-house-and-nasa-gear-up-for-national-day-of-civic-hacking						X	X			
4	http://www.huffingtonpost.com/lily-liu/when-hacking-is-actually-_b_3697642.html	X						X			
5	https://www.opendemocracy.net/civic_hacking_a_new_agenda_for_e_democracy					X					
6	http://www.npr.org/2014/05/30/317361626/techies-white-house-take-part-in-national-day-of-civic-hacking	X	X				X				X
7	http://open.nasa.gov/blog/2013/05/08/what-is-a-civic-hacker/	X							X		X
8	https://www.ted.com/talks/catherine_bracy_why_good_hackers_make_good_citizens/transcript?language=en#t-97180	X	X	X	X	X		X	X		X
9	https://www.youtube.com/watch?v=kDFhzNfd-bg	X	X			X					X
10	https://www.youtube.com/watch?v=n4EhJ898r-k			X	X						X

Appendix D – Consent Form

Goldsmiths
UNIVERSITY OF LONDON

PhD Research Participant Consent Form

Department of Sociology

Goldsmiths, University of London

CONFIDENTIAL

I agree / do not agree to take part in the following research activity as part of research carried out by Douglas Haywood for use in a research based PhD at Goldsmiths College Sociology Department into 'humanitarian hackers':

I understand that;

Interviews will be to collect my views on this subject.

My identity will *not* be linked to any data collected, stored, or reported by the researcher. All identifying information associated with me will be anonymously coded and kept securely by the researcher. No other individual or party will have access to the information.

The results of the study may be published, but no individual information will be included unless approved I approve.

I will be given the opportunity to review any information relating to myself before publication.

I am free to refuse to participate in any or all of the evaluation activities. I may withdraw my participation or the data I have contributed at any time by contacting Douglas Haywood at sop02dh@gold.ac.uk.

Name (please print clearly)

Signed

Date

Please complete and sign this form (whether or not you consent to participate).

Douglas Haywood,

Many thanks for your help.

- END -