
THE UNIVERSITY
*of* EDINBURGH

# Critical infrastructure: A social worlds study of values, design and resistance in Tor and the Tor community

Ben Collier

Submitted to PhD in Law

University of Edinburgh

2019

# abstract

While cybercrime research has become well-established within criminology, there is very little criminological research which treats the infrastructures and platforms of the Internet as subjects of criminological enquiry. These are increasingly taking on responsibility for the governance of large populations of users, and the engineers and developers of these platforms are increasingly having to navigate problems of crime, harm, and policing. This thesis explores, through qualitative empirical research, an Internet infrastructure which has particularly faced these issues: the Tor Project, an anonymity network which gives millions of users around the world extremely strong protections against online surveillance and censorship. This has been an important tool for whistleblowers, journalists, and activists, however it has also become associated with a range of criminal uses, especially the rise of 'cryptomarkets', marketplaces for illegal services and goods accessible through the Tor network which are very difficult for law enforcement to shut down. I explore how the Tor community attempt to navigate these issues and how they make sense of the role Tor plays in society, drawing on interviews with members of the Tor community, including designers and developers, the people who maintain Tor's infrastructure, and others in the Tor community, as well as extensive archival research in Tor's online mailing list archives.

I use frameworks from Science and Technology Studies, in particular, social worlds theory, to explore the values of the Tor community, how they attempt to materialise them through infrastructure, and the challenges they face in practice. The Tor community, rather than sharing a strong set of shared values, is in fact a dense thicket of contradictory values and meanings. Using social worlds theory, I distil this into three internally-coherent social worlds, each of which makes sense of the work Tor does differently, rooted in differing practices, sensibilities and understandings of the political salience of privacy technology. These are: the engineer social world,

which views privacy as a structure, understanding privacy technologies as reshaping the topologies of power in information systems; the activist social world, which views privacy as a struggle and privacy technologies as part of a political movement; and finally, the infrastructuralist social world, which views privacy as a service and privacy technologies as the neutral facilitators of their users' action.

I explore the relationships between these three social worlds, how they have come into contact and conflict with one another, and how they have changed over the years. These each shape Tor's material form, its attempts to cultivate resilience against disruption by powerful actors, and how it navigates its implications in crime, harm, and power in different ways, each of which I explore in detail. Although Tor represents an attempt to act in the domain of infrastructural power, it has found that doing politics through design and engineering relies on a lot of hidden work and complex negotiation in practice, spilling out into the domains of politics, administration, and governance and becoming caught up in the very technologies of control which it tries to subvert. I end the thesis with a discussion, drawing from my empirical research, of Tor's place in the wider landscape of geopolitics and online power and how it makes sense of this. I argue that the challenges Tor faces are reflective of deeper tensions between freedom and control at the heart of liberal societies and how they are governed.

# declaration of own work

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where states otherwise by reference or acknowledgment, the work presented is entirely my own.

Parts of this work have been submitted for publication to the journals Information, Communication and Society (Chapter 6) and Science, Technology and Human Values (Chapter 7), and to an edited volume on the Human Factor in Cybercrime (Chapter 9), and are awaiting reviewer appraisal.

Ben Collier

03/12/2019

# lay summary

In this research, I studied how groups come together to build Internet infrastructure, and how they deal with the problems with crime, harm, and power, which arise. Most criminological research on the Internet to date has left the infrastructures on which the Internet relies in the background, however I bring these to the fore in order to better make sense of the role they play in crime and power in contemporary societies. I studied a particularly important example of this, the Tor network, using interviews with members of the Tor community and archival research. Tor is a network of computer servers operated by volunteers around the world, which users can access through a free-to-download piece of software called the Tor Browser. When using the Tor Browser, users' Internet signals are encrypted and bounced around the Tor network before they reach their destination. This makes it very hard for external observers to see what is going on and allows users to browse the Internet or host web services with very strong privacy and security protections. These protections prevent even law enforcement or state security services from seeing what they are doing online.

In this thesis, I use an approach developed to look at scientific and engineering projects called social worlds theory. This allows the researcher to map out the different kinds of work involved in complex technical projects, and how the people involved make sense of the project in different ways, producing a set of 'social worlds' which characterise the project. Each of these 'social worlds' is a coherent, self-consistent way of understanding the values of the technology and its purposes and is linked to a particular type of work involved in making the technology function. Contrary to what might be expected, Tor is not characterised by a strong shared set of values, goals, and perspectives. Rather, is a home for three distinct social worlds, each of which understands what Tor is doing rather differently. The 'engineer' social world, linked to the software developers and encryption experts who work on Tor,

views Tor as reshaping the landscape of power online by making changes to the structures of the Internet and the way it works. Conversely, the 'activist' social world, associated with the practices of lobbying, outreach, and policy work, sees Tor as a social movement and explicitly political. Finally, the 'infrastructuralist' social world, connected to the work of running the Tor network itself, sees Tor as a neutral service which is divorced from politics or explicit values.

I explore in depth how these three social worlds fit together and manage this conflict and consensus, and how this is changing over time as they begin to shape and influence one another. These three worlds are able to work together despite these conflicts due to key individuals who can translate between these perspectives. They are helped in this by the ways in which the worlds overlap, as they share a common set of category systems for Tor's users which allows them to leave the politics of Tor ambiguous. When cultural changes cause this arrangement to break down, the worlds shift and change as well.

In addition to exploring and mapping these different ways of making sense of Tor, I study how the values of the people who make Tor influence the way the technology works. I use Tor's open archives, including mailing lists which document the early design work of Tor, to study how the developers try to realise their values in the way that Tor's infrastructure is designed. I show that ideas of what Tor was and how it should work developed iteratively throughout the processes involved in developing Tor's design. The engineer world's understanding of Tor as restructuring online power arose from this design process.

However, design and development work is not enough to make Tor's visions of a private Internet a reality on its own. Tor relies on an infrastructure of relays to work, and so depends on a great deal of maintenance and administration work as well. This work has its own values and perspectives: those of the infrastructuralist social world. I explore this work in depth, and how it is related to Tor's design. In particular, I discuss how Tor tries to defend itself against attack by nation state secret services as an example of how design is not always enough on its own.

Finally, I take these maps of Tor's values, the kinds of work involved in making it possible, and the perspectives of its community, and use them to understand how Tor becomes involved in issues of crime and harm. Although Tor's community intend it to be used for socially beneficial use cases and to fight online surveillance, some people use its privacy protections to commit crime. This causes problems, both for its public image, and for the people who run its infrastructure, who can sometimes come to the attention of the police. Each of Tor's three social worlds adopts a different strategy for coping with these problems. The activist world seeks to strongly assert Tor's values in public. The infrastructuralist world, by contrast, tries to withdraw Tor from these discussions about values and politics, relying instead on clever mechanisms and legal loopholes to allow the network to run smoothly. Finally, the engineer world looks to get Tor incorporated into other technologies as a security standard, allowing it to become so ubiquitous that it becomes simply a part of how the Internet works.

I argue that criminology could usefully use the social worlds framework to better understand the role played by Internet infrastructure in issues of crime and power, as this allows researchers to develop a very deep understanding of infrastructures as sites where many different perspectives and visions of future worlds can be worked out in different ways.

# acknowledgements

I would firstly like to extend my heartfelt thanks to the Tor Project, the Tor community, and all those who contributed their time and participation to the research. This PhD would not have been possible without the enormous kindness and generosity of the Tor community, and I am deeply grateful for the opportunity to speak to so many people. I would also like to thank the members of the Tor developer community who have contributed to the mailing lists over the years for the humour and wit which punctuates these enormous, dry technical discussions. These interventions made the experience of reading these vast archives substantially more bearable, and often even enjoyable. Coleman (2013) has written before of the importance of humour in hacker culture and practices, and the Tor developer community is by no means an exception. I am immensely grateful to the people who agreed to be interviewed for this project, and hope that I have done their contributions justice, represented them fairly, and done something to bring the more hidden perspectives in Tor to wider light. It has been my wish to represent the contributions from the Tor community in this research in good faith, bringing to the surface hidden perspectives and fairly portraying the ways in which the people to whom I spoke make sense of Tor. Any errors in representation are mine.

A number of other people helped me a great deal throughout this research. Firstly, I wish to thank my supervisors, Richard Jones and James Stewart, for their advice, support, and guidance throughout the PhD. This guidance, our discussions, and their comments on the writing have done a great deal to shape the form it takes and have made it a substantially better piece of work. This PhD would not have been possible without them, and I am also deeply grateful to Richard for his mentorship and guidance in the early days of my criminological education. I am also very grateful to the other law school and SPS academics who helped me throughout my Master's

and my PhD, and who gave me a deep love for the subject. I am also very grateful to those who gave me comments on draft papers associated with the thesis. Additionally, I would like to thank my colleagues at the Cambridge Cybercrime Centre for their support and friendship over the last year, and for reading through and discussing some of the ideas in this thesis.

I would also like to thank my parents, brother, and sister, and the rest of my family for their support, love, and friendship throughout the past four years, and my non-criminological friends, particularly Gareth, Joss and Anna, Adam and Artemis, Kapil, Cammie and Alice, Jono, John and Trina, Richard and Claire, Brian and Craig, Melissa, and Michael, whose friendship and support have meant a great deal to me throughout the thesis.

To another set of friends I would like to extend particular thanks: my crim colleagues and friends, especially Louise Brangan, Ben Matthews, Shane Horgan, and Jamie Buchan. I have learned as much about criminology, social theory and academia from our coffees, chats standing in the Mezzanine Office kitchen, and long drinking sessions as I have anywhere else. Thanks also for all the discussions of the theory I use herein, for your comments on draft pieces of work, and for your friendship over the past several years.

Finally, I thank Jamie Buchan, my partner and (at the time of writing!) soon-to-be husband. Your love, friendship, generosity, and kindness has sustained me over the past four years, and this would have been impossible without you. Thanks for looking over so much of the thesis, for your help and ideas, and for listening to me talk about Tor incessantly for four years.

# contents


ABSTRACT 3

DECLARATION OF OWN WORK 5

LAY SUMMARY 7

ACKNOWLEDGEMENTS 11

CONTENTS 13

CHAPTER 1 - INTRODUCTION: VISIONS OF PRIVACY, POWER, AND CONTROL 19

INTRODUCTION AND BACKGROUND 19

TOR: ENVISIONING A FREE INTERNET 22

THESIS STRUCTURE 25

CHAPTER 2 - CRIMINOLOGIES OF THE INTERNET 29

INTRODUCTION 29

CYBERCRIME, CRIMINOLOGY, AND TECHNOLOGY 30

CRIMINOLOGY AND ACTOR-NETWORKS: TRACING SOCIO-TECHNICAL AGENCIES WITH ANT AND RAT 35

MEANING AND THE MATERIAL 37

GOVERNMENTALITY, POWER AND DISCOURSE 41

TECHNOLOGIES OF ONLINE CONTROL AND INFRASTRUCTURAL RESISTANCE 44

THE TOR NETWORK – CRITICAL INFRASTRUCTURE 48

CONCLUSION 51

CHAPTER 3 - A GENEALOGY OF TOR (AND A SOCIAL HISTORY OF THE INTERNET) 53

INTRODUCTION 53

**THE INTERNET AND ITS DISCOURSES** **55**

INTERNET PREHISTORY – MILITARY, SOVEREIGNTY, AND THE SCIENTIFIC ELITE 55

HACKERS AND CYBER-LIBERTARIANISM 56

THE NEOLIBERAL INTERNET 61

WAGING THE CRYPTOWARS – THE INTERNET AS A CRISIS OF CONTROL 64

**ONION ROUTING AND TOR** **66**

ONION ROUTING – ANONYMITY LOVES COMPANY 66

THE BIRTH AND EARLY LIFE OF TOR 70

**THE RISE OF CONTROL** **75**

THE SNOWDEN LEAKS AND MASS SURVEILLANCE OF THE INTERNET 75

SURVEILLANCE CAPITALISM AND THE NEW PLATONIC GUARDIANS 79

**CONCLUSION** **82**

**CHAPTER 4 - THEORISING THE SOCIAL LIFE OF INFRASTRUCTURE 87**

**INTRODUCTION** **87**

**MATERIAL PRIVACY – INTERNET INFRASTRUCTURE AND STEALING THE FIRE** **89**

**SOCIAL WORLDS** **93**

THE FOUNDATIONS OF SOCIAL WORLDS THEORY – SYMBOLIC INTERACTIONISM 93

THE SOCIAL WORLDS APPROACH 98

SENSITISING CONCEPTS 100

**MAKING THE LINK FROM MEANING TO THE MATERIAL** **104**

EMBEDDING VALUES IN TECHNOLOGY 104

HOW TECHNOLOGY SHAPES THE WORLD 109

**CONCLUSION** **112**

**CHAPTER 5 - EXPLORING THE VALUES OF AN INFRASTRUCTURE: METHODOLOGY, ETHICS, FIELDWORK AND ANALYSIS 115**

**INTRODUCTION** **115**

**RESEARCH QUESTIONS AND STRATEGIES** **119**

RESEARCH QUESTIONS 119

QUALITATIVE RESEARCH WITH TECHNOLOGICAL PROJECTS 121

**INSTRUMENT DEVELOPMENT AND DATA SOURCES** **123**

Interview design and practices 123
Tor's archives 127
**Fieldwork and data generation** **129**
Early steps 129
Developing trust 132
Moving forward: fieldwork details and data collection 135
Bringing in the material and ending fieldwork 138
**Ethical considerations** **140**
Ethics in Internet research 140
Anonymity for experts 145
Safety, power, and harm 147
**Analysis** **151**
Analysis in the social worlds framework 151
Coding and mapping 152
**Conclusions and methodological reflections** **156**

**CHAPTER 6 - THE SOCIAL WORLDS OF TOR** **159**

**Introduction** **159**
**Mapping the Tor community and infrastructure** **160**
**Privacy at the heart – Tor's values** **163**
**Privacy worlds** **165**
Engineers: privacy as a structure 167
Infrastructuralists: privacy as a service 170
Activists: privacy as a struggle 174
Relational perspectives 177
**Collaboration, conflict and transformation** **180**
Privacy as a boundary object 180
Cultural change and boundary breakdown 184
**Conclusions** **187**

**CHAPTER 7 - GROWING ONIONS: TOR, VALUES AND DESIGN** **189**

**Introduction** **189**

ONION ROUTING: A TECHNICAL DESIGN AND A VALUE SYSTEM 190
IMPLEMENTING ONION ROUTING - TOR'S CONSTRUCTION OF PRIVACY 192
**EXPLORING THE DEVELOPMENT PROCESS IN TOR 196**
DECOMPOSING PRIVACY VALUES AND RECONSTRUCTING PRIVACY PROPERTIES 196
GROWING A SOCIAL WORLD 201
**REVISITING TOR'S DESIGN IN A POST-SNOWDEN WORLD 203**
THE RETURN OF PADDING 203
A SHIFT IN THE ENGINEER SOCIAL WORLD 206
**CONCLUSION 210**

**CHAPTER 8 - OPEN SECRETS, HIDDEN WORK 213**

**INTRODUCTION 213**
**TECHNOSOCIAL THREATS AND DESIGNING A COMMUNITY – RESILIENCE THROUGH OPENNESS AND DECENTRALISATION 214**
RADICAL OPENNESS 216
DECENTRALISATION AND NON-HIERARCHICAL STRUCTURES 220
NEGOTIATING COMMUNITY DESIGN IN PRACTICE 222
**TECHNICAL THREATS AND THE HIDDEN WORK OF TOR: ADMINISTRATION AND MAINTENANCE AS RESILIENCE PRACTICES 229**
BEYOND DESIGN: HIDDEN WORK AND THE TOR INFRASTRUCTURE 230
MAINTENANCE AS RESILIENCE PRACTICE: "IS THIS GOING TO BE A STAND-UP FIGHT OR ANOTHER BUG HUNT?" 232
**CONCLUSION 236**

**CHAPTER 9 - ALLERGIC TO ONIONS? TOR, CRIME, POWER AND HARM 239**

**INTRODUCTION 239**
**THE DARKNET, CRIME AND MORAL REACTION 240**
**TANGLING-UP IN TECHNOLOGIES OF CONTROL 243**
**STIGMA AND THE TARNISHING OF THE 'FREE INTERNET' 247**
**BROADER STAGES OF POWER 250**
**NAVIGATING CRIME AND POWER AS A REBEL INFRASTRUCTURE 252**
**PRIVACY AS A STRUGGLE: THE *ACTIVIST* WORLD AND RECLAIMING TOR 254**

**PRIVACY AS A SERVICE: THE *INFRASTRUCTURALIST* WORLD AND BECOMING INVISIBLE** **257**

**PRIVACY AS A STRUCTURE: THE *ENGINEER* WORLD FROM SUBVERSION, TO STANDARDISATION, TO SOVEREIGNTY** **261**

FROM SUBVERSION TO STANDARDISATION 263

FROM DISRUPTION TO SOVEREIGNTY 265

**CONCLUSIONS** **269**

**CHAPTER 10 - DISCUSSION: TECHNOLOGIES OF POWER AND THE POWER OF TECHNOLOGY** **271**

**INTRODUCTION** **271**

**DESIGNING PRIVACY** **273**

**HIDDEN WORK AND HIDDEN WORLDS** **278**

**TRANSFORMING WORLDS AND THE SOVEREIGN ONION** **283**

**BROADER QUESTIONS OF CRIME AND POWER** **288**

**INFRASTRUCTURAL CRIMINOLOGY** **295**

**CONCLUSIONS** **298**

**CHAPTER 11 - CONCLUDING REMARKS AND REFLECTIONS: PRIVACY WORLDS** **301**

**INTRODUCTION** **301**

**KEY CONTRIBUTIONS OF THE THESIS** **303**

**REFLECTIONS ON LIMITATIONS AND AVENUES FOR FUTURE WORK** **304**

**FINAL REMARKS** **308**

**BIBLIOGRAPHY** **311**

**APPENDIX A – LIST OF PARTICIPANTS** **345**

**APPENDIX B – SITUATIONAL MAP** **345**

**APPENDIX C - SOCIAL WORLDS TIMELINE** **347**

**APPENDIX D - SOCIAL WORLDS MAP - DISCOURSE AND PRACTICES** **348**

**APPENDIX E – RESEARCH QUESTIONS MAP – DESIGN, WORLDS, AND HIDDEN WORK 3480**

**APPENDIX F – RESEARCH QUESTIONS MAP - CRIME 348**

# chapter 1
# introduction: visions of privacy, power, and control

## Introduction and background

This PhD arose from a deep interest in the technologies, infrastructures, and platforms which make up the Internet and the role they play in society. For most of my life, the Internet has been a subject of controversy. Being born in 1989 and with my family getting our first Internet-connected computer in around 1995, I am part of the generation who has 'grown up' along with the Internet as a central part of social, economic, and political life. I have been fascinated by hackers and hacking since I was a small child, getting my first computer (a ZX-81 Spectrum) at a young age and spending much of my free time growing up teaching myself to program.

When coming to university, my original undergraduate degree and first Master's degree were in Chemistry. Although the realities of a career in lab-based research did not appeal, I developed a keen interest in how technological and scientific projects work. Throughout this period, however, I had been becoming increasingly involved in antifascist, LGBTQ+, and feminist activism. This had exposed me to a range of different perspectives and ways of making sense of the world, and I began to develop an interest in social theory, first through reading Queer theory to make sense of my own experiences and the social issues I was trying to campaign on, and then as part of a broader interest in understanding social life.

Following my Chemistry degree, I made the switch to a criminology Master's in order to further go down this path. I particularly enjoyed a course I took on cybercrime research, however, digging into the literature, I became frustrated at the approach which much criminological research at the time took to theorising or accounting for technology in making sense of cybercrime. These studies tended to allow the technologies and infrastructures of the Internet to slip into the background, either relegating them to the status of 'social spaces' or 'situations' in which human action occurs, casting them as possessing technical properties which deterministically shape human behaviour and societies, or falling back on descriptions of the Internet as a kind of hyperspace which 'reduced time and space to zero' without any engagement with their mundane (but important) technical realities and real material qualities.

I was interested in the potential for Science and Technology Studies (STS) to engage with technologies as sites of social action in their own right. In particular, a formative influence on this research was a paper by Sheila Brown (2006), which argued for the incorporation of sensibilities and approaches from Actor-Network Theory (ANT) into criminological research, particularly its breaking-down of prescriptive boundaries between object and subject, human and technical, meaning and the material. In my Master's project, and in the early work of my PhD, I wanted to engage this more programmatically, working out how ANT might further deepen criminological understanding of technology. However, as I progressed, I found myself drifting away from ANT, eventually finding a home elsewhere within STS. In particular, a paper by Thomas Pinch (2010) which called for research on the Internet infrastructure grounded in symbolic interactionism, and my reading of Donna Haraway's scholarship (1991) led me to the social worlds framework and the scholarship of Susan Leigh Star (1999), which form the core of this thesis.

Social worlds theory, and Star's related infrastructure studies work, draws on symbolic interactionist frameworks to cast technologies and infrastructures as sites of social action, permeable to a range of different meanings and visions of the world

(Star, 1999; Clarke and Star, 2008). This framework focuses on the role of communication and interpretation, and the different kinds of work and mediations between meaning and materiality through which these infrastructures 'produce' or 'perform' social facts like privacy. It involves deep, qualitative research, mapping the different 'worlds' of discourse, practices, and sensibilities which form around infrastructures and scientific projects through interviews and archival research. In trying to draw this into criminology, I aimed to use this approach in this thesis to explore how technologies and infrastructures become implicated in power, governance, values, and visions of alternative futures.

Towards the middle of my first year of the PhD programme I decided to focus on a particular case study, having wanted to carry out empirical research rather than write a purely desk-based thesis. I quickly settled on Tor, a free-to-access online anonymity network which has become a particularly controversial site where debates about crime and control online are being worked through. This was partly due to my own interests in online privacy, which had been galvanised by the Snowden leaks in 2013 (Lyon, 2014). I judged that Tor would provide an ideal case study for the application of social worlds theory within criminology, occupying as it does such a contested space between the exercise of governmental power over the Internet and the attempts of people to resist this. It has also been relatively under-researched within sociological and criminological scholarship, which focuses almost exclusively on Tor's users, rather than the people who support and develop it. I was interested particularly in Tor as a site of social action: a form of resistance to authoritarian power and an attempt to realise a different vision of the Internet through infrastructure. I argue that although Tor is undoubtedly of deep importance to global society and the future of the Internet, the ideas, discourses, and types of work involved in its attempt to reshape this future are relatively taken-for-granted. As part of the underpinnings of public and private life for its millions of users, it is of deep democratic importance for us to understand what decisions are being made about how infrastructures like Tor work, how those decisions are made, and their broader situation in relationships of power and online governance.

## Tor: envisioning a free Internet

At the heart of this thesis is social worlds study of the Tor network. The Tor network is an infrastructure of servers, operated by volunteers around the world, which are accessed by users through a Web browser called the Tor Browser. The Tor Browser can be downloaded for free by anyone who is able to access the website of the Tor Project, the organisation which develops and maintains Tor. Tor provides its users extremely strong anonymity and security protections, preventing even nation states from surveilling or censoring their web traffic. It does this by wrapping the administrative information which this traffic uses to traverse the Internet in three layers of encryption before bouncing this around its network of 'relays' distributed around the world, preventing surveillance by even very powerful adversaries (Dingledine, Mathhewson, and Syverson, 2004).

In doing so, Tor realises a vision of an Internet very different to the one to which we have become accustomed. This is an Internet more similar to that envisioned in the 1990s, where anonymity from the powerful is possible, chaotic and creative communities proliferate, illegal markets which defy regulation, whistleblowers, and resistance movements operate under the radar of law enforcement, all, of course, with (slightly) slower connection speeds. When using Tor, one sees the Internet from a more global perspective, as adverts no longer know where you're from, services can't tailor content on the basis of your location, and the 'filter bubbles' created by services such as Google lose their grip on us, as Tor breaks the mechanisms they use to track and surveil our intimate lives and thoughts across the Internet. Although Tor began as a project of the US military's Naval Research Laboratory, it is now in the hands of civil society and is at the forefront of resistance and reaction to the practices of mass surveillance revealed in the Snowden leaks, the rise of *surveillance capitalism* in the hands of the Internet giants, and more generally to technocratic, authoritarian modes of governing contemporary societies through engineering, automated surveillance, and 'smart governance'.

Tor has largely come to the attention of criminological research in the guise of the 'Dark Web'. As a powerful antisurveillance technology, which also allows the creation of web services which are extremely difficult to locate and take down, Tor has become associated with a range of illegal use cases, particularly 'cryptomarkets', online anonymous marketplaces for illegal goods which are accessed through Tor. This illegal conduct on Tor (and increasingly, the Internet more broadly) is often referred to in media accounts as the 'Dark Web' or 'Dark Net', and has become somewhat of a media sensation, with TV shows, films, and even music videos all painting Tor as a digital demimonde: a dangerous place outside the control of law enforcement. This creates substantial issues for the Tor community, whose work is animated by values of liberation, privacy, and democracy. I contend in this thesis that framing Tor as a 'criminogenic' tool (as much of the criminological literature has) misses out far more interesting potential facets of Tor for criminological research. Tor poses extremely important questions about governance, harm, crime, and power online. Through understanding Tor as an infrastructure and exploring it as a site of social action, I argue that a social worlds approach has the capacity to unearth important aspects of justice and power at play.

I particularly draw on the work of three other scholars in contextualising this thesis: Stefania Milan's concept of "stealing the fire" (Milan, 2016), Francesca Musiani's (2012) explorations of how engineers "do politics" through architecture , and Gabriella Coleman's (2017) "weapons of the geek". Coleman and Brunton 's (2014) call to get "closer to the metal", and Musiani's to engage in research on Internet infrastructure that "isn't afraid of its subject" (Musiani, 2012) are also important in animating this thesis. Coleman, Musiani, and Milan each engage in deep, appreciative study of technology and infrastructure (and the people embedded in them) and their links to social change. They each approach this work from different perspectives, interested in a distinct facet of technological work and its attendant practices, sensibilities, and framings of technology as a site of social action. For example, Coleman (2017) foregrounds the creative, subversive sensibilities and practices of hackers, and tracks their rise to prominence as key political actors in

contemporary societies, playing with technologies, laws, and systems to repurpose them to their own ends. Musiani (2012), conversely, studies the mass-scale infrastructure of the Internet itself and how its engineers shape society in important ways through decisions made about its architecture. Finally, Milan (2016) focuses on technology and infrastructure in more explicit social movements, and how the practices and values of these activist-technologists attempt to perform and realise particular political values and visions of society.

Each of these framings reveals a great deal about Internet infrastructure and the role it plays in contemporary societies, and I draw from them throughout the thesis. However, instead of adopting one of these perspectives from the outset, I aim to map Tor as a site at which multiple different kinds of social action are attempted. I do this through appreciative, qualitative research, including interviewing members of the Tor community and deep archival study of the Tor Project's open access online archives. In doing this, I wanted to move beyond the majority of the criminological research on Tor, which focuses on the illegal behaviours of some of its users, to the largely hidden perspectives of the people behind the infrastructure. In finding out what they wanted to achieve with Tor and how they went about realising these visions, I have tried to characterise Tor as a home for multiple overlapping social worlds and kinds of social action.

In doing this, I have structured this research around a set of four main research questions, which I outline here:

1. In what different ways do the people who contribute to Tor make sense of it as a site of social action, and what different visions of privacy do these understandings evoke? In other words, what are the key social worlds of the Tor community, how do they relate to one another, and how do they come into conflict, conversation, and collaboration?
2. How do these social worlds shape the material form and design of Tor; how are these values realised as properties of the Tor network?

3. When this design is materialised as infrastructure, what other kinds of work are needed so that this infrastructure can create Tor's visions of privacy in the world, especially given the considerable opposition it faces?
4. What problems with crime, power and harm arise when Tor begins to realise its visions? How does the Tor community make sense of these issues, and through what strategies does it navigate them?

These questions evolved across the course of my PhD research, and I describe how I arrived at them in more detail in Chapter 5.

## Thesis structure

In Chapter 2, I outline the context of this research and how it fits into the broader criminological literature on the Internet. I discuss what I see as the main gaps in criminological research which I set out to explore in this thesis, in particular how it frames and accounts for technology and infrastructure. I discuss some of the ways in which criminology has begun to move towards 'situational' approaches to making sense of the Internet, in particular Routine Activities Theory and, to a lesser extent, Actor-Network Theory, and draw out what I see as the limitations of these approaches. I then make the case for a different branch of STS research, social worlds theory, to shed light on what some of these frameworks may be missing. I set out Foucault's concept of governmentality in order to sketch the broader theoretical context of this research and describe some of the specific issues which apply to Tor and the current state of criminological research on the so-called 'Dark Web'.

In Chapter 3, I set out the historical context of Tor, mapping out a history of the Internet and the discourses and ideas which have shaped it. I trace the Internet's roots in military research through to its opening up to commercial and personal use, outlining how it has been shaped by military, neoliberal and countercultural ideas among others. After discussing the rise of different strains of 'hacker' politics and

how they have fed into the development of the Internet, I turn to the conflicts in the 1990s over encryption technologies, and bring Onion Routing, Tor's precursor, into this history. I then discuss Tor's early development and growth, and the rise of technologies of online control documented in the Snowden leaks. Finally, I end this chapter with a discussion of the current issues facing the Internet and where Tor fits into them.

Chapter 4 outlines the theoretical underpinnings of this thesis, setting out the social worlds framework and how I make use of it. I begin with a discussion of research on privacy, positioning this thesis as an exploration of how Tor realises particular visions of privacy in practice through infrastructure. I then set out some of the foundational literature in the symbolic interactionist school, which forms the basis of the social worlds approach. Following this, I discuss the social worlds framework in depth and the key approaches and sensitising concepts on which I draw in this thesis.

Having set out the context of my research, the key research problems, and the theoretical underpinnings of this thesis, I set out my methodological approach in Chapter 5, giving an account of my fieldwork and analysis, and discussing the ethical issues which I considered throughout the research. I also set out my four core research questions and discuss how they fit into the social worlds approach.

I then devote four chapters to the results of my empirical research, one addressing each of my four main research questions. In Chapter 6, the first of my 'results' chapters, I begin by exploring in more depth the Tor's project's core values and the vision of the world it is trying to realise. Rather than a single core value system, Tor's values are heterogeneous, with its community drawing on a range of different understandings of the status of Tor, and privacy technology more generally, as a social actor. I distil these into three ideal type social worlds and explore how they collaborate, conflict, and shape one another.

Having mapped in depth the social worlds of the Tor community, I then, in Chapter 7, map the processes through which they attempted to enact these in practice. In

particular, I explore the ways in which Tor's *engineers* attempted to *do politics through architecture* by creating an infrastructure which not only embodied their values but aimed to make them a reality for Internet users around the world. This turned out in practice not to be a simple act of translation, and the developers' motivations and understandings of Tor were shaped as much by these design and development processes as the infrastructure itself was. I then discuss how the engineer world and its design practices have changed since the early days of Tor.

Having set out Tor's values and vision of the world and how it attempts to realise this through infrastructure, I then spend the two chapters which follow, Chapters 8 and 9, exploring what happens when this infrastructure actually meets the world it is attempting to transform.

In Chapter 8, I discuss how the ideas embedded in Tor's design are materialised in the world in practice and the hidden work which helps make them a reality. As an oppositional infrastructure aimed at disrupting the control which powerful actors wield over the Internet, and a system which carries extremely sensitive traffic, Tor is an opportune target for nation states, organised crime groups, and security companies whose resources far exceeds the few million dollars a year on which it can draw. In this chapter, I explore how Tor attempts to defend against these threats against both its community and its technologies. Through this, I illustrate how the design ideas embedded in Tor in fact rely on hidden work to be realised, which carries with it its own perspectives and values.

In my final 'results' chapter, Chapter 9, I explore what happens when Tor's attempts to wield infrastructural power meet problems with crime and harm, becoming caught up in the technologies of control which they are trying to disrupt. I map the challenges which Tor faces in practice, and how it becomes tangled up in administrative and criminal justice systems in a variety of ways. I follow this with an account of how the different social worlds of Tor understand its implication in harm and illegal activities, and the strategies which they use to assert their own claims to Tor's social meaning and vision of the Internet. Unlike most infrastructures and

platforms, Tor cannot govern crime and abuse through design, through self-policing and moderation, or through working with criminal justice organisations, as its design removes the 'control points' on which these rely. I discuss in depth in this chapter how it attempts to deal with and make sense of these problems.

In Chapter 10, I pull the different threads of my results chapters together into a discussion of Tor as a site of social action, drawing out the key themes which link my research questions together. I begin by discussing the role of design in Tor, and how this mediates between constructions of crime, privacy, and control, the material features of Tor, and its attempt to 'do politics through architecture'. Next, I discuss the ways in which these visions are produced in practice, the other perspectives which this brings in, and how this links to Tor's relationship with crime and harm. I then discuss how these social worlds and visions are changing, in part in reaction to the issues which Tor faces, especially its shift towards a more 'governmental' sensibility. In the next section, I draw these together into a discussion of how Tor fits into broader questions of power and governance. Finally, I make the case for an 'infrastructural criminology' which engages in appreciative, qualitative exploration of the infrastructures and platforms on which our societies depend.

I conclude the thesis, in Chapter 11, with some reflections on the contributions of the research and its limitations, outlining potential avenues for future work.

# chapter 2
# criminologies of the Internet

## Introduction

In this chapter, I set out the gap in scholarship which I explore in this thesis. I discuss the key literature which informs this thesis and set out the core questions which it aims to answer. This is not an in-depth exploration of my theoretical approach, which I leave to Chapter 4, rather it is an attempt to position this research within the broader fields of criminological, digital society, and Science and Technology Studies scholarship, and within the research literature on Tor.

I begin this chapter by setting out the current state of cybercrime scholarship and the broader criminological research which touches on the Internet, arguing that while there has been a great deal of excellent qualitative research on cybercrime, this has tended to neglect the social life of the technologies, platforms, and infrastructures of the Internet. These have been allowed to fade into the background, and with them key issues of power, crime, and control in contemporary societies. I set out some of the ways in which criminological scholarship has attempted to account for this, in particular using Latour's Actor-Network Theory, and some of the limitations of this approach. I then present a possible route forward, drawing on Susan Leigh Star's (1989) developments of the social worlds framework, which has proven fruitful in disentangling the complex, heterogeneous meanings and discourses which become enmeshed in technological infrastructures.

I then situate these in broader frameworks for understanding the links between discourse, power and control, discussing the work of Michel Foucault and focusing on his concept of *governmentality* and how it has shaped criminological scholarship, in particular its tracing of the links between discourse, materiality, and power. I then discuss the relevance of this framework to the Internet, and the groups which are attempting to resist this through building their own infrastructures. I argue (drawing on separate work by Milan, Coleman, Musiani, and Star) that these groups are particularly worthy of study in exploring power in the Internet age, situated as they are between state attempts at online control and the people on whom they act, and engaging in deliberate attempts at oppositional action in the domain of material power. I then discuss the focus of this thesis, the Tor Project, setting out some background and the existing research which has studied Tor. I end this chapter with a brief summary of the gaps in criminological literature which I explore in this thesis.

## Cybercrime, criminology, and technology

The spread of the Internet throughout human social, economic, and political life has posed vital questions for criminologists about the relationship between technology, infrastructure, crime, and power. Since before the turn of the current millennium, a growing body of criminological research has attempted to make sense of the apparently-novel types of crime which occur in contemporary Internet-embedded societies (Wall, 2007; Yar and Steinmetz, 2019). Much cybercriminal theoretical work has been concerned with whether the rise of cybercrime constitutes a 'novel' form of crime, or simply technologically-mediated versions of well-established phenomena. This 'old wine in new bottles' debate (Wall 1999, Grabosky 2001) is still fairly contentious within cybercrime research (Wall 1999; Yar 2005; Wall 2007). Cyber-criminology, or criminological research on cybercrime, has developed into a substantial sub-discipline over the past twenty years (Holt 2013; 2014). This has progressed from initial descriptive and framing work to a wider subfield of research, which, like criminology itself, is multi-disciplinary and brings in many types of expertise from other fields, including security researchers, statisticians, engineers

and anthropologists (and many more). This has involved substantial theoretical work, both through the development of novel theory and attempts to apply established criminological frameworks, such as differential association (Hutchings and Clayton, 2016; Bohman and Freng, 2017), feminist criminology (Hutchings and Chua, 2016; Lazarus, 2019), and radical criminology (Steinmetz, 2016) to cybercrime. In more recent years, this subfield has begun to break its boundaries, with a range of other areas of criminological study attempting to reckon with the Internet and how it affects their own subjects of enquiry. In scholarship on electronic monitoring (Nellis, Beyens, and Kaminsky, 2013), probation (Mair, 2013), border criminology (Milivojevic 2019a, 2019b), prisons (Jewkes, 2008) and policing (Wall & Williams, 2013; Dodge, Spencer, and Ricciardelli 2019), to give only a small selection, Internet technologies are playing increasingly important roles.

However, this thesis is not about 'cybercrime', about which a substantial literature clearly exists. Rather, I am interested in what the particular standpoint of criminology might be able to reveal about the technologies of the Internet themselves, and how they shape crime, power, and control. These 'deeper' elements of the Internet include the platforms designed and curated by companies such as Google, Facebook, and Twitter which mediate much of our online interaction, and the yet deeper world of protocols, Internet Service Providers, Internet exchanges, and the material infrastructure of cables, switches, and software. They incorporate important decisions about human action which shape our societies in ways which are still poorly-understood (Lessig, 1999a, 1999b; Lievrouw and Livingstone, 2002; Mackenzie, 2005; Healy, 2015; Musiani, 2015; Milan and ten Oever, 2017). Contrary to framings which describe the Internet as 'cyberspace', 'reducing time and space to zero' (Benedickt, 1991; Introna, 1997) or a transcendental 'digital dimension', the Internet does not work by magic, nor is it divorced from the material. In fact, it is composed of a myriad of different material technologies, infrastructures and platforms built atop and alongside one another, which all have their own properties and histories (Musiani, Cogburn, DeNardis and Levinson, 2016). This means that an understanding of the salience of the Internet for social life has to take into account

this complex landscape of infrastructures which are not all pulling in the same direction or working towards the same ends, in fact underpinned by often contradictory or opposed values and visions of the world. These infrastructures can both embed profound mechanisms of social control and constitute powerful attempts at resistance. Exploring these dynamics, however, requires a move beyond the existing frameworks through which criminology makes sense of technology.

There has been relatively little criminological scholarship on the infrastructures of the Internet, despite the fact that criminology is well-suited to exploring questions of power, governance and control which are deeply salient here. This work has largely been left to fields outwith criminology. Surveillance studies, for example, has shown pathbreaking critical research into the ways in which the Internet is transforming (or being transformed by) mechanisms of surveillance (see for example, Lyon, 2002; Graham & Wood, 2003; Lyon, 2007; Finn, 2011; Ball et al., 2012; Dubrofsky & Magnet, 2015). Science and Technology Studies has made substantial contributions to developing frameworks for accounting for technology and the values which underpin it (see for example Friedman, 1997; Joerges, 1999; Winner, 1999; Musiani, 2015). A broader range of 'digital society' scholarship, new media studies and critical algorithm studies have all engaged in powerful explorations of how social media and the Internet's other platforms and infrastructures are shaping, and being shaped, by human action, how they are being used by social movements, and their salience to power and social harm (see for example Lessig 1999; DeNardis, 2009; Napoli, 2015; Milan 2013, 2016; O'Neill, 2016; Just and Latzer, 2017; Goedhart et al. 2019; Aradau, Blanke & Greenway, 2019). Finally, (though this list is clearly non-exhaustive), anthropological and ethnographic studies of technology have developed a range of insights into the cultures and practices of technical work, resistance, and political action in the Internet age (see for example Escobar et al. 1994, Haywood, 2012; Coleman 2014; Brunton & Coleman, 2014; Pink, Ardevol and Lanzeni, 2016; Gehl, 2016). I argue, however, that criminological scholarship has its own contribution, as-yet largely unrealised, to make alongside these efforts. Criminology's particular focus on state-sanctioning of behaviour, governance, power, and control equip it with

useful frameworks and sensitivities for exploring some of the less well-understood aspects of the problems with crime and governance in which these infrastructures and platforms are becoming implicated.

While criminological research has substantial successes in exploring the communities (Yip, Webber, and Shadbolt, 2013; Lusthaus, 2013; Holt, Brewer, and Goldsmith, 2019), motivations (Brewster, 2015; Yar and Steinmetz, 2019) and economics (Afroz et al. 2013; Anderson et al. 2013) of online crime, there has been little progress in developing frameworks for understanding the role technology plays in in criminological accounts of the Internet and cybercrime (Stratton, 2017). Much of the scholarship which does attempt to account for the technologies of the Internet approaches cybercrime through Routine Activities Theory (RAT). RAT was developed initially to explain the changes in criminal offending which occurred following the Second World War, arguing that changes in crime were largely driven by the opportunities created by patterns of routine behaviour: situational factors such as the absence of guardians in the suburbs while people were at work and the rise of high value, portable consumer goods (Cohen and Felson, 1979). This is a 'situational' account of crime, focused on changes in material circumstances and how they shaped broader ecologies of criminal opportunity, and hence created 'criminogenic' situations. A wide range of scholarship on cybercrime uses RAT to explain changes in crime which have arisen as a result of the rise of the internet, drawing on it to understand how this has affected traditional avenues of guardianship and the coming together of offenders and victims in different ways to provide new types of criminal opportunity (Yar 2005; Leukfeldt 2016). This has led to useful studies of online victimisation (Holt, 2008; Hutchings, 2009), offending (Williams 2015; Leukfeld, 2016), and other aspects of online crime.

This line of reasoning naturally leads towards attempting to understand the material qualities which make particular technologies 'criminogenic', and how they transform physical situations in ways which promote crime and victimisation. RAT research frames internet infrastructures as 'bringing together' victims and offenders in novel

situations whose criminogenic properties are determined by the qualities of these technologies (Yar. 2005; Holt and Bossler, 2008; Yar and Leukfeldt, 2016). For example, it frames the connective properties of the Internet as a 'force multiplier', bringing would-be offenders into contact with very large number of potential victims through services such as email. This has proven particularly useful as an explanatory framework because its core concepts of guardianship, opportunity, ease of access, and risk-benefit calculus are well-suited to translation into classic experimental designs (Holt 2008) and produce outputs with direct relevance for policymakers (Clarke, 1995; Weisburd, 1997).

The 'situational' nature of this framework, as it does with more traditional forms of offending, often generates solutions to cybercrime problems which involve fixing these criminogenic situations through technological target hardening and Situational Crime Prevention approaches (Yar 2005) which alter how the built environments of social spaces are designed (whether that be the layout of park benches, locking doors, installing firewalls, or automatically deleting abusive Twitter messages and email spam) (Clarke 1983, 2005). Shifting this responsibility to the largely privately-owned companies who own these platforms does, however, ultimately also involve devolving key democratic debates about crime control, social justice, and governance to the private sphere, with little role for participation on the part of the user other than through the exercise of consumer choice (Garland 2001, Hayward 2007). Equally, it treats technology as a deterministic force, eliding cultural or social-structural factors, black-boxing motivations on the part of the offender, and ignoring the important role played by the cultural life and value systems of these technologies in shaping their design, development, and how they are used. These kinds of questions are at the heart of Science and Technology Studies scholarship, and as such this would appear to be a natural body of work from which criminologists could draw ways of better framing technology.

## Criminology and Actor-Networks: tracing socio-technical agencies with ANT and RAT

Some criminological research has begun to develop this situational approach further using theoretical frameworks from Science and Technology Studies such as Actor-Network Theory (ANT) to make sense of the role which technologies play in cybercrime (Latour, 2005; Brown, 2006). ANT argues for deep explorations of the material and social properties of technology, and how 'non-human actors' exert an agency of their own alongside human action (see for example, Murdoch, 1998; Latour, 2005; Law, 2009; Mol, 2010). ANT seeks to trace the networks of human and technological components of 'sociotechnical' systems and the different types of agency they exert (Latour 2005). In this framework, various human and non-human 'actants' come together and enrol one another in Actor-Networks, arrangements of technological and human components whose topology reflects the power struggles and perspectives involved in their creation (Latour 2005). When one actor aims to achieve something in this network, their action becomes 'mediated' by the various human and non-human intermediaries through which it travels. So, an ANT approach to cybercrime could trace the complex agencies embedded in the tools which people use in committing cybercrime, and how different human and non-human elements come together in criminal, harmful, or deviant online situations (Luppicini, 2014; van der Wagen and Pieters, 2015). This proposes research which is alive to an expanded ontology that dissolves pre-made binaries between technological and human actors (or 'actants') and which does not assume at the outset which agencies (be they human or non-human) are key to a given situation (Brown, 2005).

Within criminology, ANT is gaining increasing purchase as a theoretical framework and set of methodological directives (to 'follow the actors') with which to deepen framings of technology within cybercrime studies. A pathbreaking paper by Brown (2005) inspires much of this work, which called for a broader incorporation of some elements of ANT into criminological research on high-tech societies. ANT has been used to study the sociotechnical factors involved in the curation of botnets

(networks of infected computers) (van der Wagen, 2015), to explore relationships between hackers and their tools (Van der Wagen, 2018), to better understand data breaches (Statchel and DeLaHaye, 2015), and music piracy (Hinduja, 2012). Outside cybercrime research, it has also seen wider use by criminologists to frame subjects as diverse as charities in the criminal justice system (Tomczak, 2016) and prisons (Anderson, 2017). Theoretical work has attempted to apply this within cybersecurity and cybercrime studies as a more programmatic framework (Balzacq and Cavelty, 2016; van der Wagen, 2019) or as a looser set of sensitising concepts (Brown, 2006, Luppicini, 2014; Bossler, 2016).

While incorporating these insights from Actor-Network Theory would be a welcome step forward for criminological understanding of the internet, I argue that the programmatic application of ANT, often described as a process of 'tracing' networks of non-human and human agencies, shares the limitations of situational models of crime and technology such as RAT. In fact, De Paoli (2018) directly makes this connection between ANT and RAT in their discussion of security engineers as "engineer criminologists". This assumes that the values, meanings, and agencies of technological situations are the products of the arrangement of the network of causally-connected human and non-human agents which constitute them (Latour, 2005). This retains Routine Activities Theory's concern with the material qualities of technologies and the built environment, and how they frame, shape, and constrain human action in different ways (and exert agencies of their own). It also, however, elides the role of communication, interpretation, interaction, and culture, treating all of the links between these 'actants' as equal. From a criminological perspective, this also accepts 'crime' as a given, reproducing administrative and hegemonic constructions of crime and power; a criticism often levelled at ANT (Whittle and Spicer, 2008) and more administrative criminological scholarship (Hillyard, 2004). Other theoretical work by cyber-criminologists similarly maintains this focus on the ways in which technologies transform situations, afford users new abilities, or generate new connections between people, often taking for granted the processes by which these properties are actually designed and implemented, how they are

negotiated by users, law enforcement and the general public in practice, and the contested attempts of a range of different social groups to imbue them with meaning. In order to understand and critique power in these infrastructures, a *mapping* rather than *tracing* approach is needed, one which is more open to multiplicities of meaning, communication, and interpretation (Haraway 1994).

## Meaning and the material

There is now a wealth of theoretical writing (Hayward, 2012; Surette, 2015) and qualitative, appreciative empirical studies which go beyond purely situational frameworks to include the role of culture, interpretation, and identity in making sense of cybercrime (see for example, Melvin and Ayotunde, 2011; Dremiluga, 2014; Marcum et al., 2014; Hutchings and Chua, 2016). There is also a great deal of research outside the field of criminology which is alive to these aspects of online crime, from studies of how cryptomarkets shape users' understanding of anonymity (Bancroft, 2017) to anthropological studies of hacktivist groups on IRC networks (Coleman, 2013). This research engages with the lives, understandings, perspectives and cultures of the people who become caught up in the technological networks of the Internet, full of deep mapping and rich description of how their cultural lives, interactions, and values are lived with these technologies. While these studies have contributed some of the most impactful and transformative developments in understandings of crime, deviance, and social harm in the Internet age, they tend to centre on particular groups, subcultures, social movements, or online 'spaces'. In contrast, I focus on the discursive life of internet technologies and infrastructures themselves in order to better understand the struggles over meanings and values which underpin and surround them, and hence how they become tangled up in crime, deviance, and power (Pinch 2010). As Pinch suggests (which I discuss in more detail in Chapter 4), this requires turning this qualitative, appreciative approach towards the hidden people behind these infrastructures and platforms, bringing to

the foreground the different kinds of relationships they have with technology. As Milivojevic (2019) has shown for internet-connected mobile phones and migration, using the theoretical scholarship of Milan (2013), a more critical focus on technologies themselves has the capacity to powerfully extend criminological accounts of technologies to understand the ways in which they act in power relations.

Brown (2006), rather than mandating a programmatic application of ANT, suggests that elements of Latour's scholarship could be employed as sensitising approaches, in particular the dissolution of simple binaries between humans and technologies (the pursuit of the 'technosocial'), and an attentivity to the ways that agencies can be exerted by nonhumans. Brown further argues for a 'cyborg' approach to social theory in the model of Donna Haraway's work. Although many of the criminological papers which advocate an ANT approach draw links with Haraway's cyborg theory (Brown, 2006; Van der Wagen, 2015; Van der Wagen, 2019), in fact, these are not necessarily harmonious perspectives, and Haraway has often been critical of Latour's frameworks. Haraway critiques Latour's conception of technology as the product of 'trials of strength' (Latour, 1987; Haraway, 1997), where technosocial agencies are portrayed as agonistic and competitive, legible in tracings of networks of actants. Haraway's scholarship within Science and Technology studies orients the study of technologies instead as the *mapping* of complex, often communal and multifarious worlds of discourse and power which take up contested and contingent arrangements with materiality (Haraway, 1994; Haraway, 1997).

This allows for (and, in fact, *mandates*) technosocial arrangements which support multiplicities of meaning and a range of co-inhabiting worlds and discourses, each with their own complex shaping relationships with the material (Haraway, 1994). While a range of "post-ANT" scholarship attempts to address this multiplicity through concepts like "fire objects" (Law, 2002), where material signifiers can be mutable and multiple in meaning (Law 2005; Mol 2010), I argue that a greater focus on communication, interpretation, and discourse is needed for the type of research I

have engaged in in this thesis. Although I do not make particularly deep use of Haraway's frameworks in this thesis, her 'material semantics', which forges ways to map these difficult relationships between materiality and meaning, was an important beginning for the approach I adopt, especially the call to study the "world-building alliances of humans and non-humans" (Haraway, 1997, p51). Her scholarship was also foundational to the methodological approaches developed by Clarke (2007) on which I draw. I discuss in substantially more depth the theoretical approach which drives my empirical work in Chapter 4, however, I outline its contours briefly here.

Pinch's (2010) call for qualitative empirical research focused on the designers, developers, and maintainers of the infrastructure and platforms of the Internet argues that this project should move beyond an ANT approach, embracing the frameworks of *symbolic interactionist* social theory to map the multiplicity of meanings with which people imbue these technologies, and the complex relationships these meanings have with the material forms which the technologies take. I do this through social worlds theory, an approach from Science and Technology Studies which frames technologies as *arenas* around which complex, overlapping worlds of discourse can form (Star, 1989; Clarke and Star, 2008). These discursive worlds are implicated in complex relationships with materiality through the ways in which they structure *practices*, and the ways these practices shape (and are shaped by) these infrastructures (Star, Bowker, and Newman, 1998; Star, 1999). This has been used fruitfully to study many technological and knowledge-making projects, including museums (Star & Griesemer, 1989), art (Schlossmann, 2017), education (Bayat, Naiker & Combrinck, 2015), and online knowledge communities (through the related 'communities of practice' framework) (Lave, 1991; Angouri, 2016). It also underpins Star's 'infrastructure studies' scholarship, which exhorts us to study the "hidden work" and "frozen discourses" within the infrastructures which support our societies (Star, 1999), and how the assumptions and default settings baked into them can fail to reflect the lives of marginal groups and individuals, contributing further to their marginalisation (Star, 1990). Methodologically, this allows a deep study of technology without becoming lost in technical detail,

excavating meanings and how they become embedded through interviews and archival research. This is a deeply productive approach, framing as it does technological projects as places where multiple visions of the world can be embedded, negotiated, and go on to shape social life, and Star's theoretical frameworks and methodological approaches are at the heart of this thesis.

This approach provides a 'hook' for criminology's own standpoints as a discipline, presenting a range of theoretical tools and methodological approaches with which to frame the Internet's platforms and infrastructures in ways which fit well into criminological understandings of power, crime, and control. In order to understand the broader consequences of these visions of the world at the micro-level, we also need to understand the relationships these discourses have to higher levels of power in a wider social and historical context. Accordingly, I situate this research, as Hacking (2004) describes, "between Goffman and Foucault", attendant both to the actual practices, processes and mechanisms through which control is enacted and crime problems are established, but also to the broader history and context of these discourses, where they come from, and why particular voices and visions of the world gain influence (Lippert, 2010). I discuss Goffman's scholarship and how it relates to the thesis in more depth in Chapter 4, where I set out the core theoretical framework which drives my empirical research. To situate this research in its broader context, I discuss in the following section the Foucauldian frameworks which I use to frame the wider mechanisms of control by which the Internet's infrastructures are governed, and the discourses and visions of the world which underpin these. I use Foucault's *governmentality* scholarship, whose framing of power as mediated by materiality and meaning resonates with these questions, as an entry point for this.

## Governmentality, power and discourse

Internet technologies are increasingly implicated as sites of power in our societies, and the precise *kinds* of power wielded by their designers and the governments who attempt to control these infrastructures are at the heart of many of the core debates around data, privacy and power with which contemporary societies are wrestling (Kahler, 2011). Some of the most vital questions for criminological understandings of the Internet relate not only to the novel forms of online harm and crime which have emerged in the Internet age, but changes in the way that nation states and other powerful forces understand and carry out the business of governing their societies.

In the previous section, I made the case for qualitative, appreciative research into the understandings, values, and visions of the developers of Internet technologies and platforms, how they are realised as material infrastructure, and the problems of power, governance, and control which they then have to navigate. In situating this research in the broader field of criminology and histories of governance and control, I draw on the body of scholarship which is broadly defined as *governmentality studies* (Lippert and Stenson, 2010). This work, which draws on social theory developed by Michel Foucault (Foucault, 1991, 2007, 2008, 2010; Garland, 1997; Lemke, 2015), has been particularly influential in describing the changing ways that power and control have been shaped by the late modern turn (Garland 2001; Lippert and Stenson, 2010). Foucault's governmentality work is a good basis for framing the technologies, platforms, and infrastructures of the Internet, as it approaches power as the materialisation of visions of the world, exploring how these visions provide the basis for people's attempts to imagine themselves as subjects (Darier, 1998; Badouard, Mabi, and Sire, 2016). This is particularly well-suited to contextualising the empirical work in which this thesis is engaged, providing as it does a way of making sense of infrastructures and platforms as sites where different visions of the world are realised and contested, the relationship this bears to power and the people who become tangled-up within them. In this section, I set out the fundamental elements

of governmentality theory, then in the following section articulate it as it has been applied to the Internet.

Foucault's concept of governmentality draws from his understanding of power as linked to changing ways of thinking about and understanding society and the business of government; what Foucault describes as the "conduct of conduct". Foucault argues that one cannot understand the ways in which modern societies exert power and control, their *technologies of power*, without understanding the *rationalities of government* which underpin them (Foucault, 1991; Garland, 1997). Rationalities of government are the changing discursive formations, or ways of thinking, through which different states at different historical moments frame and approach the work of government and crime control. These discourses are ideotypical, and the point of Foucault's work is less to identify these understandings as a total depiction of any particular individual, organisation, or state in a given historical moment, but as useful ways of conducting a genealogical account of the history of forms of government and control (Garland, 1997; Foucault, 2007, 2010). This leads to an epochal view of the history of ideas, rather than one necessarily reflective of messy historical reality, something for which Foucault is oft-criticised by historians (Weeks, 1982). Foucault argues that modern societies are characterised by the development of new forms of power which he describes as the formation of *governmentality*: rather than the domination of society from above, power operates throughout society, clustered around governing bodies, requiring new types of knowledge about populations (through censuses and social-scientific research) for its operation, and expressing itself through the social shaping of populations and how they experience the world and understand themselves (Mehta & Darier, 1998; Rose, O'Malley & Valverde. 2006; Foucault, 2010).

Foucault argues that these ways of making sense of how to govern societies become materialised in *technologies of control*, as the documents, practices, policies, infrastructures, institutions, laws and architectures with which governmental actors engage in the business of government. These technologies of control reflect the

rationalities which underpin them both in their material design and the ways in which they operate in and shape the world. They also operate as important conduits of power, both as direct mechanisms of control over people and their behaviour, and the more subtle ways in which they shape how people in their societies think and understand themselves (Foucault, 2007).

Foucault's understanding of this kind of power changed across the course of his writing (Garland, 1997). In early work such as *Discipline and Punish*¸ power operates almost deterministically on individuals, with the logics embedded in institutions, architecture, practices, and other materialisations of control rendering them coercively as passive objects, or "docile bodies" (Foucault, 2012). His later writing, however, acknowledges this as a process of *subjectification*, with people actively constructing themselves as subjects in ways which are shaped and structured by the materialised discourses embedded in institutions, architectures, and other technologies of control (Garland, 1997; Foucault, 2010). These technologies of control therefore also become *technologies of the self*, 'held out' to individuals as resources with which to construct themselves, and it is through this subjectification that the state exerts its sovereignty and lays claim to individuals, shaping in its own image the kinds of people which they are able to be (Garland, 1997; Foucault, 1991, 2007, 2010). Foucault offers the rise of 'biopolitics' as an example of one form which these technologies of control can take in modern societies, through which the collection of information, through censuses and social scientific research, about subject populations forms one of these mechanisms of subjectification, calling out individuals to fit themselves into the category systems and frames of representation which these collection mechanisms employ (Foucault, 2008).

This has been taken up by criminologists as a way of problematising the idea that the institutions and ways of governing (such as prisons, or the police) by which our societies are characterised are somehow inevitable, rather asking us to map their histories to find out why they take the forms they do, what visions of the world underpin them, and how things might have been (or might be) different (Garland,

1997; Williams and Lippert, 2006). I use these ideas in the thesis to frame the operation of power as the result of contested attempts to materialise different *visions of the world*, as constituted in worlds of discourse. Although, as Brown (2006) notes, technologies are often left somewhat inert in these accounts, I argue that this is not by necessity, and that a *governmentality* approach has much to add to study of the technologies and infrastructures of the Internet. In this thesis, I use this to connect Star's (1999) developments of the social worlds framework, which tackle how meaning is negotiated within technical projects and becomes imbued in material technologies, to their broader context of governmental power as realised in the Internet infrastructure.

## Technologies of online control and infrastructural resistance

Applying a governmentality perspective to the Internet, one can begin to draw relationships between these ways of thinking and the mechanisms through which the governance and control of online space are arranged (Mehta & Darier, 1998; Badouard, Mabi & Sire, 2016). The Internet is both governed by technologies of control (such as the police, Internet Service Providers, regulatory bodies), and a technology of control in its own right (as a set of infrastructures that operate as conduits of control, which embody the rationalities of their designers). The original egalitarian promises of these technologies bringing the world together have been contradicted by the physical infrastructures of the Internet largely replicating, and even deepening, existing inequalities and power relationships (Mehta & Darier, 1998; Hand & Sandywell, 2002). I discuss the history of the rationalities of the Internet and the technologies of control within them in further detail in Chapter 3.

This paints a rather bleak view of the Internet and its infrastructures; however, these platforms are also the focus of powerful visions of hope. While Foucault focuses on the rationalities of states and other powerful actors' in their attempts to discipline and govern (although understanding the power of their discourses as dislocated and

dissipated through society), they are not the only ones whose visions of the world are asserted through these kinds of power, and other groups are able to contest power in this domain (Musiani 2013; Milan 2019; Zalnierute & Milan, 2019). A range of counter-movements have attempted to resist these increasingly authoritarian trends in internet governance and renew its status as a platform for liberation and social transformation (Marechal 2015; Milan 2013, 2016). The privacy properties of these infrastructures are hence a key battleground in which the futures imagined by technological innovation and political struggles are contested (Dencik, 2016). This takes place within conventional institutions, such as parliamentary democracy, constitutional challenges in the courts, and traditional activism (Bennet 2008); however important parts of these conflicts take place outside this sphere. These movements have given rise to a number of technological organisations which engage in internet politics by developing new tools and infrastructures which better reflect their values (Dencik 2016; Milan 2013, 2016). This is possible on the scale we now observe due to a fundamental quality of Internet architecture: it permits new, alternative infrastructures to be built to extend its capabilities in different ways with relative ease, changing its technical properties and creating new imagined spaces (Van Schweick, 2012). As governments have sought to reimagine the internet as a space of control through building surveillance infrastructures on its foundation, so too have citizens and organisations begun to build their own infrastructures alongside it which have different constructions of privacy at their heart (Milan 2013, 2016). These constitute oppositional engagements deliberately situated in the terrain of power imagined by Foucault; clashes between material infrastructures which stand as proxies for conflicts between distinct, opposed visions of the future of our societies.

These oppositional attempts to assert alternative visions of the world to those embodied in our current Internet are the subject of a growing and vital body of digital society scholarship, of which I here highlight three perspectives which have been particularly useful in situating the research in this thesis. Coleman (2017) frames these attempts through the rise of 'hackers' as a class of practitioners who

are now increasingly engaged in political struggles, distinct from other kinds of technological workers in their "impulse for craftiness" (Coleman, 2017, p92), and their drive to subvert and repurpose static and established systems. This subversion is accompanied by a range of attempts by these hacker groups, aligned with a wide range of different political sensibilities, to build their own platforms, expressive of particular ideological agendas. Aggressive state assertions of control of the Internet and attempts to claim sovereignty over and regulate its technologies bring these subaltern technologists into direct conflict with established power, drawing them into political domains which they might otherwise have avoided (Coleman, 2017). As they become drawn into these political arenas, the 'hacker' sensibility extends further than merely experimentation with technical systems, especially as they begin to build platforms and infrastructures which need to sit within established legal and administrative contexts. As a result, Coleman argues that these groups become adept at 'hacking' the law as well, finding loopholes and clever edge cases to allow them to do their political work. The political character of this 'hackery' social action often demonstrates a certain ideological pragmatism, as these groups often enrol odd bedfellows who might not be expected to work with one another in the service of overlapping goals. Coleman's research documents the rise of this new class of political actor, arguing that these "weapons of the geek" are reflective of a particular shared set of cultural practices, sensibilities, and strategies.

Outwith these oppositional 'hacker' communities, Musiani, Cogburn and DeNardis' work (2016) draws on a range of Science and Technology Studies scholarship, but particularly the infrastructure studies work of Susan Leigh Star (1989, 1999), to describe how the structural, or 'architectural' forms of Internet infrastructures constitute an important domain of politics in their own right in which a variety of groups can engage. This documents the broader attempts by communities of software developers and engineers to 'do politics' through architecture and a "turn to infrastructure" in Internet governance (Musiani, Cogburn & DeNardis, 2016). The 'architectural' or 'infrastructural' domain therefore becomes a key domain of power, not only subject to governance, but itself a form of governance. Musiani draws on

Star's scholarship to pull out the hidden work behind the design of this infrastructure and to critique its connection to power relations (Musiani, 2013). Musiani's studies excavate the ways in which politics and design are worked out in the creation of decentralised Internet infrastructures, which she argues frame relationships between users and providers, power and control points, in different ways to more centralised designs. She uses this to extend the idea of infrastructure as a site of social action, unearthing the spaces where engineers and developers attempt to realise alternatives to the dominant visions of the future through building infrastructures which reflect their own imagined future worlds (Musiani 2013).

Finally, Milan's (2016, 2019) research on the intersections between technologies, infrastructure, and activism provides another catalyst for this thesis, and frames this more explicitly through the lens of social movements. Milan (2016) argues that the Internet has led to a multiplying of the pre-existing traditions of community-run infrastructure, manifesting as 'tech activism'. Milan (2016, 2019) describes this as "stealing the fire", the challenging of power interests by activist groups in the terrain of infrastructure, asserting a radical democratisation of the 'plumbing' (Milan, 2016) of everyday life and reclaiming the power which these technologies exert over populations. This action occurs in four domains: the "creation of alternative infrastructures", "the appropriation of existing enclosed spaces", "hacking and tinkering", and "bypassing legislation through technical fixes" (Milan, 2016). Milan argues for exploring the complex relationships between practices and values at work in these types of social action, and how they "merge in the moment of technology design" (Milan, 2016).

Each of these foregrounds a different facet of Internet technologies as a site of social action, bringing out a distinct package of sensibilities, rationalities and practices. Rather than adopt any one of these, I make use of a social worlds approach (which I describe in more detail in Chapter 4) to try to make sense of how infrastructures like Tor can become places where multiple different kinds of social action come together in conversation and conflict. These infrastructures are increasingly where important

battles over power, policing, and control are being fought. I argue that focusing on these conflicts and how they play out through deep qualitative empirical research has the capacity to deepen criminological understanding of the Internet in important ways. In this thesis, I study how these platforms and infrastructures actually engage in this domain in practice through the study of a single 'rebel infrastructure', or attempt to "steal the fire" (Milan 2019) which touches particularly on issues of salience to criminologists: the Tor network, which attempts to directly frustrate and subvert the technologies of mass surveillance and censorship through which the internet is governed.

## The Tor network – critical infrastructure

This brings me to the central subject of this thesis: the Tor network. Tor is an anonymity network built on top of the Internet's backbone, a rebel infrastructure originally developed by the US Navy but long since moved outside the domain of military research to the NGO sector, where it has become the technological jewel in the crown of the Internet freedom movement. It is maintained and developed by the Tor Project organisation and is supported by a vibrant community of volunteers who help develop and scrutinise the code, run the servers which make up its infrastructure, and promote its use around the world. It is a profoundly successful intervention in the topologies of online power and an attempt to realise a subaltern vision of the future of the Internet. The Tor network is generally accessed by its users through a free web browser (the Tor Browser) and allows them to browse the Internet and host websites while effectively undermining the ability of the government to surveil their actions. This has an important secondary quality: by and large, websites which are blocked by Internet Service Providers are freely accessible over Tor, making it extremely difficult for governments to censor online content. The Tor network can be used both for browsing and for hosting, allowing users to set up websites called Onion Services, which are extremely difficult to take down and can

only be accessed through the Tor network (Moore and Rid, 2016). I discuss the technical design through which Tor achieves this in greater depth in Chapter 3 and explore its development in Chapter 7. In brief, the administrative information which the users' internet signals employ to navigate the Internet are encrypted, then these signals are bounced around the Tor network, a volunteer-run infrastructure of servers around the world, which creates a 'crowd' of users which it is very difficult for even nation states to unpick.

Criminological research on Tor has almost entirely focused on its capacity for crime. In particular, this has taken the form of the 'Darknet' or 'Dark Web' – a colloquial term for the relatively small number of Onion Services which have been set up by those looking to facilitate illegal or harmful action (Moore & Rid, 2016). The Tor network is unquestionably implicated (in the same way that the Internet itself is) in a degree of harmful traffic which flows through its servers. Some online communities involved in illegal activities make use of these services to set up forums where they can discuss these activities, interact, and form communities (Bancroft, 2017; Fonhof et al., 2018; Kamphausen and Werse, 2019). Particular academic interest has been directed towards 'cryptomarkets', online marketplaces hosted on Onion Services which facilitate trade in a variety of illegal goods, such as drugs or stolen credit cards (Martin, 2014). There is a substantial body of research on these cryptomarkets, from their effect on broader drug markets (Aldridge & Decary-Hetu, 2016; Gilbert & Dasrupta, 2016; Demant & Munksgaard, 2017) mechanisms through which they cultivate trust and reputation (Tzanetakis et al. 2016; Morselli & Decary-Hetu, 2017; Lorenzo-Dus, Cristofaro, 2018), their effects on harm (Barrat et al., 2016a; Barrat et al. 2016b), their resilience to police intervention and disruption (Decary-Hetu & Giommoni, 2017; Ladegaard, 2017; Ladegaard, 2019), and the internal dynamics and cultures of their communities (Maddox, Barratt & Allen, 2016; Bancroft, 2017; Tzanetakis, 2018).

It is important to note that these services facilitate a range of legal use cases. The largest Onion Service belongs not to a criminal group, but to Facebook, whose Onion

Service allows users nations in which Facebook is blocked to access its services (Muffet, 2014). Several major, well-respected newspapers run Onion versions of their websites or services, including the New York Times (Sandvik, 2017) and the Guardian (2019). Onion Services are used by whistleblowing organisations such as SecureDrop to provide a secure means of releasing information and protecting whistleblowers' identity (SecureDrop, 2019). Even organisations such as the CIA operate Onion Services of their own (CIA, 2019). The Tor network provides an important service for researchers, activists, and investigators, as it allows people to access websites without revealing their identify. This enables those attempting to research online crime to scrape websites without being blocked, allows the officials at the Internet Watch Foundation to investigate online child sexual abuse on the regular Internet securely, and provides law enforcement with a range of tools for investigating crime, especially by powerful corporations and organised groups (Laidlaw, 2012). It is equally important to note that the vast majority of online harm occurs on the regular Internet; in fact, the barriers to entry posed by Tor use mean that many online criminal economies operate on the regular Internet, without the use of Tor, in order to attract the largest possible amount of commerce (Hutchings, 2016; Pastrana, Hutchings, Caines et al. 2018). Tor use also facilitates a range of other security benefits, protecting its users from a range of common security threats, and frustrating attempts by web services to track them across the Internet using cookies and other fingerprinting techniques.

There is a small body of sociological and legal (Minarik and Osula, 2015) research on Tor outside criminology which does not frame it solely in terms of crime and harm. Gehl, for example, has discussed in depth the attempts of the Tor community (and other anonymity technologies) to cultivate legitimacy of different kinds, analysing online archives and other materials (Gehl 2018a. 2018b). He has also engaged in more theoretical work which discusses the ramifications of Tor for private and public space online (Gehl and McKelvey, 2019). Bancroft (2017) has engaged with the links between values and the material, focusing on user perspectives and studying the interactions between the material anonymity properties of cryptomarkets and the

discourses through which their users construct anonymity. Marechal has more directly engaged with the Tor community itself, studying it as a social movement and tracing its political economy and attempts at professionalisation (Marechal, 2018). What is missing, however, is a systematic sociological account of the Tor community, its values and visions of the world, and how these are linked to Tor as an infrastructure; its design properties, the challenges it faces, and how it actually engages in questions of power.

## Conclusion

In many ways the most interesting unanswered questions about the Internet for criminologists have little to do with cybercrime as conventionally conceived. I therefore argue that a 'criminology of the Internet', in partnership with but distinct from cybercrime scholarship, would be a fruitful next step for criminological research. Tor clearly poses a set of extremely interesting questions for criminologists beyond the particular communities, harms or illegal activities which it facilitates. In undermining the fundamental technologies of control through which states govern the Internet, Tor presents not only a challenge to governmental power, but also an attempt to realise a distinct vision of the future Internet., Foucault's concept of governmentality provides a useful framework for understanding the context of these struggles, as it shows the technologies of control which characterise our societies (such as mass online surveillance and censorship) to be far from inevitable, rooted instead in the ways of making sense of the business of government which have provided the backdrop to the history of the Internet. As Garland (1997) contends, however, the most productive criminological research in this area does not take these rationalities and technologies as total, rather it uses them as ideal types which are realised and conceived in partial, contested ways, in heterogeneous partnerships and oppositions with other forces and factors. Tracing the complex reality of how these are worked out in practice requires a deep investigation of how these visions of the world are actually materialised and the challenges they face: as Musiani

(2012) argues, “doing a sociology of networks that is not afraid of its subject of study”.

Criminology as a discipline has been a locus of enormously productive work exploring the ways in which the materiality of technologies of power interact with the discourses which shape them and the world at large. In its studies of laws, architecture, institutions, practices, and policies it has greatly extended academic understanding of power and the complexities of how our societies are governed. As yet, criminological research has been surprisingly slow in engaging the infrastructures and platforms of the Internet in this way. It is in the nature of these technologies that they ‘black box’ their values behind complex computer code which obfuscates this connection between meaning and the material. However, social worlds theory presents a possible way forward for this research as a project of qualitative, appreciative exploration of the people embedded in these technologies, and how they understand these questions. In this thesis, I engage in deep empirical research on Tor’s attempt to “steal the fire” (Milan, 2016), how the people of Tor make sense of their values, the different ways in which they attempt to realise them in material infrastructure, the problems they face in practice when they come into contact with the technologies of power which they are trying to undermine, and how they navigate these challenges.

In the following chapter, I situate this work in context, engaging in a genealogical history of Tor to fit it into the broader history of the Internet, online governance, and social control. I argue that the position Tor occupies in the world and the way it works was by no means inevitable, and is deeply contingent on its history, the interaction between the ideas underpinning its creation and those embedded in the Internet, and how particular groups attempted to meet the challenges which arose throughout its lifetime. In Chapter 3, I sketch this history of the ideas which shaped these technologies, the developing mechanisms and rationalities of online control, of Tor’s design and how it has evolved alongside the Internet, and of the challenges which Tor and its community have faced.

# chapter 3

# a genealogy of Tor (and a social history of the Internet)

## Introduction

Having set out the gap in academic scholarship which this research aims to address, in this chapter I step back to explore Tor's history and the history of the Internet. I write this as a genealogical history, mapping the changing ideas, contexts and challenges which have shaped what Tor and the Internet have become today. In doing this, I draw out a series of core issues which this thesis explores through empirical research.

Tor as it stands occupies an extremely contested position. Public knowledge about Tor is scant, with most people only knowing it as the Dark Net or Dark Web, a 'Wild West' where crime is conducted with impunity from law enforcement (Bartlett, 2015). Where Tor is portrayed in the media or academic research, it is usually this use for criminal harm which is the focus, with a token gesture towards its origins as a military technology and use by whistleblowers and journalists (Chen et al. 2008; Jardine, 2015; Bartlett, 2015; Weimann 2016). This presents a rather confusing picture from the outside: that a technology exists which undermines the police and intelligence services' attempts to surveil the Internet, which is widely used for crime, government-defying journalism and whistleblowing, but is not criminalised in all but a handful of nations despite its clear challenge to power; one which was invented by the US military, but now appears to undermine the ability of the US to surveil its

population (Jardine, 2015; Minarik and Osula, 2016; Moore and Rid, 2016; Gehl and McKelvey, 2016). Situating Tor within the history of the Internet and the different ways people have attempted to control online infrastructure does a great deal to explain these apparent contradictions but makes Tor no less fascinating a subject of criminological research. In fact, as I argue in this chapter, there are much more interesting aspects of Tor (and by extension, the Internet) for criminologists than only its involvement in crime.

In this chapter, I set out the historical context for this thesis, aiming to break up the idea that Tor's current design and social situation are natural or inevitable, and trace why it occupies this contested position. In laying out this history, I draw on archival research, my interviews with members of the Tor community, and a review of relevant literature. I begin this chapter by setting out a brief history of the Internet and the different ideas which were influential in shaping it up until the turn of the millennium. Then, I discuss the struggles over encryption and control which have been fought since the early 1990s, often termed the 'Cryptowars', and the genesis of the Onion Routing technologies which preceded Tor. The following section discusses the early years of Tor's development and the problems it faced. I then discuss the Snowden leaks, which revealed the extent of the growth in US surveillance and the securitisation of the Internet in the wake of 9/11, and their salience to Tor's work and the Tor organisation (Lyon, 2015). Finally, I return to the present day and the issues which Tor (and the Internet more generally) face, including the backlash against mass surveillance and the rise of surveillance capitalism (Zuboff, 2015). At each turn, I attempt to link the evolving material infrastructure of the Internet and the different approaches which people, states, and corporations have taken to controlling it with the discourses and visions of the future which have grown up alongside it.

# The Internet and its discourses

## Internet prehistory – military, sovereignty, and the scientific elite

The history of computing and the Internet is not one of 'neutral', 'inevitable' technical progress, rather it is bound up deeply with ideas, cultures, and social context (Castells, 2004). Throughout this history, the Internet and the mechanisms through which it is governed have been shaped by a confluence of several intersecting *rationalities*; different ways of thinking about society and technology, and distinct visions of the Internet and its future. There have been many different attempts to separate these out, such as Castells "four cultures" of the Internet (Castells, 2004), or the multi-stakeholder mappings in the Internet governance literature (Pickard, 2007; Chenou, 2014). Instead of sticking programmatically to one of these systems, I try to draw them together into something which usefully frames different ethics of control, freedom and openness, the discourses underpinning the Internet and their consequences for how it is organised. In this section, I characterise some of the main ideas which underpin the Internet and their salience to the shape it has taken.

The Internet's roots are well-documented and can be traced back to the Advanced Research Projects Agency (ARPA), a US government agency founded in 1957 to carry out scientific and technological research projects for the Defence Department (Rosenzweig, 1998). ARPA and their contractors began the development of the ARPANET computer networking project in 1967, an attempt, using an idea developed by the RAND Corporation, to solve the problem of nationwide computer communications in a hypothetical nuclear war scenario when centralised exchanges might be destroyed. This Cold War context led to the development of a 'distributed' network, which routed packets of information along different paths through the network – the 'packet switching' design – and assembled them at the destination, without the need for a centralised authority (Sterling, 1993; Rosenzweig, 1998). These initial aims also extended to the scientific community (which, in any case, was

viewed as crucial to maintaining US military supremacy), allowing the sharing of computing resources between researchers distributed around the nation as well as the implementation of systems for more direct military use (Rosenzweig, 1998).

The Internet's foundational visions have their roots in the ideas, motivations, and perspectives of the US military and a research and technological elite based in US universities and research labs (Leiner et al., 2009; Curran, 2012; Cohen-Almagor, 2013). Although the Internet is built around a decentralised model, this way of thinking is not particularly committed to 'decentralisation' or 'centralisation' as values in their own right, rather it was (and is) more concerned with the pragmatics of developing the interests of the US nation state, both domestically and in the sphere of geopolitical power. As such the scientists were engaged in designing systems to solve particular research problems which were determined by their funders in the military; rather than attempting to achieve a particular kind of system for its own sake, they were attempting to develop an infrastructure for the Internet which could both be resilient, and have a topology which would allow the US to establish itself at crucial control points (Edwards, 1996; Curran, 2012). In the case of the packet switching design, this gave rise to the apparent contradiction of the centralised, hierarchical US military finding its needs best met by a fundamentally decentralised system. While this was happening, though, a counter-discourse had been developing among the communities of technical experts, researchers, and academics involved in designing the technologies, and in the hobbyist communities which had been increasingly gaining access to these networks (Rosenzweig, 1998; Curran, 2012).

## Hackers and cyber-libertarianism

Despite their close engagement with the US military (Rosenzweig, 1998), the technologists and researchers who developed the early technologies of the Internet incubated a radical countercurrent to these more establishment sensibilities. Rooted

in 60s and 70s counterculture (though perhaps more "libertarian rather than liberational" (Rosenzweig, 1998)), a radical body of thought and practice arose which equally shaped the foundations of the Internet and how it has evolved over the years. This set of ideas, emerging variously from computer science departments (especially the much-documented Tech Model Railroad Club and Artificial Intelligence Lab at MIT) and the countercultural movement in 1960s and 1970s San Francisco, established a vision of technology in which the structural forms, design principles, and technical practices of information systems were themselves the embodiment of a particular politics: the 'hacker ethic' (Levy, 1984; Jesiek, 2003; Nissenbaum, 2004; Coleman, 2012). The developers at work in these labs mobilised the 60s and 70s countercultural values of anti-authoritarianism and liberation which were growing out of the anti-Vietnam and civil rights protest movements, envisioning that the technologies which they were building might be able to reflect these ideas. Underpinned by a techno-libertarian ethos of personal liberty and freedom of information, they prized decentralised systems as powerful political statements in their own right, alongside practices of creative experimentation and repurposing of existing systems in subversive ways (Levy, 1984).

As the hacker subculture spilled out from research departments to the growing hobbyist computing movement and the underground forums of the Internet's 'demimonde' it developed a far wider cultural relevance of its own. Its romantic, techno-utopian visions flowered in science fiction depictions of hackers, from Gibson's (1984) *Neuromancer,* to *Trouble and Her Friends* (Scott, 1994), to *The Matrix* and more recent fiction such as *Rosewater* (Thompson, 2016), and hackers are now staple characters in contemporary action films (Yar, 2012; Wall, 2012; Taylor, 2012). There is now a substantial scholarship on hacker subcultures, initially portrayed as male, introverted, and based around a narrow set of values (Levy, 1984), which now reflects an diverse range of communities with very different goals and perspectives (see for example, Coleman, 2004, 2008, 2010, 2011, 2012, 2014; Steinmetz, 2016; Milan and van der Velden, 2016). Coleman and Golub (2008) argue that there is no individual 'hacker ethic', but that it encompasses a range of 'moral

genres' stemming from the diverse array of people, practices and politics within a range of hacking communities around the world. They identify three distinct rationalities within this: *crypto-freedom*, *free software*, and the *hacker underground* (Coleman and Golub, 2008). Although all steeped in essentially liberal values and hacker practices of creative engineering, each of these 'variants of liberalism' (Hall, 1986; Coleman and Golub, 2008) emphasises a different facet, reflecting the tensions and discontinuities within liberal thought. I adopt this threefold framing here, as it is particularly useful (as will become apparent) for contextualising how the history of the Tor Project fits into the history of the Internet.

The first of these, crypto-freedom, is particularly important for this history, as these ideas go on to form a core part of Tor's development and its reason for existence. The crypto-freedom sensibility stems from the computer scientists and cryptographers who were developing the encryption technologies which grew up alongside the Internet. For many involved in this work, it took on a distinctly political character: these encryption technologies could have a powerful impact beyond their use by the military in underwriting a liberal conception of privacy and autonomy of the individual, protecting the Internet as a space for freedom and information, commerce and community (Coleman and Golub, 2008). While they shared a utopian view of the Internet with other hacker sensibilities, they believed that this would need to be guaranteed by robust technical mechanisms for ensuring privacy, lest it become a dystopian tool of repressive control and surveillance. This developed beyond the research community into the cypherpunk movement (a formative influence on Tor, whom we will revisit in the next section), an association of cryptographers, hackers, and privacy enthusiasts centred around the infamous 'cypherpunks' mailing list[1] (Hughes, 1993; Bartlett, 2016). The particular trust and security requirements of these systems, which counter-indicated reliance on a centralised authority, tended to mandate decentralised networks, and this is

[1] An archived copy of the Cypherpunks mailing list can be downloaded at: http://mailing-list-archive.cryptoanarchy.wiki

reflected in the values of the cypherpunks, who share with the other hacker ethics a love of decentralisation as a value of its own (Jordan and Taylor, 1998).

The second of these 'hacker ethics' finds its home in the Free and Open Source Software movement (Stallman, 2002). Some of the hackers who had played a role in the Internet's early years of development had begun to set up foundations and communities dedicated to developing software in a new way, which embodied their techno-utopian values and hopes for the Internet as a vehicle for social transformation. In reaction against 'closed' and 'proprietary' models of software development, in which source code is obfuscated to prevent unauthorised copying or changing, they envisioned a future Internet in which code was the foundation of a radical democratisation of the material underpinnings of social life (Coleman and Golub, 2008; Coleman, 2009, 2012; Soederberg, 2015). By opening up source code to public scrutiny, they argued that as the Internet became more central to everyday life, so too would it empower people to question and shape the ways in which the programs they depended on worked. This was underpinned by an ethic of radical participation, arguing that not only should the source code be open, but the people who use it and others interested outside the academy should be able to take part in development (Berry, 2008; Powell, 2012). Prioritising the free and open sharing of ideas and the right to experiment with technology free from regulation, this is a separate facet of an essentially libertarian view of the world, emphasising the freedom to act rather than freedom from surveillance. There is a substantial scholarship on the Open Source movement which has drawn out the conflicts and tensions within this movement, and the cultures, beliefs, sensibilities and practices which have formed within these communities (see for example, Coleman 2004, 2008, 2010, 2011, 2012, 2014; Elliot and Scatchi, 2005; Powell, 2012 ).

As the 1980s progressed and hobbyists and computer enthusiasts were increasingly getting access to networked computing, a burgeoning hacker underground was growing (Sterling, 2002; Skibell, 2002; Taylor, 2012). Over the 1980s a range of other computer networks, often set up by user communities,, were proliferating outside of

the ARPANET. Two of the most famous of these were Usenet, a community platform which had been developed by Unix users which operated as a series of boards which they could post on about a variety of topics (Turner et al., 2005; Tepper, 2013), and Bulletin Board Systems (BBSes), a set of home-made bulletin boards hosted on user computers which could be connected to over telephone lines[2] Myers, 1987). These networks developed "from below", rather than imposed from above, and developed a set of vibrant cultures of their own (Rosenschweig, 1998, p. 1544). In these hobbyist communities, a distinct hacker subculture began to arise, similarly concerned with technological experimentation, creativity, and anti-authoritarianism, but interested in disruption and subversion of power rather than the creation of cryptographic tools or participation in an open software organisation (Coleman and Golub, 2008). Steeped in these techno-libertarian ideas, and worked out online and through in-person meet-ups (which still exist today), this grew into the 'hacker underground', a range of Internet communities engaged in sometimes criminalised attempts to hack, repurpose, tinker with, and exploit computer systems, either out of curiosity, to establish a reputation, for personal gain, or for political purposes (Bachmann, 2012). A substantial cultural life has grown up around these communities (Taylor, 2012). When criminologists study 'hackers', it is generally the hacker underground to which they refer.

Coleman's research on open source hacker communities identifies in them a deep distaste for overt politics, or "political agnosticism" (Coleman, 2004), but her later scholarship shows that many of those engaged in hacker practices are increasingly (if often reluctantly) entering the terrain of political action, wielding technological and infrastructural power in the form of what Coleman terms "weapons of the geek" (Coleman, 2017). The three distinct moral genres of hacking which Coleman and Golub (2008) identify have played crucial roles in the development of the Internet. Cypherpunks have created encryption and anonymity technologies which are now fundamental to global finance and communication, as well as to more contested

[2] An excellent collection of archived BBSes can be found at https://www.textfiles.com

privacy technologies such as Tor and Bitcoin (Dingledine, 2004; Nakamoto, 2008). Free software can be found as a component in almost all technical systems and provides the backbone for huge swathes of the Internet. Tor itself is developed open source and draws on many of the beliefs of the open source ethos (Kelty, 2008). Equally, the hacker underground has been a powerful force, allying with social and activist movements like Anonymous, becoming involved in more serious crime, and provoking (and resisting) a backlash of control from governments (Sterling, 2002; Coleman, 2014, 2017). Still others have spilled out of the academy, free software communities, and the underground into the corporate world, where the ethic of Internet-mediated disruption has upturned whole industries and allowed them to create entirely-new power structures of their own (Guttentag, 2015; Jones, 2017; Levina and Hassinoff, 2017; Zuboff, 2019). These more corporate visions of the Internet resonate with the dominant political rationality in the US of the 1990s: neoliberal capitalism.

## The neoliberal Internet

The 1990s saw the growth of the Internet away from its roots as a military and scientific network culminate in the 'commercialisation' of the Internet and its opening up to businesses, everyday users, and global commerce (Weis, 2010). While the Internet pre-1990s had been largely managed by a "technical/scientific" elite, businesses and corporations now began to cultivate an increasing interest in developing it as a space of capitalist exploitation (Chenou, 2014). As the Internet grew, the development and popularisation of email, bulletin boards[3] and other such applications marked the beginnings and growth of a burgeoning consumer market for Internet-connected technologies, which led to the handing over of custodianship from the military to the National Science Foundation. This dream of an Internet open

[3] for an excellent introduction to these bulletin boards, visit the website www.textfiles.com

to everyday users and commerce was realised in the creation of the World Wide Web in 1991, which allowed users to explore these networks through 'websites' where text and multimedia content could be hosted, which were linked through 'hypertext' links which created a semantic connection between different sites (Berners-Lee and Fischetti, 2001) The release of the Mosaic web browser in 1993 and early search engines began the expansion of the Internet to an even wider audience, and in the 1990s, Internet use grew rapidly (Kim, 2011).

Arguably some of the most important ideas which have shaped the contemporary Internet are those of *neoliberal* thought, which underpinned much of this vision of a commercialised Internet which could form the basis of new global free markets in ideas, commerce, and communication (Mansell, 2011; Pickard, 2007; Chenou, 2014; Curran, 2012). The neoliberal vision of the world envisions the increasing dissolution of national and international barriers to free trade, free movement, and communication, with a vision of modernity synonymous with the spread of capitalist democracy and market freedom around the world (Alfredo Filho and Johnston, 2005; Wacquant, 2012). It views the market as the 'true' arbiter of democracy, bringing democratic force to every element of the provision of every public good, as publics "vote with their money". It claims that market provision has the effect of maximising efficiency and quality through open competition, and hence argues for a minimalist conception of the state. This model of freedom is based on individual choice and is deeply suspicious of technocratic attempts to govern from the centre (Harvey, 2007).

In practice, this involves the delegation of traditionally public services (including order maintenance and policing functions) to the private sector and free market competition. The counter-current to these *lassiez faire* postures of the state within neoliberal governmentality is that it traditionally entails the presence of some extremely strong forms of state control in order to enforce and protect these free markets (Harvey, 2007; Wacquant, 2009). Control becomes, therefore, a force enacted at a distance, with states "steering, not rowing" (Crawford, 2006). This

vision of the world has been roundly critiqued by a vast scholarship of political and social scientific thought (and by social movements and civil society groups) for its naivete towards (or calculated disregard for) the effects which such systems have on the poorest in society (Wacquant, 2009), how they concentrate wealth and power, its implication in neo-colonial geopolitics (Mohanty, 2013) and the entrepreneurial, consumerist, individualised vision of the subject and the citizen which they create (Giddens, 1991, Bauman, 2000; Rose, O'Malley, and Valverde, 2006; Harvey, 2007; Beck, 2009; Gane, 2012, 2014).

The Internet and the World Wide Web grew up in the shadow of these ideas, and the governance regimes and shape of the Internet which grew up over the 1990s are reflective of this (Von Bernstoff, 2003; Chenou, 2014). This can be seen in much of the neoliberal discourse which surrounded the Internet in this period, which framed it not only as enabling free markets but, through a kind of technological determinism, embodying open and decentralised structures which inherently promoted democratic and free market capitalist forms of society.

> Liberty will be spread by cell phone and cable modem… We know how much the Internet has changed America, and we are already an open society. Imagine how much it could change China…. Now there's no question China has been trying to crack down on the Internet… Good luck. That's sort of like trying to nail jello to the wall.
>
> Bill Clinton, speaking in 2000, quoted in John Lanchester (2019)

Many of the foundational policy papers and documents which led to the formation of core Internet governance organisations like ICANN are explicitly neoliberal in sensibility, imagining the Internet as facilitating the proliferation of free markets and competition (Pickard, 2007; Chenou, 2014). This extends both to the *purpose* of the Internet, but also to the way it is administered, largely delivered by private companies competing in a free market. However, the ways in which the Internet and online power have developed since Clinton's speech in 2000 show up the tensions within neoliberal visions of society and how easily these free and decentralised structures can be repurposed for control and repression.

## Waging the Cryptowars – the Internet as a crisis of control

The commercialised, global Internet soon began to pose problems for the very nation states which had championed it. In order to realise these visions of an Internet which might underpin business, commerce, and communication in global free markets, robust mechanisms for securing this traffic from eavesdroppers were vital (Thomas and Wyatt, 1999). The cryptographic technologies invented by the Cypherpunks and academic researchers took on a new importance outside their traditional military applications. For much of the 80s and 90s, cryptographic protocols remained classified by the US as munitions for export purposes, a hangover from the period following WWII, when such technologies were nearly exclusively in the hands of the military and the US was loath to allow other nations to take advantage of them (De Nardis, 2007). With the invention of the World Wide Web in 1989, its release to the public in 1991, and the release of the Mosaic web browser in 1993, Internet use began to spread beyond businesses, the military, academics and hobbyists, and a burgeoning consumer market emerged (Berners-Lee, Fischetti, 2001). Encryption technologies, suddenly vital for business and citizen use of the Internet, posed a number of issues for law enforcement and the military as they fell into the hands of the public (Monsees, 2019).

In particular, law enforcement, intelligence and government agencies in the US viewed this as a direct threat to the ability of the criminal justice system to maintain order, protect national security, and investigate crime. The creation of social spaces and forms of communication which could not be surveilled posed what appeared to many policymakers as an unacceptable hurdle to the gathering of intelligence (De Nardis, 2007). This resulted in a range of attempts at policymaking in order to permit the use of encryption for security and the protection of consumer and business privacy, but also to allow the law enforcement agencies and intelligence services access to communications and data *in extremis*. This marked the beginning of the Cryptowars, a protracted series of attempts by governments (especially in the US) to compromise and weaken encryption, which still continues to this day (Swire and

Ahmad, 2012). These proposals ranged from physical compromise of machines through technologies like the Clipper chip (which would allow authorities access to encryption keys), to limiting the strength of encryption allowed for sale to consumers, to the 'backdooring' of encryption technologies (by which secret weaknesses would be built in that could be exploited (Saco, 1999; De Nardis, 2007).

These inevitably came up against material and moral constraints. Firstly, it is widely considered by cryptographers to be impossible to weaken encryption systems and plant backdoors in ways which could not also be taken advantage of by organised crime, hackers, rival corporations, and other malicious actors (Rivest, 1998; Swire and Ahmad, 2012). Secondly, the removal of privacy protections from mass populations of citizens conflicts with widely-held sensibilities and conceptions of legally-protected human rights within liberal democracies (Raab, 1997; Nissenbaum, 1998; Hoboken, 2016). Thirdly, the argument that encryption technologies are an existential threat to law enforcement's capabilities is undermined somewhat by the fact that such protections in practice do little to frustrate tried-and-tested forms of investigation, such as human intelligence gathering and targeted surveillance, and more novel approaches such as the compromise of machines with malware. What encryption technologies mostly threaten is novel modes of surveillance-at-scale (Guerses, Kundnani and van Hoboken, 2016).

As these efforts ramped up over the 1990s, they galvanised substantial resistance both from within the technical and academic community and from civil society groups. In particular, it led to a call-to-action from the Cypherpunks, who attempted to resist across a variety of domains. In addition to policy engagement, lobbying, and legal action, they continued to develop and popularise the use of encryption technologies (Levy, 1996; Bartlett, 2016). They also used more creative methods of resistance, including eye-catching stunts, such as undermining the export regulations on strong cryptography by having the code of encryption programs printed on T-shirts, which would hence allow them to fall under constitutional protections for speech and expression (Burgers and Robinson, 2018). Despite some abortive

attempts at controlling encryption, these battles have generally favoured the Cypherpunks, not least because their interests overlapped with those of businesses, and with the dominant neoliberal ethos of *lassiez faire* state control and globalised free markets. As a result, the Internet as it exists today is supported by strong encryption technologies, which secure browsing, commerce and communication by default for most applications and users. Nevertheless, state attempts to push back on this have been frequent, flaring up particularly in recent years. As I discuss towards the end of this chapter, liberal democracies have increasingly put pressure on the Internet giants which have taken over responsibility for much of online space to backdoor their platforms and compromise their encryption protections to allow access to law enforcement (Lyon, 2015; McLaughlin, 2016). It is at this point, in the mid-1990s, that Tor's involvement in this history begins in earnest, with the Onion Routing project.

## Onion Routing and Tor

### Onion Routing – anonymity loves company

In this section, I discuss Tor's place in this history of the Internet, building on the previous discussion of the Internet's formative years and discourses to discuss how Tor came to exist, and its early life. I first discuss the Onion Routing project, Tor's early precursor, and then the foundation of Tor, how it has grown, and some of the challenges it has faced.[4]

While the Cryptowars were heating up over the 1990s, the US military and intelligence services were engaged in solving a separate problem: anonymity. Much

[4] Much of the history of Tor and Onion Routing in this section is informed by interviews with members of the Tor Project and the historical information and mailing lists archived at www.onion-router.net and www.torproject.org

as with the development of the Internet's traffic routing model itself, a decentralised model for *identity* and *traceability* has notable security and resilience benefits for military uses. The centralisation of the Internet around ISPs and the inherent traceability of communications poses the same problems for the military as it does for human rights activists and privacy-conscious citizens, granting the government of a nation state a substantial capacity to observe the Internet within its own borders Demont-Heinrich, 2002). This design works well for the US state's domestic interests, as it allows the government to establish itself at key control points and surveil user traffic, however the spread of the Internet around the world has also given non-US states this power over their domestic communication networks (Thomas and Wyatt, 1999). This means that US intelligence and military personnel abroad who want to make contact with their handlers in the US or communicate with base have a problem if they do so using the Internet.

While encryption technologies protect the *content* of messages, the *metadata*, the administrative information which these messages use to route themselves to their destination, can in fact be extremely revealing (Edman and Yenner, 2009; Lyon, 2015). For example, if a CIA spy is in a foreign nation and sends a message over the Internet back to the CIA's home servers, ISPs in this nation can observe this and deduce who they are. Protecting this routing information from surveillance is extremely difficult, as the signals need to be able to travel through the Internet to their destination and so at least some of this information needs to be exposed. Even if the US government were to run their own network of servers which could hide their users' traffic, this would not solve this problem. In practice, this would simply mean that the authorities would observe someone connecting to the CIA's secret anonymisation network, and hence become even more suspicious (Dingledine and Matthewson, 2006).

As a result, an *anonymity* system cannot only be used by the US military, or even by people in the US, rather, it has to be open to as wide a range of users as possible so that the fact that someone is using the system doesn't reveal anything about their

identity. Thus, rather than an encryption system, which could conceivably remain a military-only technology, an anonymity system requires a diverse base of users (Dingledine and Matthewson, 2006). This philosophy, of a system open to the general public, in which small numbers of high-risk users could hide in cover traffic from more everyday users, underpins what became the Onion Routing paradigm, the predecessor to Tor. Work on the Onion Routing design began in earnest in 1995, led by Paul Syverson, David Goldschlag, and Michael Reed at the US Naval Research Laboratory. This early work led to the publication of a design paper for Onion Routing called *Hiding Routing Information* at the First Information Hiding Workshop in 1996 (Goldschlag, Reed, and Syverson, 1996)). Onion Routing has undergone many changes and refinements over the years, however the basic principle involves wrapping the routing information which packets of internet traffic use to navigate the Internet in layers of encryption: the layers from which Onion Routing gets its name. This is then sent into a network of Onion Routers: servers, or "relays" located around the world which bounce the traffic around between themselves, each decrypting a layer of encryption to reveal the address of the next server in the network, until the final server reveals the destination of the traffic and makes a connection to the target web service (Dingledine, Matthewson, and Syverson, 2004).

This serves to separate the information used to route signals from the identity of the user. Each relay involved in carrying the signal only has access to the previous and following steps in this chain: the first relay knows the identity of the person entering the network, but not where they are going, middle relays only know the identity of other relays within the network, and the exit relay knows the final destination, but not the user who made the request. This means that no single part of the infrastructure has both the identity of the sender and the identity of the receiver (Goldschlag, Reed, and Syverson, 1996). If these servers can be set up in countries around the world, this means that an adversary would have to have a 'global' view of all Internet traffic in order to deanonymize the users. Equally, this means that this network infrastructure could not be run by the US Navy, as only people who trust the US Navy would use it. For a CIA agent to use Tor without suspicion in non-US nations,

for example, there need to be plenty of citizens in these nations using Tor for everyday Internet browsing.

This ethic of widespread adoption, making the Internet a more private space for its users, meant that the US military had mutually overlapping interests with a range of groups to whom it might traditionally be considered to be opposed, particularly the countercultural 'cypherpunks', a loose association of academics, security researchers, technologists, and privacy activists. Having met several members of the cypherpunk community at the Symposium on Security and Privacy in Oakland, California in 1997, the NRL developers discussed the possibility of collaboration, to establish what kind of system the military could create which would actually be used by the privacy-conscious general public. This culminated in the Onion Dinner, a meeting during the Symposium on Security and Privacy (including a range of onion-themed food) in which the potential goals and futures of Onion Routing were discussed in depth[5]. Several of the cypherpunks would play a long-term role in the efforts to create Tor, and while the development remained largely with the NRL scientists in the 1990s, they played a vital role in reviewing and shaping the direction these efforts took. The birth of Onion Routing therefore represents a confluence between two distinct but overlapping, visions of the Internet: the interests of the military, and those of the cypherpunks.

The ways in which these two groups see the Internet are not in fact that different. Both the cryptographers working as US military researchers and those of the Cypherpunks had a deep technical understanding of computer systems, and were attempting to make changes to the structures of these systems in order to undermine the ability of nation states to exert centralised control over the Internet infrastructure. In one case this was to support the geopolitical and military aims of the US abroad, and in the other to promote privacy and resist authoritarian control

[5] A discussion of the Onion Dinner can be found in the or-dev archives at https://www.onion-router.net/Archives/onions-1997.txt

(in the 90s, these were still considered by many to be compatible ideologies). At the same time as one part of the US government was trying to clamp down on encryption, another was developing a technology which would give strong anonymity protections to large parts of the world. This highlights a central tension within contemporary liberal societies between freedom and control, one which would only become more evident as Onion Routing continued to grow.

## The birth and early life of Tor

Moving past the 1990s to the early years of the new millennium, the Internet was entering a new era. The bursting of the Dot Com bubble (Goodnight and Green, 2010), global recession, and the September 11th attacks signalled the end of the techno-optimism of the 1990s, and the utopian visions of the Internet began to give way to a rather bleaker picture of surveillance and control (Scordato and Monopoli, 2002; Ball and Webster, 2003; Lyon, 2005; Yar, 2012; Zureik and Salter, 2013). At the same time, development work on the next generation of Onion Routing was beginning. In 2002, the developers of Onion Routing at the Naval Research Laboratory, in collaboration with Roger Dingledine (a developer from the Free Haven project), Nick Mathewson, and a handful of other developers, set about designing and developing an implementation of Onion Routing intended for much wider use than the test networks which had been attempted throughout the late 1990s, with scrutiny and assistance from some of the remaining cypherpunks, such as Lucky Green. The main contributors on the development mailing list in these early days were Nick Matthewson, Roger Dingledine, Andrei Serjantov, Paul Syverson, Matej Pfajfar, and Rachel Greenstadt. This built on an initial codebase produced by Matej Pfajfar at the University of Cambridge as part of an undergraduate dissertation project.

The early design work of Tor is recorded in substantial detail in archived mailing list discussions which are freely-available on the Tor Project website. Although Onion

Routing was by this point fairly well-established within the research community as a paradigm for anonymity systems, no truly wide-use system had yet been developed. In building something which went beyond a prototype, the Tor developers needed to make a number of decisions about the practical implementation of Onion Routing in a real infrastructure. I discuss these decisions in detail in Chapter 7. This took place over a series of mailing list discussions from 2002 onwards (and the development of Tor is still ongoing on the same list). This development is documented extensively on open, freely-accessible public mailing lists, with Tor remaining an open source project to this day and embodying many of the practices of the Open Source movement, which I discuss in more depth in Chapter 8. After the launch of the Tor network and the publication of its codebase in 2003, the organisation continued to grow, beginning to receive funding from the Electronic Frontier Foundation in 2004[6], and founding the Tor Project in 2006 to manage development and support. The potential for Tor to be a tool for liberation, helping activists and journalists in authoritarian nations, and whistleblowers in liberal democracies, was becoming even more evident over this period, and this became a key focus of Tor's development and public goals. While there was a focus on Tor's potential as a human rights technology from these early days, this more politically engaged sensibility was within the context of a fairly 'broad church' community which welcomed contributions from those with a range of views and political standpoints.

Once Tor was released to the world, the community needed to expand beyond the developers and researchers working on the software on which Tor depended. To make its vision a reality, Tor needed *infrastructure,* which meant that it also needed people to maintain and administer it. Due to their desire to attract as large and diverse a community of network operators as possible, and their understanding that many potential users would not trust a service run by a US organisation, the Tor developers decided to have the network entirely run by volunteers, with the Tor Project minimising their involvement in running the network as far as possible.

---

[6] https://www.eff.org/press/archives/2004/12/21-0

Equally, unlike other anonymity networks, there was no formal sign-up procedure for relay operators, who (while scrutinised by Tor for suspicious activity) are able to add relays to the network without providing proof of identity. The initial Tor network pulled relay operators from the existing Mixmaster and Mixminion projects, and although at the start the developers knew most of the operators, as the network grew other people began to contribute.

Throughout this period, Tor was steadily growing in popularity, with the relay network reaching around 160 nodes by mid-2005, and tens of thousands of daily users. Despite this, Tor was initially fairly difficult to use, relying on making a number of different tools work together. This was both a problem in terms of its initial design, which relied on as wide and large a community of users as possible for its privacy properties, and also from the perspective of those who wished to see its protections extended to as wide a community as possible, rather than just becoming a high-tech security tool for experts.. This led to the creation of the Tor Browser (led by Steven Murdoch), released in 2008, which integrated these components into a single easy-to-use program which could be downloaded from the Tor Project website. Another development in Tor's design which would prove pivotal in the years to come was the development of Onion Services. Originally developed as somewhat of a hobby project by Roger Dingledine, Onion Services allow the hosting of services on the Internet which are extremely difficult to locate or shut down. They do this by forming a connection through the Tor network in much the same way that Tor users do. This creates a rendezvous point within the Tor network to which users can form connections, protecting both the identities of the users and the providers from one another. These Onion Services have a range of potential uses (both licit and illicit), which I describe in Chapter 2.

It did not take long for Tor to come into conflict with the world around it. First came a wave of DMCA complaints and other abuse notifications directed at the relay operators, as the automated systems which manage the Internet picked up the illegal activities of some Tor users and traced it back to the Tor network. Tor then

began to come into conflict with other networks and services, as a subsection of its users began to use its anonymity protections for vandalism and abuse. For services such as Wikipedia, this meant blocking edits and comments from users connecting through the Tor network; a potentially deeply worrying problem for Tor, which depended on the 'network effect' which came with being able to connect to as many other services as possible. Onion Services were also becoming a serious public relations issue for Tor. A community of libertarian techno-utopianists who believed in total freedom from state regulation of commerce had used this technology to set up cryptomarkets where drugs could be bought with what appeared to be total impunity from law enforcement. These saw widespread media attention, especially the infamous Silk Road market, and were one of the key developments in the rise of Tor's construction as a crime problem in the public eye (Munksgaard and Demant, 2016). The romantic figure of the Silk Road's administrator, the Dread Pirate Roberts, made for compelling headlines across the world, with substantial publicity following his arrest. While law enforcement have generally been able to shut down these cryptomarkets, the ease of creating these Onion Services and potential for substantial profit have led to cryptomarket trade quickly displacing to new markets as old ones have shut down, and the media and Tor has as a result become associated with crime, often referred to in reporting and academic research simply as 'The Dark Web'.

As its popularity has increased, Tor has also become a go-to tool for security researchers and police officers investigating online crime. It is important to emphasise here that the vast majority of crime online occurs on the "Clearnet" (the regular Internet) rather than on Tor Onion Services, and as a result the protections which it offers are particularly useful for law enforcement attempting to gather intelligence on illegal conduct on Clearnet websites who wish to hide the fact that they are connecting from police servers (Watson, 2012; Minarik and Osula, 2016). Equally, the protections which Tor provides are extremely strong, but do nothing to protect users from other law enforcement techniques such as human intelligence gathering, manipulation, targeted surveillance, and actions against pinch points in

physical infrastructures such as the postal network. Despite this, Tor has also achieved a somewhat totemic status among the 'hacker underground', both for the security protections it provides and for its implicit anti-authoritarianism, and Tor has become a cultural force in its own right, featuring in rap songs (Pitchfork, 2019)[7], films (including Michael Mann's *Blackhat* and more low-budget fare, such as Susco's *Unfriended: Dark Web*), and television programmes (including the Netflix show *Dark Net*). It has also seen substantial use by whistleblowers, journalists, and human rights activists, and has become a core part of many organisations' 'security toolkit'[8] (Jardine, 2018).

Finally, in addition to the anti-surveillance protections it provides for those browsing the Internet or hosting their own Onion Services, Tor has an additional property: it has become a powerful tool for circumventing censorship. A side-effect of the way which Tor works is that, by routing user traffic around the world, it also evades attempts by nation states to block access to web services: as long as a user can enter the Tor network, they can largely access whatever services they desire. This works both at the national scale, allowing access to websites blocked by ISPs under orders from governments, and at the local level (Chaabane et al., 2014; Fifield et al., 2015). As a result of this property, Tor is blocked by a small number of governments who maintain a regime of strict control over Internet access, most notably China, which blocks Tor access entirely (Afroz and Fifield, 2007; Winter and Lindskog, 2012). As the Tor network's relays are publicly visible, blocking access to Tor is fairly easy, however Tor has developed a range of mechanisms for circumventing this blocking, such as a semi-secret list of 'bridge' relays which allow people access to the Tor network where direct connections to the public relays are blocked, and tools such as pluggable transports, which disguise Tor signals as other kinds of traffic (Murdoch and Kadianiskis, 2012).

---

[7]Teejayx6's track *Dark Web* can be accessed at: https://www.youtube.com/watch?v=ubs9b-ssuuM&feature=emb_title

[8] For example, Tactical Tech's 'Security in a Box': https://securityinabox.org/en/

Instead of understanding Tor as a technology balanced between prosocial and harmful use cases, I frame Tor instead as an infrastructure which acts as a home for a range of diverse visions of potential futures: at the same moment embodying a vision of libertarian, regulation-free marketplaces for drugs, helping US to subvert centralised control over the Internet in hostile nation states for the benefit of its military and espionage, creating a space for human rights defenders, journalists, and activists around the world to communicate and organise, realising a vision of the Internet where everyday users can browse and participate in democratic society free from censorship or surveillance, and undermining the visions of law enforcement of an Internet in which crime and harm can be governed at scale through surveillance and censorship. These visions have not been static, and as the mechanisms through which nation states and powerful actors have sought to control the Internet have evolved over the past two decades, so has Tor's place in the Internet and in broader society.

# The rise of control

## The Snowden leaks and mass surveillance of the Internet

In the years since the 9/11 attacks, the US state had been undergoing a profound reorganisation of its approach to security, control, and geopolitical power online (Brodeur, 2007; Schuilenberg, 2017). The full extent of this was revealed by one of the most significant events for the Internet of the 21st Century so far. In 2013, Edward Snowden, a contractor working for the NSA, leaked a substantial number of Top Secret internal documents relating to US communications surveillance to the Guardian and the Washington Post (Lyon, 2014). In doing so, Edward Snowden, who would soon become the face of a new online privacy movement, revealed three key facts about US surveillance practices. Firstly, the US government and other Five Eyes nations had developed arrangements with telephone and Internet communications providers and platforms to share vast quantities of personal data with them, and set

up other collection mechanisms, such as the Tempora programme, which involved the tapping of the undersea Internet cables between the US and the UK by GCHQ. Secondly, this underpinned the collection of huge amounts of information about the telephone calls, browsing habits, and communications of large swathes of the world's population, which were being processed and fed to systems through which intelligence officers could browse with very little in the way of safeguards. Thirdly, this surveillance relied on deep data-sharing relationships between the Five Eyes nations and extended both to surveillance of politicians and everyday citizens in nations outside the Five Eyes (including their allies), and to the citizens of these nations themselves (Lyon, 2015; Greenwald, 2014).

What Snowden revealed was the enormous, hidden scope of a general process of *securitisation* which had been ongoing since the turn of the millennium, through which liberal democracies, in particular the US and the Five Eyes nations had been engaging in a range of ways to reassert their sovereignty and retain control over the Internet (Deibert, 2008; Schuilenberg, 2017), pulling it into the *surveillant assemblage* (Ericson and Haggerty, 2000), the heterogeneous set of sites and control points where the state records the flows of data generated by people's everyday lives (Lyon, 2015). In particular, the collection and processing of enormous amounts of communications metadata (the administrative information, such as time of delivery, identities of conversational participants, and location, attached to communications) in the US and around the world was revealed to have become a key part of the US national security strategy. This was exactly the problem identified by the developers of Onion Routing in the 1990s: this administrative information is often even more revealing than the content of communications (Schneier, 2014; Lyon, 2014, 2015). Especially when pored over by algorithmic systems, the timings of who was talking to whom and when could reveal characteristic patterns of behaviour which were a powerful form of intelligence of their own.

This had implications for policing as well as for national security. The well-documented jurisdictional issues which police face in maintaining order and

investigating crime online (Jewkes and Yar, 2012; Wall and Williams, 2013) are compounded by the fact that the Internet is largely delivered and administered by private and non-profit organisations (Wall, 1998; Hoar and Hope, 2002). This devolution of responsibility away from state-run services accords with the free-market supremacy of neoliberal ideology but presents states with problems for maintaining online order, as these organisations have control over the vast amounts of administrative information which law enforcement and security services feel they need to establish a view of what is actually happening on the internet at any given time, to develop intelligence leads, and pursue investigations. While throughout the 1990s this took the form of targeted subpoenas by police for these platforms' customer records, since the World Trade Centre attacks in the US this had increasingly been the domain of what criminological research terms *high policing* (Brodeur, 2007). High policing, as opposed to low policing, which involves more traditional police work, is characterised by a focus on gathering and processing large amounts of intelligence, the conflation of separate legislative, executive and judicial powers, the framing of their role through security, rather than crime, and the use of informants (Brodeur 2007).

After the end of the cold war and increasingly since 9/11, the distinction between high and low policing has been increasingly blurred (Brodeur, 2007). In tandem with the collection mechanisms and intelligence gathering which Snowden documented, policing had been attempting to adapt to the Internet, a domain to which traditional police practices were ill-suited (Wall and Williams, 2013; Holt, Burruss, and Bossler, 2015; Jewkes and Yar, 2012). Law enforcement adapted to this by establishing centralised bodies, either within, or with links to, high policing bodies such as the UK's Government Communications Headquarters (GCHQ) and National Crime Agency (NCA), or the US's National Security Agency (NSA) and Federal Bureau of Investigation (FBI) (Wall and Williams, 2013; Levi and Leighton Williams, 2013; McGuire, 2016). With intelligence services becoming more involved in policing transnational serious and organised crime, and local policing increasingly devolving more specialist functions to centralised units such as the NCA, this means that the

tools of espionage, automated mass-scale data gathering and processing, were (and are) increasingly being used for policing functions (Brayne, 2017; Ferguson, 2019).

This places the private companies running platforms and infrastructure at a key control point in the operation of power in the Internet age (DeNardis, 2009). Where states have devolved the provision of public infrastructure to private internet companies, a countervailing trend throughout the War on Terror has been their reassertion of authority and mechanisms of control through the establishment of intelligence-gathering relationships between state security services and private infrastructural companies (Lyon, 2015; Schuilenberg, 2017). In practice, the co-option of infrastructure, service, and platform providers has taken two key forms: first, the security services attempted to compromise the technologies, either through directly compelling companies to backdoor their tech, or indirectly through wiretapping and state hacking (Lyon, 2015). Secondly, they attempted to develop sympathetic relationships with the organisations, through establishing liaisons, serving formal subpoenas or data requests, and getting people within them with whom they can negotiate (Greenwald, 2013). Both of these involve the collection of bulk data on users of the internet, and targeted data about particular high-value individuals, as well as the capacity for "target discovery" (Schafer, 2016). Through developing wide-reaching novel surveillance capabilities, the Five Eyes nations had developed automated, scalable mechanisms for administering the business of intelligence gathering and crime control under the auspices of 'national security' (Greenwald, 2013; Lyon, 2014, 2015).

The revelation of these capabilities had deep consequences for Tor as a technology and an organisation. Most importantly, it brought issues of online surveillance to the forefront of public debate for months, allowing Tor to reposition itself as at the forefront of a massive civil society campaign against mass surveillance. From being vulnerable to criticism that it was being used for illegal and harmful activities, Tor suddenly had a powerful articulation of the moral justification for its existence which was on the front page of most major newspapers in the world (Greenwald, 2013).

The backlash to the practices revealed in the Snowden documents brought with it a growing critique of online surveillance, and especially the role played by private platforms and infrastructure providers, which has only continued to grow (Lichka, 2015, Dencik and Cable, 2017). Tor itself received not-inconsiderable free advertising in these documents, featuring prominently in the Snowden leaks, where it is described in a NSA Top Secret briefing as "the king of low-latency anonymity – there are no contenders to the throne" (Guardian, 2013). These documents also revealed a wide-ranging research programme within the security services of the Five Eyes nations focused on attempting to find ways to undermine the Tor network. This has also changed Tor significantly as an organisation, leading to a wave of people, especially those with a background in policy work, lobbying, and activism joining the community. Finally, it provided the largest trove of material intelligence to date on the actual practices of security services against which Tor was trying to develop technologies to defend.

## Surveillance capitalism and the new platonic guardians

Bringing this history to the present day, we arrive at an Internet in a deeply contested moment, when many of these issues of power and control are coming to a head. The way in which people use the Internet has changed dramatically since the 1990s (Agger, 2011; Vincent and Haddon, 2017). From something which could be considered a discrete space of its own by its users, the Internet has exploded into a network which is embedded in every aspect of contemporary high-tech societies and is now largely accessed through ever-present mobile phones rather than static computers (Hine, 2015). In tandem with this proliferation has been a profound centralisation, with the 'Web 1.0' of static websites, individual homepages, and a glorious mess of small services and sites having given way to an Internet which for most people is hosted or mediated through a small number of enormously powerful companies (Boyd and Ellisson, 2008; Barassi and Trere, 2012; Moore, 2016; Moore and Tambini, 2018; van Dijk, Nieborg, and Poell, 2019) . The neoliberal free markets

of the Internet have condensed into monopolies around the Internet giants of search, for which Google now has a near-monopoly, social media, dominated by Facebook, Instagram and Twitter, commerce, through Amazon and Paypal, and a range of other 'disruptive' services such as Deliveroo, AirBnB, and Uber. Many of these companies drew heavily on the hacker ethic's 'disruptive' sensibilities, seeking to break up existing power structures in, for example, journalism or the music industry, or invent pioneering, creative new platforms for human interaction, community, and financial gain (Marwick, 2017).

The rise of social media in particular has been behind many of these transformations in the way the Internet fits into public life. 'Content' - the stories, videos, music, and other information which people consume online - is now increasingly not created by platforms and websites themselves, which instead act as a hosting service for user-generated content of different kinds (Ritzer and Jurgensen, 2010; Ritzer, Dean, and Jurgensen, 2012; Ritzer, 2015) . As a result, and supporting their disruptive innovation by allowing them to undercut traditional providers, many of these services are provided extremely cheaply, or for free. This means that they need to make money in other ways. Shoshanna Zuboff's (2016, 2019) work documents at length the rise of a business model which she argues is a novel form of capitalist exploitation, coining the term *surveillance capitalism.* This involves these platforms using the enormous amounts of personal data about behaviours, interactions, and demographics which their infrastructures handle in conjunction with 'algorithmic' methods of processing to create very detailed individual profiles of their users. This includes both data which users directly host on these platforms, and a range of 'tracking' mechanisms through which the platforms download tracking software ('cookies') onto users' computers and follow them around the web. These profiles then provide the raw material for a market for extremely finely targeted advertising – this advertising revenue is what sustains the current platform economy (Zuboff, 2016, 2019).

The collection of this personal data and the creation of these intimate profiles of opinion and behaviour create a substantial capacity for abuse. While criticism from academia and civil society had been growing, this was brought to a head by the Cambridge Analytica scandal, in which a company had engaged in massive data farming without consent through an application, facilitated by Facebook's systems, which allowed them to target political advertising illegally (Cadwalladr and Graham-Harrisson, 2018; Isaak and Hanna, 2018; Laterza, 2018). This added fuel to the fire of a wider critique of the increasing surveillance-based governance of society. There is a substantial and growing literature within digital society scholarship and 'critical algorithm studies' which draws attention to the problems with these models of governance, which involve collecting enormous amounts of information and using machine learning techniques to, variously, 'predict' crime, tailor insurance prices, direct healthcare, and change behaviour in ways which have a veneer of 'neutral' scientism, but in fact often exacerbate existing inequalities (see for example, Gillespie and Seaver, 2016; O'Neill, 2016; Brannon, 2017; Wachter-Boettcher, 2017; Williams, Brooks, and Shmargard, 2018; Eubanks, 2018; Noble, 2018).

All of this represents an increasing critique of the rise of the engineers who design and develop these platforms as arbiters of power. The disruptive ethos (as typified in Facebook's old motto, 'move fast and break things') has increasingly transformed as these people and their platforms have gained real power: they have become administrators and governors, increasingly taking responsibility for the huge (sometimes billions of people strong) communities on their platforms (Kohl, 2013). Having spent many years attempting to avoid responsibility for policing their communities, they are increasingly finding themselves forced into this role (Trottier and Fuchs, 2014, Chapter 1; Wagner, 2013). While they are often described in media profiles as 'philosopher-kings' (see for example, Adams, 2018), this largely reflects the self-valorisation of a very small number in the Bay Area tech elite, and in fact a more fitting term might be 'platonic guardians', reflecting the existence of a wider class of software engineers, data scientists, and infrastructure and platform developers who are increasingly taking on an important governmental role in

society. Loader (2005) uses the term 'platonic guardians' to describe the rise and fall of a particular elite group of experts in shaping criminal justice and the governance of crime across the second half of the 20th Century. Much like these platonic guardians, the engineers designing and implementing these platforms and their 'algorithmic' management technologies represent a group that presents itself as a neutral, expert elite on whom the state draws; one possessed with a particular claim to a particular kind of knowledge, and who view themselves as steering and shaping society.

Across recent years, as these transformations have been ongoing, Tor has also changed considerably as an organisation. Tor increasingly sets itself against not only government surveillance, but also the efforts of private sector organisations such as Facebook to surveil their users. This is evident both in the published materials which set out Tor's aims as an organisation and also in their development work; substantial work has gone into adapting the Tor Browser to defend against surveillance and tracking by these private platforms. Tor has also taken steps in recent years to professionalise as an organisation (which I describe in more detail in Chapter 6), instituting a range of changes to working practices, reporting, and management culture within the Tor Project. In remaking itself from a fairly loosely-organised free software project to a modern NGO, Tor has placed a far greater emphasis on branding, usability, and messaging, and has begun attempts to move further away from US government funding (which still makes up a large percentage of their income) and towards a more diversified, crowdfunding-based model.

## Conclusion

The picture which this history paints is a deeply contested one, in which the infrastructure of the Internet has been a focal point within liberal democracies for the working through of the essential contradictions and tensions within liberal thought: between control and freedom, centralisation and decentralisation,

openness and closedness, market and monopoly. Issues of privacy, control, and freedom and how they are realised in infrastructure are at the heart of the Internet and its salience to social, political, and economic life. As I argue at the beginning of this chapter, Tor itself poses much more interesting questions for criminologists than the crime and harm in which it is implicated. It embodies in a particularly pure form many of the less well-understood criminological issues for the Internet, such as the role played by infrastructure and platform providers, how they fit into relationships of governance and power in contemporary societies, how they cope with the increasing responsibility they have for policing their platforms, and for the crime and harm in which they become implicated. In this thesis, I explore how Tor actually fits into these questions of power, crime, and harm.

The formative discourses of the Internet represent a meeting of several different groups and perspectives. Given the pivotal role played by the US in this history, it is unsurprising that many of these are reflective of versions of *liberal* thought (including the related schools of *libertarian* and *neoliberal* ideology). The dominant voices shaping the Internet as it stood in the 1990s gave rise to a marketized Internet which embodied utopian visions of the spread of liberal capitalist democracy around the world. Tor itself arose from a collaboration between the cypherpunk movement, whose anti-authoritarian focus on privacy mandated strong protections for Internet traffic, and US military researchers, who sought to create a tool for the protection of US personnel abroad and the undermining of authoritarian nations' control over their citizens' communication. As Tor grew and became the go-to online privacy technology, the US state's vision of the world was also changing, emphasising the primacy of control, the increasing securitisation of society, and the development of wide-ranging practices of surveillance, as revealed in the Snowden documents. These practices relied on the centrality of Internet Service Providers and the increasingly-powerful platforms such as Google and Facebook, and their developing model of surveillance capitalism, which provided a wealth of information on citizens which could be exploited both for advertising revenue and for the cultivation of intelligence by law enforcement and security services. Tor has positioned itself at the vanguard

of resistance to these developments in control, and increasingly articulates itself as an attempt to imagine (and realise) an alternative future for the Internet through infrastructure.

The priorities, discourses, and motivations of US law enforcement, military, and intelligence services – in short, the concerns of US sovereign power – have played a disproportionate role in shaping the history of the Internet. While the system designs which meet these concerns have often taken a shape which aligns with that of groups like the cypherpunks, prioritising decentralisation of control and distributed trust, this does not stem from any particular enthusiasm for these kinds of systems. Rather, the interests of US sovereign power are in reshaping power relationships and designing systems which allow them to establish themselves at key control points, to undermine the control of rival actors, and to ensure the resilience of their own infrastructures. However, as Donna Haraway's (1991, 1997) scholarship advises us, infrastructures and technologies are rarely the product of a single vision, nor are the possibilities they hold for the future anchored solely in the aims of a single group. Tor (and the Internet more broadly) is a repository not only for these visions of a reasserted US liberal world order at a time when it appears to be faltering, but also of a range of other potential visions, such as the radical, crypto-utopian cypherpunks, the hacker underground, the US military, and Internet freedom activists.

This history has drawn on both the discourses which have shaped the Internet and the types of structures which the Internet has taken as it has evolved. Tor can be understood as an attempt (both by govt and civil society) to act on this structural level: to decentralise power and to disrupt established mechanisms of control. However, the discourses and material structures I describe in this chapter are represented at a fairly high and abstract level: *neoliberalism*, *surveillance capitalism* and *crypto-freedom*; *centralised* or *decentralised.* The empirical work of this thesis takes this discourse in the Foucauldian sense, as a contextual macro-level framing device, but it then attempts to study Tor and how people make sense of it at a much deeper level, that of Giddens' discourse at the micro scale, engaged in real practices,

beliefs, and ideas. In Chapter 2, I describe this as attempts at "doing politics" through architecture (Musiani, 2013), "weapons of the geek" (Coleman, 2017), or "stealing the fire" (Milan, 2013), and in my results chapters I explore how these attempts actually work in practice: the specific ways in which the Tor community makes sense of Tor as a technology, how they understand the kind of action in which they are engaged, the ways in which this shapes the material form which Tor takes, and how they navigate the problems which arise.

In mapping how Tor aims to realise a vision (or visions) of the world through building infrastructure, I draw on deep empirical research in the Tor community, including both interviews and extensive archival research. To make sense of this, I use frameworks from Science and Technology Studies, in particular the work of Susan Leigh Star and Social Worlds Theory. In the following Chapter, I set out my theoretical framework in depth: the conceptual tools through which I explore materiality and meaning within the human and technical infrastructures of Tor.

# chapter 4
# theorising the social life of infrastructure

## Introduction

Technologies and infrastructures have a rich social life, but one which is not always easy for researchers to access (Star, 1999). In this chapter, I set out the theoretical framework through which I explore Tor, and which guides my empirical research and analysis. While there has been a substantial body of research, which I sketched in the previous chapter, into the changing ways in which Internet governance and crime have evolved, there has been very little criminological research which engages in depth with the platforms and infrastructures of the Internet. Through a Foucauldian lens, the material forms and practices through which power and governance are exerted on the Internet can be understood as reflections of the discourses and understandings of the business of government which underpin them (Foucault 1991). As Garland (1997) argues, this depiction of power is at its most useful when considered as a set of ideal types, used to frame analysis at a lower level which shows the partial, contested ways in which these discourses are materialised and worked out in practice.

While I have mapped out the key discourses which have played a role in shaping the broader history of the Internet and of Tor, this thesis dives well below this contextual level, investigating the actual ways in which a particular part of the Internet infrastructure, the Tor network, is made sense of by the community which develops, supports, and maintains it, and what the consequences of these understandings are. As I argue in Chapter 2, criminology in the late modern era is well-used to pulling

apart complex policy documents and organisational charts; working practices and political processes; architecture and institutions to map the rationalities which connect them to power. However, the analytical and methodological frameworks it uses to do this are not particularly well-adapted to perform this work for Internet communication platforms and infrastructures, as they embed meaning in the material in different ways and rely on forms of technical work where this meaning can be rather difficult to discern (Star, 1999).

In conducting a sociology of Tor through empirical research, I explore how its attempt to "steal the fire" is actually worked out in practice (Milan, 2016). This entails breaking this idea of making a vision of the world a reality through building infrastructure into a range of questions to be answered about Tor and the Tor community. What are the actual values of Tor, below these abstract ideas of crypto-freedom, liberalism, and anti-authoritarianism? How do these values change and in what different ways are they put into practice and made sense of when they are put to work in a technical project: the creation of a real infrastructure? How are they materialised in the design and development of this infrastructure as qualities, practices, and structures of its software and hardware, and of the people who support them? Further questions are generated once Tor's initial design is complete and it is released into the world. To what extent, and through what mechanisms, if at all, does the infrastructure make these values and visions a reality, and what kinds of work are required to support this in practice? What factors enable this to happen, and what shapes the outcome? Finally, what happens when Tor, which situates itself as a direct challenge to existing technologies of control, comes up against the systems which it is trying to subvert and undermine? How do the Tor community understand the crime and harm in which Tor becomes implicated, and how do they navigate these questions of governance? What other problems arise, and how do the people involved make sense of them? Encompassing these is a broader question: how can we make sense of Tor as a site of social action?

In exploring these questions, I draw theoretical frameworks from Science and Technology Studies. In particular, I use social worlds theory, a symbolic interactionist approach to the study of science and engineering communities (Star and Griesemer, 1989). In Chapter 10, I draw on the findings of my empirical work on Tor to reflect on the potential of the social worlds framework as a productive companion to criminological research, expanding and deepening its framing of Internet infrastructures, however here I set out the core elements which I use in this thesis. In this chapter, I first discuss the literature on privacy, situating my theoretical framing of privacy technology within existing scholarship. In the following section, I set out the Social Worlds framework, which provides a "theory and methods package" (Clarke and Star, 2008) through which to separate out the multiple, overlapping, and contradictory ways of sense-making which accrete around infrastructures and scientific projects. Finally, I draw on Star's (2003) concept of 'convergence' to frame how these worlds of discourse go on to shape the material form and design of Tor itself, and the concept of 'performativity' to frame the ways in which Tor might realise its visions of privacy in the world (Law and Singleton, 2000).

## Material privacy – Internet infrastructure and stealing the fire

As I describe in Chapter 3, the Internet has long been a site of political struggle, and issues of privacy and power have been at the forefront of debates about the politics of the Internet. There is a substantial research literature on online privacy, including scholarship on governance and policy (Bennett & Raab, 2017), people's perceptions and experiences of privacy (Viseu, Clement & Aspinall, 2004; Lyon, 2017), and privacy's place in social and political life (Nissenbaum, 2009; Rider, 2018). Although privacy and anonymity are related concepts (and often used interchangeably), I refer to privacy in this thesis using Vedder's (2011) broad definition, as socially constructed category systems pertaining to the control of information about

individuals, with spatial, relational, decisional and informational dimensions, and deep links to social order, power, and culture (Steijin and Vedder 2015).

The research literature on privacy recognises that it is not monolithic, in fact composed of a range of related concepts and values (Solove, 2008) and understood very differently in different contexts and cultures (Nissenbaum 2009; Steijn and Vedder, 2015). Privacy is a core value through which liberal democracies construct their systems of government (though by no means exclusive to them) and underpins many of the conceptions of rights and public goods therein (Wright and Raab, 2014; Raab, Jones and Szekely 2015). The right to a private life, to have control over the intimate information circulated about oneself, and to establish spaces distinct from the 'public' sphere underpin the ability to formulate selfhood and identity as conceived in liberal democracies and to engage in democratic participation free from coercion (Wright and Raab, 2014). While privacy is certainly not confined to liberal democracies, it is crucial to their conception of the state, and a core way through which they differentiate themselves from more authoritarian modes of governance.

This distinction is particularly important for Tor, whose public communications explicitly frame it as both *protecting* privacy within liberal democracies and *providing* it to those in authoritarian nations. Privacy as a value is by no means absolute, even within liberal and democratic nations, and is often balanced against other concerns, such as security and order maintenance (Solove, 2011). For example, the security services and law enforcement are routinely permitted to violate individual privacy in carrying out their duties (Lyon and Zureik, 1996). I distinguish privacy from anonymity, which (as befits privacy technologies like Tor) is the material affordance which allows an individual to control the knowability of their own identity in a given situation (Danezis and Guerses 2010). For the purposes of this thesis, privacy is a predominantly social concept, linked to a range of cultural factors, while anonymity is a narrower material property concerned with the actual distribution of information about people.

Conceptions of privacy, as will be apparent from the history I describe in Chapter 3, have changed substantially alongside the rise of Internet technologies (Lyon, 2007). Lyon argues that the form which the Internet has taken over the past ten years, providing communications platforms which allow and encourage their users to display private information in spaces which are accessible to billions of people around the world has created a 'surveillance culture' (Lyon, 2017), where people actively take part in their own surveillance, and surveil one another as an everyday part of social life. This poses deep problems for the balance of social power; these social transformations are being driven by private companies for financial exploitation and are having potentially harmful effects on vulnerable individuals and social groups, and broader human societies. Lyon argues that they constitute a power grab away from democratic institutions, and are opening societies up to greater control from prospective employers, insurers, law enforcement and security services (Lyon, 2007, 2014, 2017).

As the mechanisms through which states and corporations govern the Internet expand to involve increasingly intimate surveillance of everyday life, the platforms and infrastructures of the Internet have become key sites of resistance, and these struggles are often framed around conceptions of privacy (Lyon 2015; Raab, Jones, & Szekely 2015). There is a well-documented history of privacy as a subject of social action, tied up as it is with ideas about state overreach, law enforcement, and democratic participation (Raab, 1997, Nissenbaum, 2009). This has historically occurred through traditional mechanisms, including protest, lobbying, policy engagement, the democratic political process, and legal challenges in the courts (Saunders, 1991; Garrow, 2015; Leizerov, 2000; Heisenberg, 2005). In this research, however, I explore an attempt to realise a particular vision of privacy through building infrastructure. The Internet freedom movement, a loose arrangement of NGOs, lobbying organisations, and activist groups, engage both in these more traditional routes of resistance, and through supporting the creation of privacy and anonymity technologies (Postill, 2014; Milan, 2016). Although Tor's roots may be in military communications, as far back as the mid-90s this cypherpunk conception of

privacy as crucial to realising the utopian visions of the Internet (and averting its potentially dystopian futures) has been at the core of Onion Routing, and Tor.

Social constructions of privacy are composed of multiple different elements which are understood and put into practice very differently in different contexts and cultures (Nissenbaum 2009, 2011; Steijn and Vedder, 2015). For example, Lewis' work on *Queer Privacy* highlights the radically different types and constructions of privacy valued in the everyday lives of queer people (Lewis 2017), and other researchers have outlined the different ways in which privacy is understood, attached meaning to, and achieved within different religious traditions (Cannataci 2009) and in older and younger groups (Steijn and Vedder, 2015). The Internet freedom movement frames its understanding of privacy in yet another way, as a reaction to developing technologies of control online. There has, however, been little research into the mechanisms by which these understandings are translated into technical properties through design processes. In addition to technical and engineering research on privacy technologies, a small but growing body of research applies sociological approaches to understanding the relationships between social constructions of privacy and privacy as a feature of technological systems. This research posits that privacy properties of technologies are material realisations of their designers' understandings of privacy (Musiani 2010). The social constructions of privacy and anonymity held by their developers are therefore important in shaping the actions and understandings of their users (Bancroft 2017; Pfitzmann and Hansen 2005).

Some researchers have begun to explore the different ways in which developers conceptualise privacy in technological systems (Baer et al., 2009; Danezis and Guerses 2010; Musiani 2012). Danezis and Guerses (2010), for example, document a range of different understandings of privacy in technical systems which have developed since the turn of the millennium (Danezis and Guerses, 2010). This work has also been a fruitful avenue for critique. For example, Guerses, Kundnani and Van Hoboken argue that the conceptions of privacy by contemporary anonymity

technologies are often guilty of reproducing colonial logics which counterpose democratic nations to 'alien' practices of mass surveillance (Guerses, Kundnani and Van Hoboken, 2016) imported from so-callled 'Eastern' societies. They further argue that many of the mechanisms for providing anonymity which anonymity technologies employ are largely designed to protect groups who face less societal oppression, opposing themselves to mass surveillance in ways which implicitly or explicitly attempt to justify "targeted" surveillance which disproportionately affects people of colour (Guerses, Kundnani, and Van Hoboken, 2016).

As I found when beginning my interviews, Tor is not characterised by a single shared set of values, practices, and understandings, or even shared constructions of privacy and its relationship with technology. In separating these distinct perspectives out and mapping the terrain of discourses and values which cluster around Tor, I employ a framework from STS: social worlds theory (Clarke and Star, 2008). This framework takes broader approaches and theory from symbolic interactionist scholarship and develops them within STS to explore complex relationships between sense-making, values, and the material world of science and engineering. Rather than study Tor as a social movement, I study it as a site where multiple different kinds of social action are attempted, of which an activist approach is only one potential frame. In Chapter 10, I discuss in more detail (drawing on my empirical research) the potential contributions which this framework could make for criminological scholarship on technology, the Internet, and cybercrime, however here I set out an overview of its foundations and key ideas.

# Social Worlds

## The foundations of Social Worlds theory: symbolic interactionism

I now turn to the theoretical framework which underlies the research in this thesis, and through which I explore Tor and the Tor community: social worlds theory. This

framework stems from the sociology of the Chicago School, whose ecological approach at the level of city regions went on to incorporate studies of micro-scale interpersonal interactions and how they contributed to group-level meaning-making (Deegan, 2013; Mathews, 1977; Park and Burgess, 1921; Plummer, 2000; Clarke and Star, 2008). The *symbolic interactionist* sociology which developed out of this academic community and their body of work is at the heart of social worlds theory.

The focus of the symbolic interactionist school of social theory is on humans as interpretive beings who assign meaning to the actions of others and themselves (Blumer 1954, 1962). This situates the sociological level of analysis at the micro-level of interaction and interpretation, building these up into larger structures with wider social ramifications. Rather than studying social, cultural, structural, or biological 'forces' that act on individuals and groups, this studies the self-making and meaning-making behaviour of human beings themselves (Blumer, 1986; Plummer, 2000). These wider social contexts and structural features are treated as the conditions within which this meaning-making and action occurs rather than determining individual action in their own right. The work of George Herbert Mead (see for example Mead, 1934), and later Herbert Blumer (for example, Blumer, 1954, 1962, 1986), is foundational for this school of social theory. Stemming from 'social psychology', this focuses on the interiority of human beings, and the ways in which they not only interact with others, but also interact with themselves, attempting to make sense of the things which they do and build up a set of understandings of their own internal lives (Plummer, 2000; Albas et al., 2003). Mead posits that this is at the core of how humans engage in social life, experiencing the world through processes of 'self-indication' as events are interpreted, assigned meaning, and acted upon (Mead 1934; Blumer, 1962).

This is effectively a theory of subjectivity; the world with which people interact is experienced through these frames of interpretation, rather than a direct experience of any objective properties of the objects in the world themselves. This is the 'symbolic' dimension of symbolic interaction, that humans engage in the world not

through solely through reactions to the material, but through a dense symbolic realm of meaning-making (Plummer, 2000; Mead, 1934; Blumer, 1962). The world as interpreted is therefore built up of an aggregation of these symbolic interpretations, which form the basis for and give meaning to individual action. As a result, social life is not fixed, rather it is constantly emerging and evolving, always being actively created and constructed by the people who make up societies (Albas et al., 2003).

Where this picture extends to groups, these interpretive frames which are built up individually are able to align with one another through group interaction (Mead, 1934; Becker and McCall, 2009). People share and learn the meaning-making frameworks of one another through these processes of interaction and interpretation, and within groups these align over time into a shared set of meanings and concerns. In fact, while the conception of the self is foundational to symbolic interaction, this body of scholarship does not consider individuals in isolation. Instead, what is studied is *interactions* and collective behaviours, and how these interactions and interpretations shape themselves and one another to produce collective action (Becker, 1986).

Although many of the foundational studies which are often taken to be representative of social interactionist research focus on extreme micro-perspectives, such as the minutiae of gesture, expression, and speech in interpersonal interactions, the classic critique of interactionism as myopic and unconnected to broader relations of power is overstated (Plummer, 2000; Dennis and Martin, 2005). For example, Becker's work on labelling theory connects this up to the much wider social processes of crime and deviance, which explores the role of others' interpretations of us, in particular where these are stigmatising, in reinforcing group membership and the process of meaning-making, creating "outsiders" (Becker, 1963, 2018). This explicitly tackles how patterns of interaction and meaning-making at the level of interpersonal interaction become perpetuated, building up through self-reinforcing loops (for example, where labelling of a group as deviant shapes that group's behaviours and understandings, producing a situation which reinforces the

initial deviant label in the minds of the labellers) to have effects at much higher social levels. This scholarship tends to reject the 'micro-macro' distinction entirely for an exploration of the particular processes at work in a given situation, none of which are *ex ante* given primacy over another (Haynor, 1989; Fine, 1993; Plummer, 2000; Dennis and Martin, 2005).

This concern with connecting up interactions and interpretations to broader social structures can also be found in Erving Goffman's work, which takes these concerns with self-presentation and the production of social meaning and situates them within institutions, occupations, and power relationships between and within groups (Williams, 1986; Goffman, 1961, 1963, 1967, 1974, 1978, 1983, 1986). Although Goffman did not strictly identify his work within the interactionist tradition (Blumer, 1986; Williams, 1986), his approach to empirical study and social theory resonates strongly with the interactionist concerns with interpretation, meaning-making, and communication, and is often considered as a core part of the interactionist canon. Goffman's scholarship is chiefly concerned with the management and production of human social life, particularly the role of face-to-face interactions and how they allow people to inhabit particular roles in social settings (Goffman, 1963, 1967, 1978). This frames interactions and social situations as performances and rituals in which individuals take on particular roles, engaging in active management of the ways in which they and their actions are perceived.

Goffman's research frames this through the interaction order: the conditions, rituals, staging and performances which constitute social life (Goffman, 1983). This engages not only with the performances themselves, but the conditions and structures which make them possible, the 'frontstage' and 'backstage' areas of social life, the preparations and framing devices required, and the ways in which 'audiences' for these ritual performances are defined (Goffman, 1961, 1967, 1978, 1983; Pinch, 2010). It is through the commonly-established rituals of interaction which characterise particular societies and groups that broader social relations, values, and social stratification are reproduced (and it is also through these which they might be

changed). For example, in an interaction between a doctor and a patient, both 'perform' their assigned roles, thus reproducing the power dynamic between them (Goffman, 1961).

This depicts society as composed of a plethora of overlapping and interacting *social worlds*, the higher level structures of discourse and meaning which form around professions, subcultures, organisations, and other groups and focal points of social action. Strauss packaged this up into a broader theory of social worlds, conceptualising these as "shared perspectives that form the basis for collective action" (Clarke and Star, 2008; Strauss, 1978). Becker was another early contributor to this body of scholarship which takes the social world as a primary unit of analysis (above the micro-studies of affect and gesture), most notably in *Art Worlds*, which maps the different perspectives, forms of labour, necessary conditions, and frames of meaning making which feed into the production of a work of art (Becker, 2008).

As these interactionist perspectives began to gain more traction within Science and Technology Studies in the 1980s, they provided a powerful alternative approach to the tracings of Actor-Network Theory (which I describe briefly in Chapter 2) (Clarke, 1997; Latour, 2005). Turning this concern with interpretation, communication, and meaning to the business of science and engineering has allowed a range of studies and theoretical conceptualisations which engage directly with the material world and how people attempt to attach meaning to it in different ways and through distinct practices. Although this theory draws from Strauss' foundational work, the particular instantiation of the social worlds approach which I deploy in this thesis is that developed by Star, Bowker and Clarke within Science and Technology Studies (Bowker and Star, 2000; Clarke and Star, 2008). Within STS, this has been an extremely productive framework, providing an approach for separating out the heterogeneous terrain of intersecting perspectives, practices, and discourses which scientific, technical, and engineering work enrols due to the wide range of different kinds of work and actors on which it depends (Star and Griesemer, 1989).

## The social worlds approach

Scientific research and engineering work are often characterised as processes through which groups arrive at consensus about the material 'truth' of a shared subject of enquiry (Star and Griesemer, 1989). However, as Star and Griesemer argue in their foundational (1989) study of Berkeley's Museum of Vertebrate Zoology, the stories of scientific endeavours are in fact often characterised by the maintenance of substantial dissent and diversity of understanding between groups which nevertheless manage to "co-operate without consensus". Clarke and Star (2008) lay out a framework for exploring these dissonant perspectives within Science and Technology Studies through the concept of social worlds: "universes of discourse" (Mead, 1938; Strauss, 1978; Clarke and Star 2008) which accrete around a common focus, splitting, converging, interacting, and conflicting over time. This frames particular infrastructures, technologies, artefacts or knowledge-making projects as *arenas* around which multiple ways of understanding can gather and "interweave" (Clarke and Star, 2008 p113).

The precise 'discourse' at issue in Social Worlds theory draws from a Meadsian understanding of discourse as bound up in "collective, material action" (Mead, 1934, 1964; Clarke and Star, 2010, p116), rather than focused around the conventional groups which often form the units of organisation and analysis for other social scientific approaches to the study of discourse. As a result, social worlds research does not pre-define such groups as elements of analysis, instead mapping the messy, overlapping ways in which worlds of discourse draw their boundaries across arenas, often ignoring the neatly-defined social groups which may be most obviously apparent, such as "organisations, institutions, and even social movements" (Clarke and Star, 2010, p116). The symbolic interactionist concern with the role of the micro-level processes of interpretation and interaction, and how they aggregate into higher-level structures, is at the core of this approach. Although some social worlds scholarship focuses on individuals (Shibutani, 1955), the majority, and the scholarship on which I draw in this thesis, does not, instead focusing on the social

worlds themselves as subjects of enquiry. For this research, this means that a single characterisation of Tor's 'values', or of Tor as a site of social action, is not sought from the outset, rather what is attempted is a mapping of the complexity of discourse and action, of meaning and materiality, which actually characterises the organisation.

Methodologically, this leads to an approach heavily drawn from grounded theory, an inductive approach to fieldwork and analysis. This generally generates data through deep qualitative empirical research, including interviews and ethnographic study, which are then coded inductively, building up a set of very low-level codes which are then grouped into higher levels of meaning. This involves a "tack[ing] back and forth" (Clarke, 2005, p59) between this painstaking building-up of semantic structures and higher-level interrogation of meaning, which converges on a framework for making sense of the empirical data. This is as distinct from a more *deductive* approach, which begins with a coding framework, usually drawn from pre-existing theory, and fits the data into it, drawing analytical purchase from investigating the structures the data takes within these predefined categories (Bonnell,1980). Clarke has developed this further into *situational analysis,* which I discuss in more detail in Chapter 5, along with a more thorough accounting of my methodological approach (Clarke, 2003).

In order to guide the process of inductive analysis, social worlds research uses sensitizing concepts (Blumer 1954; Clarke 1997; Clarke and Star, 2008) which indicate potentially interesting avenues of investigation, commonly-found features, and sensibilities with which to approach data generation and analysis. Rather than a programmatic toolkit, in which all elements must be present, these can be taken up and used as best suits the research and put back down or ignored when they cease to be relevant. As a knowledge-making process in itself, social worlds theory is hence formulated as a community of academic research practice which shares these methods and ideas: as a conceptual reservoir on which to draw rather than a

prescriptive set of frameworks which need to follow a standard form in every case (Clarke and Star, 2008).

## Sensitising concepts

I now turn to describe in detail the sensitising concepts which I have found particularly helpful in shaping this research. The first of these is the concept of 'social worlds' itself. Social worlds are "universes of discourse" (Strauss, 1978, p121) which intersect around a shared focus (which Strauss terms an *arena*), populated by individuals and groups whose working practices engage them in different ways with this central site of concern, and who develop distinct ways of making sense of the activities in which they are engaged and the focus and purpose of their work. These package up practices, discourses, ways of understanding, and sensibilities into a coherent form which constitutes a distinct perspective on a mutual topic of concern (Strauss, 1978; Star and Griesemer, 1989; Clarke and Star, 2008). For example, an operating theatre may be the site at which many different social worlds intersect, with the worlds of the surgeon, the neonatologist, and the obstetrician (and by extension, the nurse, the cleaning staff, the researcher, the architect, the computer programmer, and the anaesthetist) all contributing to the production of a situation in which surgery can occur in different ways (Casper, 1998). Each of these have their own understandings of the situation, their own place in it, and their own contribution to make.

Social worlds tend to be associated strongly with a primary activity or set of practices and a distinctive ideological position on the work in which they are engaged (Clarke 1997). This allows the technologies, infrastructures, or endeavours at the focus of an *arena* of discourse to represent a multiplicity of meanings, as multiple social worlds cluster around them. These social worlds are linked to the material elements of these technologies, infrastructures, and artefacts through *points of passage*, particular sites through which they can shape and influence the material, and hence

stabilise their own perspectives and steer the collective action towards their own goals and visions (Latour, 2005; Clarke and Star, 2008). Taking the example of the operating theatre, a computer programmer may influence the way in which the digital systems of the theatre are designed, the nurse may, through established practices and policies, shape important elements of patient pre-care and preparation, and so on. In this way, they materialise elements of their social world's discourses and frameworks of meaning in the situation, which represents a multiplicity of overlapping worlds which shape the material in different ways.

Crucially, this does not lock the social worlds of discourse which form rigidly to distinct groups of actors, rather it allows individuals to inhabit multiple worlds of discourse (Unruh 1979). Although particular social worlds may stem from and be tied to particular practices or groups, they have a life of their own above this and can overlap, conflict, influence one another, and be drawn on by a range of different (and often surprising) groups and individuals. Worlds may change over time, incorporating one another, subdividing internally, or changing entirely (Clarke and Star, 2008). The participation of individuals themselves in these worlds is fluid, and groups and individuals are able to draw on dissonant or conflicting ways of understanding their arena in different situations, becoming themselves sites where social worlds come together and interact. A substantial amount of boundary work is therefore involved in maintaining and negotiating the distinctions between social worlds (Star, 2010). In addition to these core participants are *implicated actors*, which are those which those directly involved conjure or draw on in doing work, but whose own voices are not present in these discussions (either because they are present but silenced, or because they are simply not involved directly). For example, in design processes with little user consultation, the users of a technology might be considered implicated actors, speculated about and used to argue for particular solutions or designs, but not active participants in the arena in their own right (Clarke and Star, 2008). These also extend to nonhumans which are gestured at in discussions and discourse but whose actual material forms are not closely interrogated through empirical inspection or brought in actively.

The boundaries between worlds are particularly productive subjects of enquiry (Star and Neumann, 1988). Actor-Network Theory frames this boundary work between different groups through *interessement*, a process through which one group becomes enlisted in the aims of another and the concerns of that group are translated into the language of the dominant group through *points of* passage and reframed to suit their goals (Star and Griesemer, 1989; Latour, 2005). In social worlds scholarship, however, translation work is not unidirectional and agonistic, rather it occurs simultaneously between multiple interacting social worlds. As such, the formations of the different actors retain their essential character despite this translation, and the work of the researcher becomes mapping the ecologies of these different perspectives and the ways in which they interact and engage in this mutual work of translation, without assuming that any of the worlds have a better claim to truth than the others (Star and Griesemer, 1989).

Social Worlds theory explores this translation work through the concept of *boundary objects* (Star and Neumann, 1988; Star, 2010; Star and Griesemer, 1989). These are concepts, artefacts, or technologies which tie social worlds together, allowing "cooperation without consensus" (Star 1989; Barret 2010; Star, 2010). These constitute "practices, structure, and language [which] emerge for doing things together" (Star 2010 p602; Becker, 1986). Where the perspectives of contrasting worlds need to work together, it is boundary objects which permit the necessary translation work to occur. They do this by having some fixed elements which are shared between worlds, allowing a common language for collaborative working and translation. In addition to these fixed elements, they have some elements which are left more amorphous and are permitted to differ in different worlds, allowing them to take different, or even totally conflicting shapes in order to facilitate specific kinds of work. (Star, 2010). These properties allow them to "inhabit several intersecting social worlds… and satisfy the informational requirements of each of them" (Star and Griesemer, 1989), and be used in those settings where worlds overlap while being repurposeable as more specific formations within the worlds themselves (Star 1988; 2010). Where these become established together within infrastructures, they can

extend to greater levels of scale, becoming classification systems which allow multiple large groups to carry out different kinds of work (Bowker and Star, 1999). Boundary objects can be physical artefacts or infrastructures that constitute sets of work arrangements such as a library, which is characterised by a classification and organisation system which supports multiple different kinds of work (Star, 2010), or more conceptual constructions; ideas which permit groups to cultivate shared elements of understanding that bind them together despite their differences.

Susan Leigh Star's development of the social worlds framework is the guiding light for this thesis, which takes inspiration from Star's studies of information systems and their designers (see for example, Star and Ruhleder, 1996; Star 1999). Infrastructures are core parts of social worlds, and are embedded with their key values, logics and constructions – they are "*frozen discourses that form avenues between social worlds* and into arenas and larger structures" (Clarke 2008). Star and Ruhleder (1996) lay out a theorisation of infrastructure which has a number of key characteristics. Infrastructure becomes *visible on breakdown*, and relies on a substantial degree of 'invisible work' in order to function in a way which is *transparent* to its users: the "sinking into the background" (Star and Ruhleder, 1996) which is often ascribed to infrastructure is only ever partial and contingent on maintenance work and material conditions (Star and Ruhleder, 1996; Star 2010). This maintenance work is also a productive subject of sociological enquiry (Star, 1999; Graham and Thrift, 2007). It is *built on an installed base,* constructed atop and relying on existing infrastructures and shaped by the assumptions and historical legacies which they embody. It also allows further systems to be built on top of it and alongside it, becoming part of a system of *standardisation* which can fit into other systems, infrastructures, and technologies. This also creates a level of inertia, as the size of such systems mean that top-down change is extremely difficult, and so transformations are local, partial, and slow. It is linked to *conventions of practice* which both structure its material forms and need to be learned by new people who want to engage with it. Finally, it supports a wide range of different use cases, and is permeable to multiple different meanings (Star and Ruhleder 1996; Star 2010). This conceptualisation of

infrastructure is particularly conceived within the context of the rise of large-scale, distributed and decentralised infrastructures and the problems they pose for attempts at standardisation, arguing that "one person's standard is in fact another's chaos. There are no genuine universals in the design of large-scale information technology" (Star and Ruhdeler, 1996).

In using a social worlds approach to study Tor, I treat it both as an infrastructure, but also as the focus of a range of different people, kinds of work, perspectives, and attempts at sense-making. This allows us to explore the plethora of hidden work which underpins the conditions which make Tor possible, allowing it to be more than a proof-of-concept, rather, a successful, widely-used infrastructure. In Musiani's terms, this constitutes a study of Tor which is "not afraid of its subject" (Musiani, 2012, p5) happy to dive into the worlds of technical development and administrative practices where necessary to understand Tor's values and its place in the world. A social worlds approach achieves this through interviews, archival work, and ethnographic study, allowing the Tor community itself (as experts in their own worlds) to give voice to their own diverse understandings of the important controversies at play, and the connections between values, practices and technical forms (Clarke and Star, 2008). In combination with studies of the practices and forms of work in which they actually engage, and the sensitising concepts I have described herein, this forms the "theory-methods package" (Clarke and Star, 2008) which I use to investigate the social life of Tor, giving due weight to the material without getting lost in the minutiae of technical detail.

# Making the link from meaning to the material

## Embedding values in technology

In studying these group attempts at the production of knowledge and the development of technologies; the question of materiality is an important one.

Moving from a framework for separating out the complex landscape of types of work, practices, perspectives, and discourses which surround Tor, in this section I discuss the frameworks which Science and Technology Studies offers to make sense of how these values and perspectives are actually materialised in practice: how they become crystallised as infrastructure (Star, 1999), embedded in the material, or 'inscribed' in technologies (Latour, 2005). I then discuss how these technologies and infrastructures might go on to reproduce these values and categories in society.

For my study of Tor, the most obvious 'material' features to study were the software and hardware of Tor itself: the code and protocols which create privacy for its users, and the infrastructure of relays which allows this to work at scale. These involve very different kinds of work, however the most 'high-profile' and visible of these is undoubtedly the development work through which Tor's initial developers created an initial design for Tor. Although there were many other important processes through which Tor grew into its current form, this early design work is undoubtedly an important point at which the kind of privacy which Tor envisions and creates in the world was fixed. In this thesis, I describe this through a set of processes and mechanisms which include 'design', 'development' and 'implementation'. Where I refer to 'design', I mean the processes by which the structure and function of the infrastructure are reasoned about and formalised, largely at the beginning, when the initial work of technological creation and engineering is ongoing, but also at other points when it is revisited. 'Development' constitutes the entire process of creation, including design, but also testing, implementation, consultation and other subprocesses which continue throughout the whole lifetime of the infrastructure. 'Implementation' refers to the ways in which the formal design of the infrastructure is materialised, and the modifications, revisions and compromises which this entails (Williams, Stewart, and Slack, 2005). In practice, development is multifaceted and iterative, with designs and implementations being refined, tested and reconceptualised in different ways throughout the process (Guedanna and Ayadi, 2013). I do not use a linear conception of the development process in this paper,

rather I am interested in the negotiations between different kinds of work which take place across the course of an infrastructure's creation and beyond.

Science and Technology Studies approaches to understanding how values become embedded in technologies often draw on the concept of 'inscription' from Actor-Network Theory: the "translation of one's interest into material form" (Callon, 1991, p143). The designers of an artefact, or those involved in its creation, have a particular view of the people who will use it and the kinds of action which they intend it to permit, which both reflects their own values, social structures, and understandings of the world, and is stabilised in the material forms of the technology (Akrich, 1992; Latour, 2005). Where a broader range of humans and non-humans actors (or 'actants', in ANT) are involved in the creation of a technological artefact, each of them struggles to enrol the others into their vision of the project and install themselves at key control points in the network: points of passage (Latour, 2005). Where multiple visions conflict, particular groups can assert themselves through a process of *interessement* which involves particular actors attempting to recruit those with different visions, reframing their concerns in terms of their own and hence establishing their position as gatekeepers at points of passage and exerting their control over the project (Monteiro and Hanseth, 1996). The properties of the resulting technology are the result of this struggle, and ANT frames this as a process of 'funnelling', through which the concerns of a wide range of actors are shaped down and translated through the perspective of a key gatekeeper (Latour 2005; Star and Griesemer, 1989). This has been extensively used to study the creation of technical artefacts, uncovering hidden actors and agencies at play in social life (Venturini, 2010, Van der Wagen, 2015).

Where social worlds theory conceptualises how value systems shape the material properties of infrastructure, it does so through a more multifarious conception of translation work. Rather than an agonistic perspective, where a dominant group of actors (or 'actants') enrols others in its vision, in the social worlds framework, multiple intersecting social worlds all attempt to engage in this translation work and

establish their vision of the project, engaging at a multitude of different passage points (Clarke and Star, 2008). Therefore, rather than an Actor-Network approach, which funnels perspectives down through gatekeepers, social worlds theory takes a broader approach, framing at the level of the organisation and mapping how multiple worlds shape and collaborate with one another across a range of passage points (Star and Griesemer, 1989).

While this is a useful conceptual framework for mapping which elements of the material form of an infrastructure are shaped by which actors, I am also interested in the 'backwards' flow from the material to the discursive: how the material constraints, design processes and technologies shape the social worlds of Tor as they themselves are shaped by them. For this, I draw on the idea of convergence, a process by which infrastructures and the human actors who come into contact with them 'converge' as their social worlds mutually shape one another (Star, Bowker, and Newman, 1998). Star argues that one of infrastructure's core features is transparency, the quality which infrastructure possesses for certain users at certain times, where it becomes to a greater or lesser extent visible to the user, its material resistance to user action fading into the background to permit more seamless mediation of intent (Star and Ruhdeler, 1996; Star, Bowker, and Newman 1998; Star, 1999). This transparency is the result of a convergence between the social world of a particular actor and the category systems embedded in the infrastructure itself (Star, 1990, 1999). Star uses this specifically to study *information artefacts*, or technologies and infrastructures which codify particular category systems for the purpose of knowledge work and information sharing. These form a key undergirding for social worlds, stabilising and formalising their knowledge forms and category systems, and hence facilitating knowledge work (Star, Bowker and Newman, 1998).

Tor is a different kind of infrastructure, however I have found this useful for understanding the processes at play within the design work of the Tor developers. Although Tor is used to share information, it does not primarily act as a system of categorisation for that information but as a more general-purpose conduit for

communication, the contents of which it leaves largely untouched. It does, however, embed a set of category systems within it, in particular, a taxonomy of the users of Tor and the people who are trying to attack it. I use convergence in this thesis, therefore, as a way of understanding the development process itself. Using archival records of the development process, I track the steady, iterative emergence of the social world of Tor's developers alongside the materialised category systems embedded in its infrastructure, framing these as 'converging' together as they tack back and forth between different kinds of work.

Existing conceptualisations of convergence often focus on systems already-in-place and already-existing social worlds; how the rationalities of different groups interact with those embedded in technical systems, including library systems (Star, 2003) and information systems for biological research (Star and Ruhdeler, 1996). In contrast, in this thesis I develop this approach to explore how these processes work when an infrastructure is created for the first time. When the developers of Tor first began to design it, the foundational social worlds of Tor were not yet fully-formed – they needed to pull this together from a variety of pre-existing and newly developed ideas and understandings. My approach frames the values of the developers through the category systems they use to understand privacy, and maps how they refine these categories through the design process, finally stabilising this social world in Tor's infrastructure as a set of materialised values. This is particularly useful for a study of Tor, as it also allows us to focus not only on design, but also on the more hidden forms of work, such as maintenance and administration, on which Tor relies. This extends the idea of what makes Tor 'work' beyond the mere completion of a functioning prototype, to consider the conditions and types of work which allow Tor to be robust, resilient, successful, widely-used, and usable; in short, to make its vision of privacy a reality in the world.

## How technology shapes the world

Finally, I turn to the consequences of these materialised discourses, setting out frameworks for exploring how technologies and infrastructures such as Tor might shape the world and realise the visions of privacy which characterise its social worlds and become embedded in its material forms. To do this, I use the concept of 'performativity', a core concept in STS research and theorisation (see for example, Orlikowski, 2005; Callon, 2009; Mackenzie, 2005, 2006; Law and Singleton, 2000; Licoppe, 2010; Musiani, 2015). The extensive and vital scholarship of Judith Butler (for example, Butler, 2002, 2006, 2011, 2013) argues that the social categories which make up human societies are not static, positivist, or inevitable, but need to be continuously and actively produced, or *performed*. These performances – of gender, race, social class, sexuality – are not a given, sometimes succeeding, sometimes failing, often only partially realised. While Butler focuses on the discursive domain of performance, in Science and Technology Studies, the idea of 'performativity' has been used in a wide body of scholarship which bridges the material and semantic to map, or trace, the material and discursive conditions and elements which produce, or allow the production of, particular social categories and realities (Callon, 2009; Licoppe, 2010). This framework therefore constitutes a theory of technosocial action, through which technologies can be considered as 'performing' the values and assumptions of their designers, shaping and producing social life in a variety of ways. In performing the motivations and worldviews of their designers, they can grant or stabilise access to power, capacities and resources for different people and groups (Harre, 2002), and can act as a direct representation or stand-in for particular discourses: a symbol, or set of symbols in themselves, or a frame within which symbols can be communicated. Thus, the "embedded discourses" which we discussed in the previous sub-section themselves go on to be reproduced in social life by the infrastructures and technologies in which they are embedded (Akrich, 1992).

Performances are ways of making up reality in a certain way, and this is equally the case for the "material performances" (Law and Singleton, 2000) of technologies and infrastructures. The discourses which form across the creation of an artefact and become embedded in its material form package up a range of different ideas and scripts, performing the relationships between the actors involved in their creation and their understandings of the world. (Akrich, 1992, Musiani, 2012, 2015). Performativity has been used as a conceptual framework for understanding how the Internet and its technologies become sites where particular views of the world and ideas are realised. For example, De Nardis's research studies the "embedded politics of technical architecture" and the ways in which control points designed into the Internet infrastructure act as important sites of power (Musiani, 2015; DeNardis, 2009, 2014). While there is a small but growing body of studies of the category systems at play in Internet technologies, the politics and values of their designers, and their consequences, particularly for social media platforms (Howard and Parks, 2012; Youmans and York, 2012), I engage in this study at a lower level, as Tor sits not at the 'platform' level, but just above the material infrastructures and protocols of the Internet itself.

The work of Goffman forms a useful bridging-point between the interactionist approach of social worlds theory and these concerns with 'performativity' and the ways in which technology shapes society (which are more usually tackled within STS through Actor-Network-aligned frameworks) (Goffman, 1983; Clarke, 2005). Pinch (2010), in a paper which provides an extremely useful guide for these elements of this thesis, argues that the "hidden technologies" within Goffmann's sociology play an important role in structuring the interaction order, forming the material setting which distinguishes 'audience' from 'actor', 'frontstage' from 'backstage' and the more subtle conditions in which social performances and ritual interaction takes place. These both set the conditions in which performances are able to occur and constitute performances (or parts of performances) in their own right. He further extends this to argue that understanding social action, especially in contemporary societies where a vast array of Internet services, platforms and technologies are

involved in its mediation, requires a deeper engagement with interactionist approaches to technologies and infrastructures, and deep empirical work studying the designers of platforms and infrastructures on which the Internet relies (Pinch 2010).

This framing allows us to make the final connection to social worlds. Rather than assuming the primacy of the designers, a social worlds approach aims to square the contributions of all the different worlds involved in the creation of infrastructure, and the maintenance and administration which provides the conditions for it to perform these visions of the world. This extends these worlds into the performance itself, to explore what happens when Tor meets the world and begins to perform these values and shape the interaction order of its users, to make sense of the problems which arise, how these performances are frustrated and subverted, and how Tor's different worlds attempt to navigate this. This presents an active form of technological performance, supported and shaped by a range of human and technical elements – not only the creative embedding of the values of the designers, but the other forms of hidden work, such as maintenance, public relations, administration, or resilience practices, which nevertheless play an important role in shaping and supporting Tor's performance of its particular vision of privacy.

Star's research on information systems and other kinds of infrastructures connects social worlds and the category systems which they embed in material forms explicitly to power and marginality (Star, 1990). The people who use and interact with infrastructures once they are deployed are often considered by developers only in the abstract at the design stage, and the ways in which they attempt to bring them into ongoing development or categorise them through research are themselves systems of classification, and hence, power (Foucault, 1991, 2007; Star, 1990). This means that the category systems through which the developers imagine user groups are important sites where social reality is produced, and an important form of power wielded by the developers to realise their vision of the world. Those who don't fit perfectly can find themselves shaping their own lives and selves to better conform,

and those who don't fit at all can find themselves cast out entirely and created as outsiders (Star, 1990, 1999).

The view of Tor which I set out in this thesis is not a total one. In deciding to focus on the Tor community itself, rather than the myriad different groups who use Tor, I develop only a partial perspective, which is unable to say much about how these visions of the world are performed in reality when they come into contact with users. What I can do, however, is talk about the different kinds of work and conditions which go into making these performances possible and successful; the things which help Tor to realise its vision of privacy in practice. I am also able to explore the problems with crime, power, administration, the criminal justice system, and active attempts to undermine Tor which these performances face in practice and how they are negotiated. In doing so, I set out an in-depth sociological study of Tor which breaks down its attempt to 'steal the fire' and wield infrastructural power into its component parts, mapping in detail the different people, stagings, and kinds of work (both frontstage and behind-the-scenes) which are involved; the successes, failures, and problems which it encounters; and the new forms of work, ideas, and ways of making-sense which arise as a result.

## Conclusion

This research constitutes a social worlds study of the Tor Project which aims to open up the black box of Tor and explore how it fits into these wider domains of power and ideas of privacy and the Internet. Although the empirical work in which I engage is concerned with the detailed practices and understandings of the people in the Tor community, this work does aim to connect back up to bigger questions of power. Conceptualising Tor as an attempt to 'steal the fire' on this broader stage, I use a social worlds approach to break this apart into its constitutive components. I am concerned with what these attempts at social action through technology actually depend upon in practice: what kinds of work (both hidden and overt), conditions,

ideas, values and visions are implicated, the problems which arise and how Tor navigates them.

Through a social worlds approach, this can be conceived as a process of mapping the *social worlds* of Tor, the practices and perspectives associated with them, and the *boundary objects* through which they negotiate conflict and collaboration. This engages with the different ways in which the worlds of the Tor community imbue Tor with meaning and the kinds of work with through which they encounter, support, and *produce* Tor as a collective endeavour. I then explore the materialisation of these worlds in the infrastructure of Tor itself through processes of *convergence*, not assuming that this is unidirectional, but allowing the material properties and constraints of Tor and the practices of design and development to recursively shape the values and understandings of Tor's designers even as this development work proceeds. I then use Star's frameworks for researching *infrastructure* and *hidden work* to explore the additional forms of work, maintenance, and resilience practices which are required beyond the simple picture of 'designing in values' in order to make the infrastructure *perform* these values in practice and at scale. I use Tor's social worlds as a way of understanding these different kinds of work, the rationalities which underpin them, and how they also constitute sites at which the 'values' of Tor's infrastructure are embedded and reinforced. Finally, I draw these different strands together into more explicitly criminological terrain. I use the framework of social worlds which I have characterised within Tor to explore the issues of illegal and harmful activities by its users and friction with governance and criminal justice regimes which Tor faces in practice, and how each of these social worlds make sense of and navigate them.

Taken in its entirety, this constitutes an in-depth sociological study of the Tor community and its attempts at social action, yielding insights into how wider concerns of power and values at play in Internet privacy are actually worked out in practice. In the following chapter, I set out how I went about exploring these questions through empirical research. I outline the methodological approach and

fieldwork through which I generated the data for this thesis, the ethical practices, considerations, and issues which I took into account in the planning stages and throughout the research, and my approach to analysis.

# chapter 5

# exploring the values of an infrastructure: methodology, ethics, fieldwork and analysis

## Introduction

My interest in the Tor Project as a site of study stems from my broader interest in the Internet, online privacy, and their links to politics and power. As I was in the final stages of my MSc in Criminology and Criminal Justice at the University of Edinburgh in 2013 and sounding out potential PhD topics, the Snowden leaks broke, revealing that liberal democratic nations were engaged in mass surveillance at home and abroad (Lyon, 2014, 2015; Wood and Wright, 2015). Already sensitised to issues of governmental power from my activist work, I developed a keen interest in what this might mean for conceptions of how societies are governed, how power is enacted, and the consequences for justice and liberation movements in contemporary societies. Over the next few years, throughout the process of applying for the PhD, carrying out fieldwork, and writing up my thesis, surveillance and data privacy have become only more contentious issues, with significant public controversies around surveillance by social media companies (Zuboff, 2015; Smith, Henne and von Voigt, 2012; Carlson, 2018), the use of surveillance-driven advertising for election interference (Allcott and Gentzkow, 2017; Guardian, 2019), and worrying shifts towards the management of public services and policing by algorithmic processing of mass-collected personal information (Ferguson, 2016; Casady 2011; Zwitter, 2014). I

share with the Tor Project a deep anxiety about the potential visions of the future which are implicit in these trends: of societies governed through unaccountable surveillance and control managed by private companies and spy agencies outside robust democratic institutions (Tor Project, 2019).

My intention in this research was to take frameworks and approaches from social worlds theory and bring them into criminological study of the Internet. However, rather than simply doing theoretical work, I was keen to do this alongside a programme of qualitative research through which I could explore the benefits and challenges of these approaches in practice. I initially intended to do a comparative study including multiple technologies and projects, however, in conversation with my supervisors, I decided that an in-depth qualitative study on a single infrastructure would develop a richer picture than a comparative study might. I aimed to choose a subject for this study which particularly showcased the links between values and technology, and, having previously had an interest in the work of the Tor Project, with whose mission I was sympathetic, this seemed to be an apposite choice. Tor occupies a deeply contested space at the meeting point between state control of the Internet and attempts at resistance. It also poses particular questions around the governance of online crime and the appropriate limits of state power, constituting a potentially productive case study for bringing social worlds theory into criminological study of the Internet.

In the first year of my PhD, I discussed at length with my supervisors which potential sites for collecting data about Tor might be available and how best to capture these sources. The openness of the Tor community meant that, unlike with for-profit infrastructure providers such as Google, Facebook, or ISPs, the Tor Project would not have commercial sensitivities preventing them from speaking to me (although they have other considerations which made this difficult, which I discuss below). This, along with the fact that Tor was beginning to engage more in public conversations about its values through blog posts and news interviews, meant that conducting interviews with members of the Tor community was potentially feasible, if requiring

careful handling. In addition to this, the public nature of much of the Tor Project's work meant that there were numerous potential sites for ethnographic observation, including IRC channel meetings, developer meetings, and conferences. Finally, the existence of Tor's expansive public archives of mailing lists, design documents, feature proposals, and code changes meant that even if all the other avenues fell through, there would still be sufficient material for a PhD thesis. My own technical background was important here: having worked with computers throughout my life, including as a statistical programmer, I was able to read and understand technical material, had a good understanding of how to talk fluently about technical issues with engineers, and was attuned to what might be interesting problems and controversies. This meant that I was able and willing to engage with the technical fundamentals of Tor to the extent needed to explore how they might be linked to questions of sociological interest.

The Tor Project presents both unique challenges and opportunities for sociological research. From the researcher's perspective, it exists in tension between two countervailing forces: its policy of radical openness means that its developers, code, discussions and public life are uniquely accessible, while its position as a resistance technology (which comes into conflict with law enforcement and state security services) means that many in its community are deeply reluctant to engage with researchers, and the human cost of mistakes is potentially very high (Gehl, 2018b). Even aside from the difficulties of negotiating access, Tor's openness, which it adopts both as an expression of its core values and as a protective mechanism (as I discuss at length in Chapter 8), presents the sociological researcher with difficult decisions as to how much of this archival material and open discussion spaces such as chat channels are really 'fair game' (Gehl 2018a; Gehl, 2018b; Kozinetz 2010). Researching technological projects is a challenge in its own right and pulling this wealth of technical detail into something sociologically meaningful, ethically defensible, and engaging to read has its own difficulties (Star, 1999).

At the core of my research was a desire to study Tor as a site of social action: as an attempt to 'do politics' through infrastructure (Musiani, 2015). I wanted to break this infrastructural politics down into its component parts, studying in depth the values which shaped each part, the ways in which the material design of Tor was created, the additional forms of hidden work and other conditions which allowed it to succeed, and the problems which its 'performance' of its vision of the world faces in practice. In doing this, I undertook both semi-structured qualitative interviews and archival research. Given the explicitly political nature of their work, I had expected the Tor community to have a set of strong, shared values and understandings of Tor. In fact, the earliest finding of my research was that its community was characterised by a diverse range of conflicting motivations and perspectives. The social worlds framework proved to be an ideal approach for distilling this into three main social worlds which could then be used to answer other questions about Tor and make sense of some of the contradictions which characterise it as a site of social action (Clarke and Star, 2008).

In this chapter I focus on the practicalities of the fieldwork and analysis, describing how this theoretical framework fits into these more practical concerns and why I made the methodological decisions I did. I begin this chapter by discussing the design strategies and research questions of the study, drawing out the links between my theoretical framework and my fieldwork approach. I then discuss how I developed my approach to interviews and the archival data sources of which I made use. Next, I describe my fieldwork journey, from initial approaches through to building trust, to the corpus of interview data I managed to generate. I then set out the ethical principles and considerations which structured the design of this research. In the next section, I then set out my analytical practices, from the initial coding and mapping to the organisation of my data into a set of findings. Finally, I reflect on some of the potential methodological limitations of my research.

# Research questions and strategies

## Research questions

As I describe in the previous chapter, the social worlds framework is based in symbolic interactionism, and the inductive, grounded methodological approaches which stem from this means that research questions evolve across the course of the research project. I began with a broad set of research questions and areas of interest and refined these as particular themes and findings arose from my fieldwork. The initial questions with which I began were as follows:

1. What are the main social structures, kinds of work, and technological infrastructures which make Tor function?
2. What motivates the people in the Tor community, and how do they understand what Tor is trying to do? What is their vision of privacy? Do they share a single coherent perspective and set of values, or is the community characterised by multiple different perspectives?
3. How do their views on crime, privacy and surveillance affect their work and shape the technology itself? How are decisions about Tor software development made and negotiated? How do contributors manage or mitigate the potential harms which could arise from use of their software, and how do they deal with friction from the criminal justice system and law enforcement?

As my interviews with the Tor community progressed, it became apparent that there was no single set of 'Tor values' or a single vision of privacy, rather the Tor community was a home for multiple distinct perspectives which appeared to be associated with particular kinds of work. This suggested that mapping these as social worlds might be a productive way to make sense of the Tor community. Equally, from my archival research, I found that the values and ways of understanding Tor which I was finding in the Tor community could be linked to specific design features and practices documented in the development mailing lists. Additionally, my

mappings of different kinds of work, through interviews and from my study of the mailing list archives, found that a huge amount of work was going on beyond the design and development of Tor's technologies in order to maintain Tor's resilience against attack and allow it to reliably realise its visions of privacy for its users in practice. This led me from an investigation of Tor as a technology in the abstract to an attempt to understand it as an infrastructure, supported by many different kinds of work. Finally, it was apparent that conceptions of crime, power, and harm were implicated in important (and often unexpected) ways in Tor's design and the various other kinds of work involved in the community, forming key parts of the emerging social worlds which I was beginning to find.

This led me to develop these initial questions into a series of four core research questions, each of which is the subject of one of my results chapters (Chapters 6 to 9).

1. What are the key social worlds of the Tor community, how do they relate to one another, and how do they come into conflict, conversation, and collaboration?
2. How do these social worlds shape the material form and design of Tor; how are these values realised as properties of the Tor network?
3. When this design is materialised as infrastructure, what other kinds of work are needed so that this infrastructure can create Tor's visions of privacy for its millions of users, especially given the considerable opposition it faces?
4. What problems with crime, power and harm arise when Tor begins to realise its visions? How do the social worlds of the Tor community make sense of these issues, and through what strategies do they navigate them?

Although this may appear to be a linear, causally-driven set of questions, in other words that there are a pre-existing set of values which become materialised in infrastructure, then go on to exist in the world in practice, then run into practical problems with crime and criminal justice, in fact this is merely a useful framework for setting them out as different domains of enquiry. One of the core findings of my

research was that for Tor (as is the case for other Open Source projects – see Guedenna, 2015) these do not follow a linear pathway; the processes of creating infrastructure are iterative, messy, and looping, with values changing over time, design needing to be revisited and changed (and in fact not being the only relevant technical practice), and problems with crime (for example) arising as a consideration at every stage of the project. This has been well-established in the research literature as a feature of these multifaceted infrastructural and computing projects (Guedenna 2015; Pollock and Williams 2008, 2010; Williams, Stewart and Slack, 2005). As such, the way in which these are presented in the thesis as four discrete domains in a linear order should not be taken to assume a causal direction. An exploration of the relationships between these (as befits my findings) can be found in Chapter 10, and in the maps in Appendix E and F.

## Qualitative research with technological projects

The social worlds approach is not solely a theoretical framework, but is a "theory-methods package" (Clarke and Star 2008) with strong methodological implications. Social worlds research draws on practices of mapping and coding, using deep qualitative enquiry methods, interviews with as wide a range of members of a community as possible, and archival research to map out material relations, practices, meanings, and discourses. As discussed in the previous chapter, social worlds theory involves a grounded theory approach to research design (Clarke, 2007). Grounded theory requires that analysis begins at the very beginning of data collection, continuing throughout the research and iteratively working up categories from micro-coded data, tacking between different levels of abstraction, and between data and theory (Clarke, 2007; Strauss and Corbin, 1994). As interesting questions arise from the initial mappings and throughout the research, these drive iterative development of approach strategies and interview formulation. The social worlds approach enables the researcher to avoid the problem of "collaps[ing]" (Brunton and Coleman, 2014, p94) arenas where multiple perspectives overlap over a single site of

collective action into a unitary perspective, instead attempting to reflect this multiplicity of meaning.

This entails study not only of people, but also of things. In studying the material world of technology itself, the practices with which people interact with it, and the values which are embedded in it, I drew methodological insight from social worlds scholarship, particularly the contributions of Susan Leigh Star, and her related infrastructure studies research which draws out the specific application of social worlds approaches to infrastructures (Star, 1999, 1989). Star describes this as "a call to study boring things" (Star, 1999, p 377). Trying to research infrastructure is not always easy: technical documents, code, and design discussions are very alienating (and often unintelligible) to the non-expert, and it is often hard to discern narrative structure or the human underpinnings and values which are expressed as code, protocols, and design jargon (Star, 1999). Despite this, it important not just to consider these technologies as backdrop for action, but as sites of social action themselves. Star (1999) argues that this should involve a combination of "historical and literary analysis… interviews and observations" (Star, 1999, p384), using interview investigation about practices of design and maintenance, particular controversies and design decisions as a mechanism for gaining purchase on these more technical data sources such as archives of code repositories. This approach has been put to productive use in studies of computer and information systems (Star; Star; ref, and outside explicitly Social Worlds studies, Brunton and Coleman, 2014).

Having discussed potential approaches with my supervisors, I began with an initial pilot study of three interviews. This was intended to scope out interesting potential avenues of investigation for the main project and to help my supervisors and me assess whether the Tor community were likely to be amenable enough to constitute a viable subject of research. Having used this to generate initial data and themes, I sought to approach in my main fieldwork as wide a range of people from within the Tor community as possible, not simply concentrating on the more famous or influential people within the Tor community as I was equally interested in the hidden

perspectives and more invisible work of Tor. In combination with this, I conducted substantial archival research in the Tor Project's online archives of design documents and mailing lists. Moving back and forth between these two main approaches, I was able to develop a 'deep' sociotechnical study of Tor, which I describe in depth in the remainder of this chapter.

## Instrument development and data sources

Before the fieldwork began, I identified a range of potential data sources, and began the processes of study design which would continue throughout the project. The choices I made in these early stages, much like those made by the Tor developers in their early design work, shaped the data and findings which I and my participants generated across the course of the research (Ritchie et al., 2013). In this section, I outline my main instruments of data collection and the decisions I made at the preparatory stages in designing my approach. First, I discuss my interview design, in particular, choices of questions, topics and ordering, and the different kinds of interview I conducted (through a range of different mediating platforms, and face to face) and the benefits and drawbacks of these different approaches. Finally, I set out the archival data made available by the Tor Project and how I approached its study.

### Interview design and practices

Working in consultation with my supervisors, I decided to carry out semi-structured interviews with members of the Tor community, split into four key thematic parts. Semi-structured interviews are a well-established form of qualitative enquiry, especially in grounded theory approaches, where research questions are non-prescriptive and exploratory (Holstein and Gubrium, 1995; Kvale, 2008; Kvale and Brinkman, 2009). This allows a more fruitful exploration of the values and understandings of the interviewee, and can often reveal new and unforeseen

avenues of investigation. I gave design of the interviews careful consideration, and drew from the initial findings of the pilot study in drawing up interview schedules and plans. Although I had a list of potential questions within each section, I was very happy to let the interviewee lead, and aimed to establish a more loosely-structured discussion rather than a prescriptive set of questions. Having a loose thematic structure was useful for providing a sense of progress to the interview and allowing the sections to flow into one another naturally, and having a bank of prepared potential questions was useful for where the interview faltered or began to meander into less relevant topics. As Ritchie (2013) advises in *Qualitative Interviewing*, question order is often important, and I explicitly structured these sections to facilitate rapport and openness, beginning with very general, reflective questions which would set the tone of the interview and ease the participant in. These broader questions about values, subjective interpretations and motivations set the tone for the rest of the interview, encouraging deeper and more reflective answers to the more practice-oriented discussions. This could then move onto more specific questions about practices and problems, before finishing again with a more reflective exploration of the politics of Tor and privacy technology.

The interviews were broken up into four sections. The first of these was a general discussion of motivations and values intended to ease respondents in and develop rapport. This began with a broad question about how they had become involved with the Tor project, which led to follow-up questions and further probing around interesting lines of enquiry. I then asked them questions about the dynamics in the Tor community, the values of Tor, and their personal motivations for their work.

The second section sought to dig into more technical detail about specific working practices. This moved from an initial broad question about the work they did for Tor to a request for the interviewee to walk me through a specific example in fine detail, outlining their rationales for the different choices they made along the way. This proceeded very differently for people with different roles in the Tor community – for relay operators, this could be about general practices of relay operation, while the

developers tended to outline what they thought were important design decisions and how they had made them in practice, or other forms of development work. Some of these were deeply specific explorations of particular features of Tor, while others were more 'day in the life' discussions of an average day contributing to the Tor Project.

The third section touched on more contentious issues, and as such was located later in the interview so that a degree of mutual trust might be established. This involved questions about criminal or harmful uses of Tor, and opinions of and experiences with law enforcement. These questions naturally raised suspicion that I was attempting to paint Tor in a negative light or frame it as associated with crime and harm (as I discuss in the ethics section and fieldwork section of this chapter), and as such I made sure that I had established a level of trust with the interviewee by this point before bringing it up.

The interviews concluded with more broad questions about privacy politics. Ending on a more expansive note, I invited the interviewees to speak more broadly about current trends in online privacy and the future of the Tor Project. This allowed the interview to end on a positive, reflective note and to clear the air after more technical or difficult questions (Ritchie et al., 2013.

Carrying out interviews with members of the Tor community posed some challenges, as the community is dispersed across much of the world. As a result, many of the interviews were carried out using ICT-mediated channels, such as Skype and Jitsi video calls, IRC chat, email interviews, and Signal voice calls, with the particular format decided by the interviewee to maximise their comfort with the setting, and enable them to have control over any privacy or security protections which they desired. A number of the interviews were carried out face-to-face, often at international conferences where many people from the Tor community were present. Carrying out interviews via these different media presented particular challenges and contributed to the individual character of each interview. Developing rapport, judging emotion and affect, and keeping a natural flow to conversation was

challenging over online video and voice chat. The text-based interviews took place over a longer time, but with more potential for short breaks, note writing and referring back to previous discussions and other media. This proved useful, especially in the case of interviews where the interviewee took the opportunity to paste links, email text and other media into the body of the conversation.

These conversations were, however, less natural than voice chats or face-to-face interviews, with more considered replies and some difficultly in ascertaining when the respondent had finished providing a response due to the lack of a typing indicator on some chat clients. The data provided from the text and email interviews was less rich in some ways than that collected through the voice and video calls or the face-to-face interviews, where interesting tangents could arise through natural conversation. As with the voice calls, the lack of visual feedback proved slightly awkward, however this effect largely disappeared as the conversation progressed and the respondents became more relaxed and began to build trust. Despite these potential barriers with voice-only interviews, they are well-established as suitable methods for qualitative research (Sturges, 2004; Stephens, 2007). The advantages and disadvantages of these different forms of interviewing are already well-documented in the qualitative research literature (Kozinets 2010; Morgan 2004).

Of all the considerations feeding into the interviews, one of the most important turned out to be an appreciation for the cultural mores of computer scientists (Laudel and Glaeser, 2007, Flammia, 1993). This was a set of sensibilities which I needed to cultivate across the course of the fieldwork. Of particular importance proved to be a dislike for ‘small talk’, and for being asked questions about technical matters of fact which could be found online. While I had initially been using these to get the interviewee talking and lead into more probing questions. I stopped using these entirely, as they inevitably either destroyed the rapport we had built up or triggered a long, technical answer which replicated available information. This is a well-covered phenomenon in qualitative research with experts, not limited to computer science, and maintaining the balance between ‘demonstrated

competence' versus 'playing dumb' is something which needs to be negotiated and learned throughout the research for each particular community (Littig, 2009; Teicher, 2015; Bogner, Littig, and Mentz, 2009). The respondents were sometimes reluctant to venture personal opinions in case they might be taken as representative of the Tor Project as a whole, and I soon included in my preamble a specific direction that I was interested in exactly these subjective ideas and the heterogeneous landscape of values in the Tor community, and that I would represent them as such rather than as a 'Tor party line'. Again, this is well-documented in interview-based research within organisations (Garsten and Nyqvist, 2013).

## Tor's archives

Archival research is a key part of many social worlds studies (see for example, Star and Griesemer, 1989; Star and Ruhleder, 1996; Bowker and Star, 2000), as it provides a physical record of design decisions, practices, and documentation of the composition of material artefacts. Where records exist of discussions about design, such as meeting minutes, mailing lists, or design documents, these can provide substantial insight into not only why particular decisions were made, but the broader practices, contextual factors, and discourses which shaped them (Guedenna 2015; Pollock and Williams 2008, 2010; Williams, Stewart and Slack, 2005). Approached with care, these can provide a record of the development of the interpretive frameworks, category systems, and master narratives which went into the creation of a particular technology, and hence the discursive constructions and interpretations of the world which the technology embodies (Star, 1999). Where controversies and arguments are documented, these too provide important evidence of the different perspectives which shaped a particular project and how they interacted (Pollock and Williams 2008). Tor follows a policy of 'radical openness', openly providing a wealth of sensitive information about itself freely online. This includes the source code of most of its technologies along with detailed design notes, online trackers and wikis which record the work of the team in real

time, the content of internal mailing lists, IRC channels, and team meeting notes, extensive financial information and considerably more (Gehl, 2018b).

The archives of data which Tor makes available online constitute an enormous and rich site of research for sociologists. Gehl (2018b) has previously identified these archives as an untapped resource for sociological study and has made productive use of them in his comparative study of various 'darknet' technical communities and their attempts to cultivate legitimacy (Gehl 2018a). The discussions and material circulated on the mailing lists were the main source of archival data which I used in this PhD. Tor has several mailing lists which it uses for communication and work. These lists constitute sets of email conversations, sorted into particular topics by 'threads', and involve substantial discussions about many of Tor's key design decisions. The first of these, and the most important for this research, is the *Tor-dev* mailing list. This mailing list has been in operation from 2002 to the present day and is an extremely full record of the design and development of the Tor browser, right back to its initial creation. Although it does not capture telephone calls, in-person meetings, and work done individually, this was the main medium through which collaborative development work on Tor was managed between its developers. I also made use of its predecessor, the *or-dev* mailing list, which was set up in the 1990s for work on the Onion Routing project, and the *Tor-talk* and *Tor-relays* mailing lists, which constitute a general discussion list and a list for relay operators to discuss practices respectively. These can be freely downloaded from the Tor Project website[9].

I coded up a set of Python programs to help me work through this, establish timelines, and do text search more efficiently than NVivo would allow. These scripts turned the mailing list into a dataset, separating out the administrative information, such as dates, names of senders and titles of threads, from the content of the emails.

[9] A full archive of Tor's public mailing lists can be accessed at: https://lists.torproject.org/cgi-bin/mailman/listinfo

This enabled me to browse and search emails more effectively, pull out particular threads and conversations with keywords of interest, and fit them into a timeline, helping me to establish when particular topics and decisions appeared and recurred. It also assisted with high-level coding of these emails, allowing me to tag up particular emails by topics of discussion. My analytical method for this material, which draws on a social worlds/situational analysis approach, is described later in this chapter. I did not use the logs of Tor's public IRC meetings as I felt that this would be intrusive, as after discussion with members of the Tor Project, it became clear that these were intended as spaces for community outreach, and might involve Tor users revealing personal information when asking for help, or the more paranoid being put off engaging in these spaces entirely. However, I did engage in study of some of the other working sites of the Tor Project – namely, their "issue tracker" site[10], which documented ongoing implementation and development work in progress, and their various wikis[11], blog posts[12], FAQs[13] and design documents[14]. These were more justifiable sources of data, as they are made available for the express purpose of public scrutiny of Tor's development.

## Fieldwork and data generation

### Early steps

In this section, I describe the progression of my fieldwork, recruitment, and data generation across the course of the project. This research began with a pilot study whose purpose was to assess the feasibility of the wider project, in particular, the

[10] https://trac.torproject.org/projects/tor/query

[11] https://trac.torproject.org/projects/tor

[12] https://blog.torproject.org

[13] https://2019.www.torproject.org/docs/faq.html.en

[14] https://2019.www.torproject.org/docs/documentation.html.en

likely access which I would be able to negotiate with members of the Tor community. Pilot studies are a well-established approach to beginning sociological fieldwork (van Teijlingen and Hundley, 2002; Sampson, 2004), allowing for the cultivation of gatekeeper relationships, refinement of research questions, and identification of key areas of interest for the main project (Kim, 2011). I made an application to the University of Edinburgh Law School's ethics committee for this pilot study, which was approved. When I began this research, I drew largely from public information about the Tor Project, such as blogs, media statements and other writing, in developing my initial research questions and interview schedules. For example, the Tor website[15] contains substantial information about Tor's history and values, and the Onion Routing website contains a detailed history of Tor's precursor projects[16]. This generated a series of initial themes to inform my pilot study and an initial sketch of the different actors, groups, kinds of work, and technologies involved in Tor. I identified the relay operators, the volunteers who run the servers which make up Tor's network infrastructure, as a potentially useful starting point for a pilot study, as they constituted fairly hidden voices in the Tor community and hence might be more interested in having their perspectives heard. Equally, I judged that the relay operators might be more amenable to my scoping out of initial themes, and beginning with them would allow me to approach the core Tor Project staff with more developed ideas and understandings of Tor.

In beginning this pilot study, I made approaches by posting on the Tor mailing lists and on websites such as Stack Exchange[17] (a widely-used technology and programming forum) asking whether relay operators might be interested in taking part. This led to three interviews with relay operators and one with a volunteer contributor to Tor's codebase. My initial findings generated a series of potential 'leads' and themes for further study, as well as beginning to map some of the

[15] https://www.torproject.org

[16] https://www.onion-router.net

[17] www.stackexchange.com

relationships, values and practices within the relay operator community. In particular, I was struck by the fact that the Tor relay operators appeared to draw on a range of different, and often conflicting, views of Tor as a site of social action, and some were emphatic in their denial of Tor as possessing any politics of its own. Instead, they viewed running a relay as either a hobby or a form of public service, rather than a form of activism. Conversely, some also switched within the interview to framing Tor and privacy technology as deeply political, bound up with human rights discourses. In addition, the role of openness and decentralisation as key values, but also as practices of resistance and resilience, was an important early theme. It became evident from the way which they talked about the developers and others in the Tor Project that meanings and discourses were deeply contested within the Tor community, rather than set around strong shared perspectives, ideas and motivations. This initial ease of finding willing participants and interesting early themes indicated that a deeper study of the Tor Project might indeed be successful.

Following the pilot study, I developed a proposal for the main fieldwork. I applied for and received ethical clearance from the University of Edinburgh Law School for an in-depth qualitative study of the Tor Project, including semi-structured interviews, observation, and archival research. This involved anticipating any potential ethical issues which might be raised by the research, including risks to myself, participants, or the Tor community. In my First Year PhD Review Panel, I discussed potential ethical issues in depth with academics with relevant expertise from Edinburgh University's Law school and Science and Technology Studies group, then submitted a written discussion of these issues to the ethics board in my department, which was subsequently approved. I give a more detailed discussion of ethical issues in a later section of this chapter, however at this early stage my main concerns involved protecting the anonymity of interviewees in such a small community, ensuring the security of my data, attempting to mitigate potential harms to myself from malicious actors who might want to disrupt my research, and identifying questions which could cause harm to Tor or people within its community.

## Developing trust

I began my approaches to further members of the Tor Community (based largely around the personnel list on the Core Tor People section of the Tor website[18]), and this took place across the course of two years, sent in batches of three once every few weeks so as not to alarm or overwhelm the organisation. My initial forays into getting interviews with developers, however, were less fruitful, and I faced substantial suspicion at the outset from members of the Tor community who thought that I might intend to paint Tor in a bad light, or even be an undercover law enforcement agent. Equally, even those who believed that I was sympathetic to Tor's mission and sincere in my desire to represent their views fairly felt that there was a chance that I might not be able to anticipate all the potential ways in which the research might be used against them.

This was understandable: at the time I was conducting this research, the Dutch secret service had been revealed to be attempting to cultivate informants to gather information on the Tor Project's developers (Techdirt, 2017), and other core members of the Tor development team had reported being approached by law enforcement (CNN, 2016). The widespread characterisation of Tor as criminal or deviant in media reporting and academic study also posed some issues for the research, as respondents were very wary that I might not be sympathetic to Tor's beliefs and goals. This is a common (if not ubiquitous) problem within sociological or anthropological research and learning to develop this trust with a community or organisation is an important part of research practice for most qualitative researchers (Hine, 2008).

This suspicion was compounded due to my disciplinary affiliation: in a spirit of transparency, I was open from the outset in all my approaches that my research was being conducted within the field of criminology and I identified myself as a

[18] https://www.torproject.org/about/people/

criminologist. This engendered a substantial degree of suspicion and guardedness from my interviewees at first, most of whom thought that criminology was synonymous with 'crime science' and assumed that I was either working for law enforcement or interested in painting Tor as a tool for crime (which is very much the opposite of the forms of appreciative enquiry in which social worlds research engages). While there are many ways in which one could divide up the discipline of criminology, scholarship commonly distinguishes between 'administrative' criminology, which is aligned with the interests of the state and law enforcement (see for example, Rock, 1994; Farrington, 1985; Cohn and Farrington, 1998; Sherman, 2009), 'critical criminology', which takes a Marxist approach and uses criminology as a vehicle for critiquing state power (see for example, Box, 2002; Walton and Young, 1998; Young, 1988; Reimand and Leighton, 2015; Vold, 1951), and the 'sociology of deviance' approach, which engages in qualitative, appreciative research to understand how criminal and deviant social categories and ideas about crime and justice are constructed and produced by groups and institutions (see for example Becker, 1963; Hall et al. 2013; Taylor, Walton and Young, 2013; Garland, 2001, 2012; Feely and Simon, 1992, Bosworth, 2017). In fact, my approach and sensibilities could not be further from administrative criminology, and I was often tempted to reframe myself as a sociologist rather than a criminologist in my approaches. Despite this, I felt that it was important to be honest about my disciplinary affiliations; I would after all still aim to publish in criminology journals, and any research on Tor might well be of interest to law enforcement, even if not initially conducted in that spirit. I decided that being open about my intentions was the best way to allow my interviewees to approach the interviews with a good understanding of how their words might be used, not just by me, but by others as well. A number of the interviewees themselves brought up these issues, arguing that although my own motives might be well-meaning, I ought to think carefully about how my findings might be used by others with less sympathy for Tor.

Equally, I was keen to adopt an approach to interview practice which would facilitate the building of trust, both with the individual participants and with the Tor

community more generally. The rise of critiques within feminist sociologies and postmodern scholarship of more traditional approaches to interviewing has led to a radical reinterpretation of traditional ideas about objectivity and the role of the interviewer (Clarke; Sprague 1993). While traditional interview practice often requires the interviewer to attempt to minimise the presence of their own reactions, values, and opinions as far as possible, for fear of 'leading' responses (Ritchie et al., 2013), this newer feminist school considers this kind of confected objectivity to be false (DeVault, 1990; Haraway, 1997). Instead, this sort of research embraces the subjectivity of the process, and the researcher as an active part of data generation (Holstein and Gubrium, 1995). This both enables a more reflective and critical approach to qualitative enquiry, but rather than hiding behind an assumed objectivity, opens the inherent subjectivity of all interactions and attempts to create knowledge up to critique and inspection, leading to better research which is more cognizant of power relations (Kvale, 1996; Haraway, 1997).

Although I did not adopt some of the more radical departures from traditional interviewing which some of these methodological critiques have developed, they did shape my research practice as a softer set of sensitising concepts. I felt it counter-productive to attempt to hide my own political opinions about Tor and privacy (which I discuss in the introduction to this chapter), and although I let the interviewee's perspective be the dominant voice, I would indicate agreement, say where I thought responses were interesting or potentially contradictory, and make it clear from the outset that I was engaging with this in a spirit of appreciative enquiry (Leibling, 2015), and that I sympathised with and supported Tor's work. I felt that this was important as it gave the participants a better understanding of the sensibilities I was going to take into analysis and reporting, and also proved a key part of developing trust within the broader Tor community.

While my sympathies towards privacy activism and Tor doubtless facilitated my interviews (and the more I spoke to and interviewed people, the easier it became to get further interviews), this also had the potential to pose difficulties as well. In

particular, my support for Tor had to be balanced with my desire to develop careful and reasoned discussions and analysis of issues such as the crime and harm committed using Tor, which might, if not handled carefully, lead participants to feel that I had misrepresented myself, or, on the other extreme, to a hagiographic study of Tor which simply represented the 'party line' of the Tor Project. I believe that I have managed to navigate this well, and although the picture which this thesis paints of Tor is generally an appreciative one, I have not shied away from discussing critical perspectives on Tor in my interviews and analysis. In public presentations of my work, such as on my blog, or in talks, I have made my own political beliefs clear, but also stressed that I am aiming to investigate Tor rigorously through sociological research.

## Moving forward: fieldwork details and data collection

After little initial luck in getting interviews, I noticed on the public Tor Project calendar[19] that several members of the Tor community would be attending an international conference in Europe. I made members of the Tor Project aware that I would be attending, and managed to set up meetings with three developers which led to in-person interviews. Having now spent time with some of the Tor community, both through the interviews and in more social settings, I found that my approaches via email on my return had substantially more success. I had made contacts with other members of the Tor community at the conference and was able to both interview them remotely and begin the process of snowballing to further interviews. I was aware that some discussion of my research was ongoing in the Tor community and asked my interviewees to point interested potential participants in my direction. Cultivation of this trust was still a slow process. At the beginning, most of my interviews were with more junior or recently-joined members of the community,

[19] https://blog.torproject.org/events/month

with the older and more senior developers coming later. This was a deliberate research strategy, arrived at in consultation with my supervisors. From a social worlds perspective, this is ideal, as it gave room for these more hidden and contested perspectives to breathe and to structure the initial analysis, rather than being dominated by the more established views of the well-known and influential developers who had been with the community for a long time (Star, 1999).

My interviews continued over the next year as I made further approaches via email. I sought to get as wide a spread of viewpoints and as good a gender balance as possible, and to represent viewpoints outside a merely US perspective. In total, across the course of my fieldwork, I approached 62 members of the Tor community, largely via email (although some were approached in person at conferences). Of these, 32 people responded. Of these, 4 gave outright refusals, and two dropped out after an initial expression of interest. These approaches were not always without friction. My approaches to developers were made through publicly available email addresses listed on the Tor Project's "Core People" webpage[20], while relay operators were generally approached at conferences, on the Tor Project's mailing lists, or on StackExchange.

The final corpus of data spanned 26 in-depth interviews, listed in Appendix A. My sample of interviewees was broadly reflective of the diversity of the Tor community, based on the information available on the Tor Project people page[21]. This included nine developers (from fairly new members of the Tor team to some who had been involved since its early days), three other core contributors to the Tor Project who were not developers, eight relay operators, three developers of Onion Services, and three other members of the broader Tor community. Based on the information available, nineteen of my participants identified as men and seven did not. Despite active attempts at establishing a more gender-representative sample, this is

[20] https://www.torproject.org/

[21] Tor Project People Page: www.torproject.org/about/people/

unfortunately skewed towards men. An advantage of online methods, given the geographically dispersed nature of contributors to the Tor Project, was that interviews could be conducted with respondents in a variety of different countries. My participants were based in a range of countries, including Australia, Canada, France, Germany, Greece, Italy, Russia, Spain, the UK, and the USA. This is fairly representative of the core Tor community, though unfortunately misses members of the Tor community in the global South.

These interviews ranged from one hour to two and a half hours, and I transcribed them as soon as possible after the interview, securely deleting the audio thereafter. I also observed a meeting of the team involved in improving the usability of Tor and its website (having approached them via email). This meeting was carried out over group video and text chat, and conducted around the midpoint of my fieldwork. We discussed this again afterwards, and I was very kindly and sensitively asked not to attend again, as the usability work was something in which they particularly wanted to involve the less well-represented members of the Tor user community, and they didn't want to put off more reluctant members of this community from taking part. I agreed with this entirely, deciding to avoid any further approaches for observation of Tor Project meetings and instead focus on interviews.

As I progressed with data collection and analysis, the 'values' of the Tor community began to surface more clearly in my interview materials. I began to find that not only was the Tor community deeply heterogeneous, with a range of different values, positions, and understandings, the individuals with whom I spoke themselves made statements which appeared to articulate multiple contradictory understandings of Tor. This inconsistency indicated that many of the members of the Tor community were members of multiple distinct social worlds. As analysis and collection progressed, and these worlds, themes, and issues began to appear more strongly in the data, I began to bring in the archival materials as a complementary data source.

## Bringing in the material and ending fieldwork

Once I had begun to develop a sense for the main social worlds of Tor and their contours, and some of the key practices, forms of work, controversies and material design elements at issue in Tor, I began the archival portion of my research alongside continuing interviews. I discuss my approach to this in more depth in the analysis section of this chapter, however here it suffices to say that this involved an initial stage of immersion, when I read the first five years of the *Tor-dev* mailing list and much of the *Tor-talk* mailing list in full, then engaged in more targeted analysis and coding, tacking back and forth between interviews and archival work. This enabled me to get a view into the material working of Tor and real traces of the working practices of developers and others, providing a useful comparator to their own descriptions of these processes and indicating how they might have changed over time.

I finished the main body of my interview-based fieldwork by attending a second major European hacker conference with deep ties to Tor. By this point, I was beginning to reach saturation (Guest, Bunce, and Johnson, 2015), with new interview material serving to reinforce existing themes and points rather than leading to new lines of enquiry. Although I did not engage in this conference as formal ethnographic research, it did provide a useful glimpse into the "lifeworld" (Coleman 2010) of Tor and the broader European hacker community, allowing me the opportunity to speak to further members of the Tor project and discuss some of my findings.

At this conference, I gave a talk at a self-organised session about my research, presenting the findings to a small group of academics and some members of the Tor community. I did this to sound out the ideas I had been working with in my analysis, to provide an opportunity to get feedback from academics and from the Tor community on the emerging themes, and in the interests of accountability, to allow community members and participants an opportunity to raise any concerns they had about the research. At this point, I had more or less established a level of cautious trust with the Tor Project, illustrated by an exchange I had on the Tor Project's

mailing lists during the conference. I posted on the *Tor-talk* mailing list to let members of the community know that I would be presenting at the conference, and that if they wanted to talk to me about the research then this would be a good opportunity. This resulted in an accusation on the list from someone (not in the core community) who insinuated that I was a police informant and should not be trusted:

> so it is easy to recover all secret users of !
>
> good try, officer Ben.
>
> I respect your perseverance, great work
>
> *Tor-talk* mailing list, 2018

At this stage, a senior member of the development staff came to my defence on the list:

> Hello angry person who fears science,
>
> This is not a productive or helpful response here. It certainly doesn't help other people think that this list is a productive or helpful space. The research world has been critical for Tor, both in understanding attacks and in helping to design a stronger system: https://blog.torproject.org/tor-heart-pets-and-privacy-research-community and while these social science approaches to studying Tor as a community are not quite the same, they still don't deserve that response. Please keep it not just civil but also productive
>
> *Tor-talk* mailing list, 2018

Following this conference, I completed a few final interviews over the next few months and then finished my data collection. Although I had been conducting analysis throughout this process, at this point, I turned my focus entirely to analysis of my data. Before I discuss this, however, I first outline some of the ethical considerations which underpinned the research.

# Ethical considerations

## Ethics in Internet research

Ethical considerations are vital to any programme of sociological study and are widely recognised as at the foundation of good research practice (see for example established institutional codes of practice from the British Society of Criminology, 2016; British Sociological Association, 2017; Economic and Social Research Council, 2019; University of Edinburgh, 2019). Equally, ethical considerations should not be considered only at the beginning of the research, as a hurdle to be cleared during research design, but taken into account actively throughout all the processes of design, approaches, data generation, analysis, and writing up (Murphy and Dingwall, 2001). Additionally, they should not only relate to the immediate practical concerns of harm to participants or researchers, but also to the broader consequences of the research; how the findings will be used, and their implications for the community under study and for wider society (Sparks, 2002). Hence, critical reflection on harm and power should be embedded at the heart of every stage as an intrinsic part of research praxis. In this section, I set out some of the core issues which I considered throughout the research, and how I attempted to mitigate them, in particular around use of archival materials, anonymity, and potential avenues for harm to participants, myself, and the broader interests of Tor.

Informed consent forms the basis for most sociological interviewing and is widely regarded as best practice for this kind of research (Miller and Boulton, 2007). This means that the terms of the interview are made clear beforehand to the participants, properly explained in a way which effectively communicates their meaning, and are agreed by the interviewee, who has a free choice whether or not to take part. Rather than over-informing the participant with a great deal of irrelevant or technical information, this instead requires balancing the information given to ensure that the meaning and purpose of the study and what will happen to the data provided are communicated in a way which the participant can best

understand (Kvale, 1996). This includes the purpose for which the data are being collected, how they will be used and stored, for how long they will be retained, the participants' rights to withdraw, how issues of harm will be dealt with, and how the data will be processed. This is a particular issue for a community such as Tor, which is both extremely well-informed about data harms and has good reason to be cautious. It is common practice to record this through the use of signatures on a consent form which states these terms in full and records assent by both parties. While I negotiated full informed consent for all my interview participants, sent them copies of these consent forms prior to interview, and restated the main points at the beginning of the interview, several of my participants indicated that they would prefer to give consent verbally, rather than recording a copy of their signature. I respected these wishes, and as a result consent was recorded verbally for some interviews.

The Internet poses particular ethical issues of its own for researchers, especially around the use of archived online material, such as in forums or mailing lists (Eynon, 2009). The ethical frameworks developed for traditional offline qualitative research do not always capture all the potential dimensions of harm and consent associated with these new data sources (Eynon, 2009; Ess and Jones, 2004). The qualities of Internet platforms, conceived of as 'social spaces', often lead to information and communications which may have been considered private at the time, being made publicly available. Much online research uses a 'human subjects' (Basset and O'Riordan, 2002) approach, which prioritises the rights of research subjects over the interests of sociological research, and as a result a degree of caution is necessary when considering whether online archival material is a suitable source of data. In many ways, this is understandable – particularly given the increasing harms to which individuals are being exposed through the misuse of personal data, and the increasing volume of this which is now being gathered and archived by social media companies without their informed consent (Zuboff, 2015; Custers, van der Hof, and Schermer, 2014). While the potential harms associated with use of online data are serious (Kozinets, 2010), Basset and O'Riordan argue that over-caution in the use of

online data itself constitutes an ethical issue, potentially leading to the silencing of the perspectives and interests of already-vulnerable communities. These online data sources have also proven important vehicles for the foregrounding of hidden or marginalised voices and perspectives, such as those in LGBT communities (Basset and O'Riordan, 2002).

An overly-restrictive approach to online research fails to account for the differentiations in private and public communications which occur therein, conflating online texts (which are often authored explicitly as public statements for wide consumption) with authors. As such, an approach which takes concerns of privacy and harm into account and reflects on the actual contexts in which particular online data sources were authored should not necessarily result in a restrictive ethic which puts all such sources out of bounds (Basset and O'Riordan, 2002; Ess and Jones, 2004; Lomborg, 2012). Through careful consideration of how results are analysed and presented, and the particular contexts of different sites and archives, ethical research on online archives can be conducted. Equally, it is now well-established within sociological and criminological research that informed consent for use of mailing lists and forum data is not always best ethical practice (given the burden of collecting this from people who may have left these communities decades ago), and that this can be waived as long as the data could reasonably considered to be public and care is taken to report findings about groups and communities rather than specific individuals (Martin and Christin, 2016; British Society of Criminology 2016).

Tor especially exemplifies this problem, as its radically-open approach puts a huge amount of archival information, including emails and meeting minutes, freely accessible online (Gehl, 2018b). I took the view that some of this material would be within bounds for ethical research, and some would not. The mailing lists, code, and issue tracker discussions I judged to be suitable, as these were either professional documentations of the work of Tor explicitly intended for public consumption, or places where communication with the community was engaged in with the knowledge that it would be recorded and made public. On the other hand, I judged

that observing meetings and using IRC logs would be out of scope, as this might make people in Tor's privacy-conscious community feel less able to contribute to these discussions. Equally, there is an ethics case to be made that these more intimate spaces of community interaction should be approached with care (Kozinets, 2010; Pink, 2016), and I judged that the benefit to the project of this source of data would not justify the potential invasion of these semi-private spaces. By building legitimacy within the Tor community, and discussing these other potential sources with my interviewees, I was able to get a better understanding of which voices I might find foregrounded in different places, the potential power dynamics and sources of harm associated with different sites, and develop a strong case for making use of the data sources which I did. The mailing lists were a particularly suitable balance between foregrounding hidden perspectives, as they are generally open to contributions and often hosted contentious discussions, and minimising harm, as they are well established as a public record of Tor's community debates. I thank the Tor Project staff who discussed these issues with me for their help.

Taking this into account, I made senior members of the Tor Project aware that I would be conducting research into their public mailing list archives, ensured that they were happy for me to do so, and have taken care not to include identifying information in any quotes which I use. I also asked their advice around any potential issues of harm which might be caused by my reporting of mailing list discussions at the outset of my archival research on the mailing lists. Rather than an potentially-intrusive practice of "lurking" (Eysenbach, 2001; King, 1996) in the Tor community, I was very clear in communicating on mailing lists what I would be doing and the aims of my research, and largely restrict the analysis herein to older discussions which are less likely to pertain to 'live' issues in the Tor community. Equally, as the mailing lists which I study herein were well-established as public to their participants, I believe that the participants in these discussions did so with the knowledge that their comments might come under scrutiny, especially as these mailing lists were explicitly set up to provide a public record of decisions about Tor's design and allow public conversations within the community. Finally, I engage in this analysis not with the

intention of finding 'scoops' about Tor, but to bring to light the wide array of hidden work which underpins it, and to give a voice to some of these more hidden perspectives.

Other researchers have developed this further, bringing ethnographic practices and methodologies into study of the Internet (see for example, Markham 1998, Coleman, 2014; Kozinets 2010, Pink, 2016). While the "distance" (Eynon, 2009) which separates the people who authored online materials and the researcher is doubtless greater than for offline research (though not always, as in the case of offline archival research), Kozinets (2010) argues that participatory research, in which the researcher immerses themselves into the community which they are studying, is one way of reducing this and hence mitigating some of the potential harms associated with studying online communities. This both makes the community aware of the research and its aims at the outset, and allows the researcher to develop a deeper understanding of the expectations of their participants and the potential avenues through which harm might occur. Through meticulous public documentation of the research process (Kozinets argues for the creation of a research website to facilitate this), the research participants have ample opportunity to comment, to ask questions, or to raise concerns (Kozinets 2010).

I was wary of adopting a fully 'ethnographic' approach in this research, and ended up maintaining substantially more distance from the Tor community. The first reasons for this are practical: my buy-in from the Tor Project was limited at first, and while they were happy for me to interview and approach community members who wanted to participate, there was little prospect of them officially endorsing the project or allowing me to conduct more embedded research, especially as this might put off other members of the community from participating in their discussions. The second set of reasons are reflective of the power dynamic between me as a researcher and the Tor Project. In qualitative research it is vital to cultivate a reflexive understanding of whom the researchers and participants are and the relationships between them (Clarke and Friese, 2007, p368). While other routes to

immersion would have been possible – for example, I could have started running a relay myself or contributed to community discussions in other ways – I was very reluctant to attempt to become part of the community in this way. While this would undoubtedly give me insights into the practices and values of this group, it would also complicate my position as a researcher, placing the Tor Project developers in the awkward situation of being obliged to engage with me as a member of the community. As I wanted participation to be on a strictly voluntary basis, I felt maintaining more distance and focusing on interviews and archival research was appropriate. I did, however, take up some aspects of Kozinets' (2010) "honest and open" approach, creating a project blog where I documented my research aims and some of my fieldwork progress.

## Anonymity for experts

While anonymisation of participant responses is common practice in the social sciences (Thomson, Bzdel, Golden-Biddle, 2005), it was of particular importance to the Tor community and required especially careful handling. Anonymisation of interview data is widely used to protect interviewees from harm, for example, if their participation might bring them to the attention of powerful actors, and to allow them to speak more freely and reveal information which they otherwise would not (Smythe and Murray, 2000). It also reduces the pressure on them to give a 'party line', which they might feel were their statements to be publicly attributable and hence scrutinised by their community. This goes beyond merely not reporting the name of the interviewee associated with a quote (especially in small communities), and quotes need to be selected with care to not reveal identifying information while preserving the richness of the data (Saunders, 2015). I decided that, unlike for many studies, where the name of the organisation is not revealed in order to protect the anonymity of respondents, this was not feasible given the importance of Tor's particular history and the relatively unique nature of the organisation.

In many studies, the power balance lies substantially in favour of the researcher, who will have a better position from which to understand anonymisation techniques, disclosure risks and other such factors than the people whom they are interviewing (Brinkmann and Kvale, 2008). In the Tor community, however, understandings of anonymity, consent, and information disclosure are highly specific, advanced, and atypical. The Tor community contains many people who are deeply concerned about privacy issues, especially where they concern data collected, stored, and processed about individuals. Additionally, the community contains several individuals who are world-leading experts on privacy technology, anonymity, and data ethics, who have spent whole careers working on data privacy issues and advancing academic and technical understanding of anonymity. As a result, conducting sociological research on Tor required managing different understandings of anonymisation to that which might be expected of most other groups.

In the spirit of providing as strong anonymity guarantees as possible, and in the knowledge that they would be particularly well-placed to critique my practices, I designed an anonymisation strategy which I believe balances making the best possible use of these data while also protecting my interviewees. All quotes are presented anonymously, and I have as far as possible taken precautions to ensure that the identities of the people whom I interviewed remain secret. I do this despite the fact that several of my interviewees said that they were happy for me to attribute their quotes to them. This is because Tor is a fairly small community, and, in the spirit of more technical definitions of anonymity (Syverson, 2009), I wanted to retain the largest possible pool of potential sources of any given quote. Every individual named would therefore, through deductive reasoning, reduce the anonymity of those who did not wish their responses to be attributed. Where participants had particularly recognisable ways of speaking or discussed information which would likely make their identity clear to someone with a knowledge of the Tor community, I took care to remove or disguise these traces from the published outputs, while retaining the sense of the statement (where quotes have been paraphrased, this is indicated).

Despite this, it is extremely difficult to fully deanonymize the outputs of sociological research in small communities (Thomson, Bzdel, Golden-Biddle, 2005; Wiles et al., 2008, p417). In a community of Tor's size, with such high levels of specialisation, there are often only a handful of people who could conceivably make informed comments about particular aspects of Tor's work. As a result, I took steps to mitigate any potential harms resulting from inadvertent deanonymisation. I largely avoided speaking about potentially sensitive topics and have been careful to avoid using quotes where there was a risk of harm or embarrassment to the respondent if they were identified. A good deal of this mitigation took place through the interview itself, and I made sure to discuss with participants beforehand my aims and let them know that I wasn't interested in talking about sensitive topics or information that would be problematic if released into the public domain.

## Safety, power, and harm

Empirical research is not without risks, and even an apparently innocuous study can result in unforeseen harms to the individuals or communities being researched, or to the researcher (Hajistavropoulos and Smythe, 2001; Bloor, Fincham and Sampson, 2010). In this sub-section, I briefly lay out some of the main potential sources of risk which I identified throughout the research and the steps I took to mitigate them.

Given the nature of Tor's work, which brings it into contact by design with groups attempting to work against powerful actors, its adversaries include extremely well-resourced actors, including the military and secret services of nation states, and organised crime groups. As an attractive target for a range of powerful organisations, Tor is subject to particular safety concerns which other similar organisations might not be. The ethics review at my First Year PhD Review Panel for progression into the main fieldwork identified a number of potential concerns with safety which needed to be addressed. The presence of these unlikely but extremely serious situations entailed protecting myself, the Tor Project, and the people who work with them

from adverse consequences from the research. The first concern was data security. Although I was not intending to ask any sensitive questions of my participants, I was still aware that aggregating the information I was gathering, especially if tied to individuals, would pose a potential risk if any of my devices were breached. As a result, interview data and transcripts were kept securely in a single copy stored on an encrypted partition of a USB disk which I kept on my person or in a locked desk drawer. I travelled to the US at one point during my research, and made sure to leave this USB disk in the UK in case of seizure by US Border control. I chose to minimise any further records of the interviews, other than a project management file stored in the encrypted partition of the USB disk, and removed saved passwords to email accounts from my devices before crossing the border each way. I also planned for potential scenarios involving law enforcement, such as a request for my raw data. In this case, I would attempt to legally fight disclosure of this as far as possible, but would inevitably be faced with the prospect of handing this information over. This is not without precedent: for example, researchers at Boston College were forced by law enforcement to hand over their interview recordings and details of participants for a highly sensitive study they had carried out on ex-IRA members (McDonald, 2016). As a result, I sought to minimise the collection of any identifying or sensitive information, and made this clear in my interviews.

The archival research itself poses important questions of harm (Tesar, 2015). Although the Tor archives are open source, and I had discussed this research with the Tor leadership, some of the people featured in these archives could potentially object to me dredging up their email conversations from twenty years ago. Although they were sent in the knowledge that it is a public board, the context of statements can shift a lot in twenty years. In the nineties, far fewer people had access to the internet, and the likelihood of someone hunting through tens of thousands of emails in an obscure archive was very low. By bringing these emails to a broader audience, I am exposing them to a kind of scrutiny which the people who sent them might not have envisioned, as they likely thought about this as scrutiny of the security properties of their decisions rather than sociological analysis of their values and

practices. I deal with this by not identifying any of the interlocutors by name, and by trying to be sensitive in how they are presented, talking about groups and ideas rather than particular individuals.

In addition to more general concerns, I had to contend with a particular issue which posed difficult questions as to best ethical practice. My fieldwork began in the immediate aftermath of a serious crisis in the Tor community. A prominent developer on the Tor Project, Jacob Appelbaum, was accused in 2016 by several members of the Tor community of sexual assault, bullying, and abuse[22] (Loll, 2016). This led to a major upheaval within the Tor Project: for most of its life, Tor had been known for being *lassiez-faire* with regards to organisational structure and practices, and it appeared to many that the time had come for serious change. Appelbaum was expelled from Tor and a new Board of Directors were appointed. This led to a programme of professionalisation within Tor, including aims to transition to more formal and healthier working arrangements, proper human resources support, and a range of changes intended to prevent any developer taking too-prominent a role in Tor's public life[23] (Marechal, 2018).

My initial feeling was to exclude this scandal as a topic of analysis and avoid asking questions about it. This was both in order to avoid causing additional harm by potentially asking participants to re-live traumatic events or disrupt the community's attempts to recover from this crisis, and because I felt that this would generate suspicion among the community that I was a bad faith actor with either a prurient interest in this topic, or a desire to stir up trouble in a community still in the process of recovery. Additionally, this was not the direct focus of my research topic. However, in practice, this topic was impossible to avoid: nearly all of my interviewees actively brought this up themselves and some spoke about it at length. It became impossible to discuss the changing values of the Tor organisation without discussing

[22] www.jacobappelbaum.net

[23] https://blog.torproject.org/statement-0

either the events themselves or the profound organisational changes for which they provided a catalyst. This in fact ended up being an important factor in the research – a signal event which communicated a shift in the underlying values and social organisation of Tor (which I discuss in more depth in Chapter 6). As a result, I do discuss these accusations and the organisational change which resulted from them in depth in Chapter 6, and attempt to do so sensitively and with my focus on how they reflect changes in the social worlds of Tor. While this all clearly also pertains to important issues of gender, the feminist movement, power relations, and abuse within technical communities as well, I have not engaged in these questions in this thesis, as I feel they deserve a fuller exploration in their own right than I am able to provide here (for a more in-depth exploration of this, see Nathalie Marechal's PhD thesis, Marechal, 2018).

Moving on to broader questions of harm, I needed to account for not only the risk of harm to the people whom I interviewed, but the broader implications of my research for the Tor community, the Tor Project, and the privacy technology community more generally. I was particularly concerned in designing and carrying out the research with either presenting information which would be damaging to Tor, or revealing information about the resilience practices, community structure, or key individuals in Tor which might be of use to law enforcement and state security agencies who might wish to undermine the Tor Project. I made sure that I gave careful consideration to what I presented in my research outputs, including presentations, reports, and this thesis, and did not include anything which I thought might primarily be of use to state security actors attempting to destabilise the project.

All research has a normative dimension, and the choice to give voice to a particular set of people is in itself an intervention in politics. Brunton and Coleman (2014) argue that the very act of conducting this kind of materially-grounded research on technical communities whose practices bring them to the interest of law enforcement itself has an ethical dimension. By bringing material reality into contention with the often speculative and "hyperbolic" depictions of groups like

Anonymous or the Tor Project, one can provide a counterpoint to these narratives and shape public discussions to be more grounded in the actual capacities which these groups and technologies have (Brunton and Coleman, 2014). As a result, I believe that I have conducted this research in a way which not only minimises any potential harm to the Tor community, but also one which potentially might have positive social effects, bringing these somewhat hidden perspectives and voices to light and potentially providing some insights for the Tor community as well. Despite this, I cannot, of course, be certain how this research will be used or interpreted by others, or how it might shape public conversations about Tor.

# Analysis

## Analysis in the social worlds framework

Social worlds theory, as with other interactionist frameworks, favours an inductive approach to analysis. This involves a coding strategy which works from "the bottom up" (Straus and Corbin, 1997), coding the individual meanings of statements at the micro-level, and clustering these into higher level categories and concepts which arise from the data themselves. This is distinct from a deductive approach, which begins with pre-defined semantic categories into which the data are fit after collection. Clarke develops this into a more formalised methodological approach through *situational analysis* (see Clarke 2003, 2011), which draws on Haraway's (1997) theoretical work and methodological critique within Science and Technology Studies research. As with social worlds theory, this is not a programmatic framework, rather a set of approaches, maps, tools, and sensibilities with which to approach and guide a programme of social worlds research. This focuses on processes of mapping, bringing in social worlds, but also other levels of consideration - mapping materiality and actors, or particular rhetorical positions on a topic. Situational analysis brings together the focus of social worlds on discourse as bound to social action with more Foucauldian concerns of discourse in the abstract, in complementary ways which

build up an inductive picture of the worlds of discourse, practice, and sensibility which accrete around sites where social life is produced (Fairclough 1992).

Clarke (2003, 2005, 2007) suggests combining interview coding and archival research with the generation of three kinds of maps which assist in the development of higher-order coding structures and the generation of findings. The first of these are situational maps, which set out the different actors, technologies, organisations and groups and the relationships between them. The second are social worlds maps, which show the different social worlds which accrete around the arena of concern, and how they relate and overlap. Finally, Clarke suggests positional maps, which map "issues, positions on issues, absences of positions where they might be expected... and differences in discursive positions central to the situation under study..." (Clarke, 2005, p126). By separating these discourses from particular people, groups or professions and analysing them first in their own right, this reflects the fact that people can and do hold multiple contradictory positions and are often not "bound" irrevocably to a particular group. Equally, discourse can and does overlap between social worlds, and this mapping of discursive terrain can provide a useful way to get past a sole focus on individual worlds and find the points of overlap and conflict between them. Using these rough maps (which can be found in Appendix B through F) together with more traditional grounded coding strategies allows for useful mechanisms and practices for stepping between different levels of abstraction and understanding how they interrelate.

## Coding and mapping

In conjunction with these maps, I used more familiar approaches to coding the interview data itself. Using NVivo qualitative research software, I inductively coded the transcripts of the 26 interviews. This involved working through the text of each interview and coding meaning at the level of sentences (or small groups of sentences). From the first interview, and increasingly as I gathered more data, I

clustered these together into higher-level concepts. These were then further clustered together, until a final higher-level structure was arrived at. This broadly, at the top level, grouped the interview data into information about practices, community structure, privacy values, and crime.

NVivo's coding system is designed around a hierarchical, tree-based model, where lower level codes are sorted into branches, leading to a many-to-few approach in which one works backwards from empirical complexity into simpler higher-order structures. This process of condensation, however, serves to generate a model of coding which seems ill-suited to social worlds analysis, which looks at connections and multiplicity. Therefore, while NVivo was very useful for the inductive coding and aggregation of discourses, facts, and themes in my data, I needed to supplement it with other approaches. This is where Clarke's maps become a vital resource, allowing the generation of horizontal links and representation of the *relationality* of these codes and discourses. Mapping these horizontal topologies within levels of abstraction across different coding 'branches', I found a set of three broader perspectives which formed a pattern across the different groups of codes. These constituted three discrete, self-consistent frameworks of understanding within the Tor community. Although these were by no means exclusive to particular groups, they did appear to be linked to the logics of particular types of working practice: the engineering work of the developers, the campaigning work of the activists, and the maintenance and administrative work of the relay operators. Having mapped discourses, I could then therefore group these perspectives into particular social worlds.

At this point I engaged, as Clarke (2011) suggests, in an intense focus in the discourse of these worlds. As these broad maps of social worlds, practices, discourses, people, and relationships were developing, I drew on the library of *sensitising concepts* which I describe in detail in Chapter 4. In particular, the idea of boundary objects proved useful in mapping how the different worlds overlapped, and how they related to the technological design of Tor itself (as I discuss in Chapter 6). Once this had been

mapped out (the results of which I present in Chapter 6), I could use these social worlds as a framework for exploring other questions, asking, for example, "which world or worlds is this discourse attached to?", or "what does this world think about this issue?". This often led to spotting things I had missed and helped with siting ideas and practices in their broader context within the Tor community.

I then took these social worlds and mapped them onto the practices, work, technologies, hardware, software, and groups of Tor. At this point, the archives became a vital record of material practices and places where the connection between values and the material could be elucidated. I approached this archive of material by drawing key sensitising themes and lines of enquiry from my interviews. I began by immersing myself in the data, reading from start to finish the first five years of Tor's *Tor-dev* development mailing list, large parts of its later years, and large sections of Tor's more informal *Tor-talk* mailing list, writing notes on content and marking up what seemed like important discussions or places where Tor's values were being articulated or struggled over. I reduced this material to a handful of key design discussions, from which I chose a single core controversy on which to focus in depth, namely Tor's choice not to include padding traffic on the network which would have further strengthened user anonymity, and instead prioritise usability and speed (I explain this in greater detail in Chapter 7). This was selected based not only on my own reading, but through the interviews, as it was often brought up as a particularly foundational and contentious aspect of Tor's design.

While I first intended to look at the different actors involved in these discussions and how they tried to get their particular vision of the project inscribed into the design, in fact I found a remarkable degree of consensus. Development in Tor appeared to be a more mutual process of working through and refining different ideas and values, rather than an agonistic struggle between different interests. This kind of iterative, cyclical, tacking-back and forth has been well-established within studies of Open Source communities and infrastructure development, in stark contrast to more traditional, linear models of development (Guedenna 2015; Pollock and Williams

2008, 2010; Williams, Stewart and Slack, 2005). I therefore decided to focus on the evolution of these discourses and category systems into a coherent social world across the discussion, rather than the actors themselves. A range of "tricks of the trade" (Star, 1999, p384) are offered by Star as strategies for directing this kind of research. In addition to Latour's (2005; 2007) approach of bringing out controversies as sites where values are brought to the surface, Star (1999) suggests a range of other approaches for pulling out sociologically interesting findings from the vast archives associated with engineering and infrastructural projects. Two of these in particular proved useful. The first of these was the identification of 'master narratives', frameworks of imagined users, purposes, and contexts with which the technology is designed to interact, and the creation of 'others' who are left out of these frameworks. This involves mapping out systems of categorisation and representation: the way in which people doing technical work seek to represent the world, and how this becomes inscribed into the logics of the system. This allows the researcher to discover the values implicit in the system through, for example, critical examination of taxonomies of user types or use cases, and hence to find out what kind of world the system envisions, and who might be left out. The second of these 'tricks' is the search for kinds of hidden work – the work which goes on behind the scenes that fades into the background, but which is nonetheless vital to infrastructure (Star, 1999). Exploring these, their links to social worlds, and their change over time, was particularly productive, surfacing many of the key findings from the archival research. Finally, in some cases, values, ideas, and discourses came right to the surface, in discussions of contentious issues, or explicit debates around the broader politics of Tor and its design.

Throughout this process, I moved between my existing interview data, the mailing list discussions, other secondary forms of archival data (such as bug and issue trackers), and the ongoing business of interviewing, as I brought in new questions and topics as they rose to prominence in the archival study. This approach bears some similarity to the kinds of mappings drawn in Brunton and Coleman's research (2014), which pull apart the technical underpinnings of their subjects of enquiry and

relate them to distinct frames of sense-making: the "multiple, sometimes contradictory, and sometimes coexistent experiences that obtain on the network infrastructure" which "thrive together, like commensal bacteria in which the by-products of one happen to create a suitable environment for the population of another" (Brunton and Coleman, p82). I believe that through this exploration of these rich data sources, and with the help and generosity of my research participants, the research in this thesis represents an initial, but hopefully rich and representative, study of some key aspects of Tor.

## Conclusions and methodological reflections

This chapter has set out the key methodological decisions I made throughout my research design, fieldwork and analysis, drawing on the theoretical and methodological literature from which I drew inspiration and guidance. I have set out my main four research questions and my broad strategic approach to answering them, and how I designed my interview schedules and approaches to archival research. I sketched out my fieldwork journey and the process of building trust with the Tor community, and reflect on some of the key ethical issues posed by the research, in particular around anonymity, the use of archival material, and harm. I have also discussed my analytical approach and the use of Clarke's (2003) *situational analysis* and Star's (1999) *ethnography of infrastructure* approaches to mapping, coding, and making sense of the densely packed human and technical communities which accrete around infrastructures.

I have enjoyed the writing up and analytical portions of this PhD immensely, however the most thrilling, exhausting, moving, and rewarding part has been the fieldwork itself. I value enormously both my experiences of doing qualitative interviewing and of archival research, which were exciting and draining in different ways. In particular, negotiating concerns around legitimacy was an issue which caused me some anxiety throughout, as I was concerned that I might give a negative impression of my intentions and have a gatekeeper close off access to other important potential

participants. In retrospect, I could have mitigated this by developing a more public relationship with the Tor Project, engaging in discussions on social media or commenting on their blog posts. This might have enabled more interviews with some of the core developers and access to other spaces in the Tor community, such as developer meetings, however this may also have backfired, potentially compromising the objectivity of the research or putting off some of the more hidden voices in the community from speaking to me.

While I have aimed to conduct this research on an open and ethical basis throughout, this process is nonetheless still ongoing. As I write up my results in the form of this thesis, and begin to present them at conferences and in journal articles, these ethical considerations continue to operate, and I am aware of the continuing potential of my research to influence the discourse which surrounds Tor, for better or worse. I now intent to feed my research back into the Tor community, circulating it amongst my participants and others in the Tor Project so that they can play a role in shaping the future life of the research, so that it can continue as a dialogue rather than merely a series of statements.

Although I believe that I have been successful in speaking to a range of people across the Tor community and that this research presents a representative view of the topology of values, discourses, and practices within Tor, it is nonetheless only a partial perspective based on the people with whom I was able to speak. Building on my findings in future research would undoubtedly involve closer co-operation with the Tor Project itself, if possible. Having established myself more, and with evidence of research findings, of my approach, and of my sensibilities towards Tor and privacy technology, I would feel more comfortable asking to attend Tor's developer meetings and work more closely with the Tor Project (if possible) in a more traditionally ethnographic approach. Additionally, the users of Tor are almost entirely absent in the account I give here, other than as *implicated actors*. Although there is a wealth of literature on Tor users, future study could entail broadening the picture of the social worlds I have identified here to see where and how they seep into the Tor

user communities (and their own worlds), and how they are shaped by the users themselves.

I now turn to the results of the thesis, which I present in the following four chapters (Chapters 6 to 9). Each of these is broadly organised as a response to one of the four research questions I outlined at the beginning of this chapter. In the first of these, Chapter 6, I map out and characterise the three key social worlds in Tor: the *engineer* world, the *activist* world, and the *infrastructuralist* world. I then explore in detail how they overlap, interact, conflict and change, and the consequences of this for Tor as an infrastructure.

# chapter 6
# the social worlds of Tor

## Introduction

Tor is underpinned by a rich and vibrant cultural life, and exploring, mapping, and representing this was one of my main goals from the outset. On beginning my research, my initial interviews revealed a very different picture than I had expected. I had imagined Tor, given the deeply political nature of its work, as an organisation with a strong set of core values and well-aligned shared perspectives. In fact, I found a dense and heterogeneous aggregation of different ideas and ways of making sense of the core work of the community and the social meaning of Tor itself. As I describe in Chapters 4 and 5, I use the social worlds framework to map this social life and to distil this complexity into a set of three social worlds. I use these social worlds to explore Tor as a site of social action, collaboration, conflict, and consensus. In this chapter, I focus on my first research question: what are the social worlds of Tor, and how do they interrelate?

Social worlds are not only ideas and discourses, but embody practices, sensibilities and interpretive frameworks for making sense of the world. They are deeply linked to the material life of technologies, but are also relational, able to interact, conflict and influence one another in the abstract. They are a link between the material and the semantic, a form of embodied discourse which is lived through practices, interactions, and relationships with people and technologies (Clarke and Star, 2008). In this chapter, I begin with a mapping of the main social worlds of Tor which I have identified and characterised. Although these worlds are not recognised as such within Tor, coming instead from my own analysis of my fieldwork interviews, I have

found them a useful framework for making sense of some of the main questions, issues, and contradictions facing the Tor Project.

I suggest that this mapping exercise is in itself valuable, a form of 'thick description' (Geertz, 1973, 2008) of the Tor community, and the lives and values of the people therein, which aims to brings some of the more hidden voices and perspectives in this community to light. My exploration of the ways in which Tor manages to square these mutually contradictory value systems and deal with the conflicts between them suggests potential explanations for why Tor has managed to succeed in promoting this "collaboration without consensus" (Star, 2010, p604) where other organisations have failed.

I begin this chapter with a mapping of the different people, groups, and technologies which make up Tor and the Tor community. I then move on to the values of Tor with an exploration of the Tor's community's perceptions of privacy more broadly and the threats which they feel it faces in the contemporary era. I then argue that this shared focus on privacy and internet freedom actually masks a deeply heterogeneous community who understand these core values in very different ways. I refine this web of discourse and values into three ideal type social worlds which I characterise in turn as the *engineer* world, the *activist* world, and the *infrastructuralist* world. In the next section, I explore how Tor manages the overlaps, discontinuities, and points of rupture between these worlds through the idea of privacy as a 'boundary object', creating a détente which has allowed the organisation to survive. I end this chapter by illustrating what happens when this détente is shaken by crisis, reflective of how these Social Worlds have begun to shift and change in recent years.

## Mapping the Tor community and infrastructure

Before I turn to the values and worlds of the Tor community, it is useful to map out the main human and technical components which make up Tor. This constitutes

Clarke's first kind of map, a situational map, and serves to ground the discussion of values and meaning-making which follows in the material infrastructure, community, and work of Tor (Clarke, 2003). A simplified graphical representation of this map can be found in Appendix B.

The Tor Project is the organisation at the heart of Tor, taking the main responsibility for its development and support. It is headed up by the Tor Project Board of Directors, a group of experts and leaders from civil society organisations and academia who act in a consultatory capacity and provide advice in steering the organisation and its connections to public life. The developers and other staff working for Tor are arranged into 'teams', each of which specialises in a particular part of Tor. These include the network team, which works on the programs which deliver the Tor network, the applications team, which develops user-facing aspects of Tor, such as the Tor Browser, the UX (user experience) team, which feeds insights from the Tor user community to the network and applications teams, the community team, which conducts outreach and advocacy, the metrics team, which collects and analyses information about the Tor network, the anti-censorship team, who aim to circumvent nation state attempts to block Tor around the world, the sysadmin team, who run the Tor Project's own systems, the operations team, who manage human resources, administration, and accounting, and the fundraising team. Historically, only a handful of developers were actually paid by Tor, with the rest contributing on a volunteer basis, but since Tor's efforts at professionalisation, the organisation supports an increasing number of paid staff. Tor is funded by a combination of grants from the US government, civil society organisations, private companies, and crowdfunding. Sometimes, this funding directly pays for particular research, such as improving Tor's usability or translating its programs into non-English languages. In addition, Tor has links to a range of other technical projects, including the people developing the Tails operating system or the developers of Onion Services such as SecureDrop, and looser links to organisations such as Mozilla, who make use of some of Tor's security and anti-tracking updates to their Firefox browser.

In addition to the core Tor development teams, there are other projects under the Tor 'umbrella'. The most interesting and notable of these is the Open Observatory of Network Interference (OONI) project. The OONI project conducts research on Internet censorship around the world through an infrastructure of collection devices run on a volunteer basis, similar to the Tor relay network itself. Contributors can download the OONI software onto their computer or phone and run tests on their local networks to detect different kinds of blocking and surveillance. This provides valuable information for journalists, for example, where governments censor the Internet in advance of elections, and important intelligence for the Tor Project developers concerning what practices of surveillance and censorship are in operation around the world. They also engage in a substantial amount of outreach work, travelling around the world to work with Internet freedom activists and better understand their needs.

In addition to technical experts, Tor also plays host to a range of people with rather different skills. In recent years, Tor has taken on board more people from an activist background, and there are now a number of people within the Tor core community with experience in lobbying, public relations, policy, user security training, working with activists, journalism, fundraising, and public outreach. It has also been making efforts in recent years to strengthen its ties to internet freedom activist and campaigning organisations such as the Electronic Frontier Foundation.

Tor is not just a computer program which people run, but an anonymity network: an infrastructure which people access through the Tor Browser. This is comprised of around six thousand 'relays', servers run by volunteers around the world which carry encrypted Tor user traffic and bounce it between them before sending it to its final destination. For reasons of trust and safety, the Tor Project tries to have as little as possible to do with running the network itself, and so a loose community of relay operators has sprung up over the years. In addition, the wider Tor community comprises a range of other contributors, including developers who make use of Tor's network in their own technologies to provide anonymity and security, and

information security researchers and academics who scrutinise Tor's code and attempt to break it in order to make it stronger.

## Privacy at the heart – Tor's values

If the Tor community can be said to be united around a common value, it is privacy. Privacy is at the heart of Tor's mission and it is privacy which gives Tor its sense of meaning and identity. Before I map out the heterogeneities within the Tor community, I first set out here some of the similarities they share; in particular, their shared commitment to privacy as a value, and the idea that this is under threat in contemporary societies.

> And I think there are for sure some common principles, and things that motivate our work, which is, you know, we believe in the right to privacy, we believe that people should be able to engage in conversations in a way that is private, and that in the end, people should have the right to access all information.
>
> Participant H - Tor core developer

The rise of 'mass surveillance', as revealed in the Snowden leaks, is of particular concern to the Tor community, and was brought up by many of my participants. In particular, they link the use of these techniques not only in authoritarian nations, but also in liberal democracies, to a dangerous trend which is threatening global society. These increasingly technocratic technologies of control and the use of automated processing of large datasets of intimate information about people were perceived as having potentially disastrous consequences, intensifying social control and removing large parts of how countries are governed from democratic scrutiny.

> For me the thing that really concerns me about… web monitoring or internet monitoring is that people are… like, basically all of politics is online now. Apart from some TV, you know? But it's very much, you know, Twitter and everything, all the other web stuff. And if this is all monitored by governments, including my own government, it's extremely dangerous for democracy… the web, while it was intended as this wonderful new, you know, invention to… essentially add a lot of freedom to people, unfortunately it has this sort of unanticipated, or somewhat

> unanticipated potential for doing the opposite and we have to be really careful that we don't slide into this disaster.
>
> Participant C - Tor core developer

My participants also drew links between issues of surveillance and other forms of online power, especially Internet censorship. A side-effect of Tor's frustration of attempts to surveil the traffic of its users is that it is also a powerful tool for evading online censorship. There is a strong 'free speech' ethos within the Tor community, and they generally saw Tor's mission as encompassing both resistance to surveillance, and to censorship:

> As censorship has increased around the world and internet freedom has declined, we realized we needed to step up our game to outpace the censors preventing people from enjoying the human right to freedom of expression and access to information on the internet.
>
> Tor Project blog, 2019

This ethic of resistance is not only concerned with government power over the Internet, but also with the power exercised by the private companies who manage the Internet's infrastructure. The 'surveillance capitalism' practiced by the Internet giants such as Google and Facebook was a particular source of anxiety (Zuboff, 2019).

> But I'm worried. Not about government or three letter agencies, but advertising. Market forces and Moore's law makes bulk surveillance both easier and more profitable every year. Maybe I underestimate the public's desire for privacy, but when offered convenience in exchange for it, I'm uncomfortable thinking where we might end up.
>
> Participant E – Tor core developer

However, beyond this commitment to privacy, free speech and resistance to online power, these values are refracted through the different practices, motivations and perspectives of the Tor community into rather different forms, which understand the salience of privacy technology to power and politics rather differently. In practice, when I began the research, I found Tor not to be centred around a unitary set of shared values but to be remarkably heterogeneous, with even individuals drawing on

multiple, complex, and often mutually contradictory understandings of the work in which they were engaged. This is also well-recognised within the Tor community itself:

> I think one interesting thing about Tor is that because we are such a large and diverse community, it's impossible to actually agree on a small set of ideals and values and goals for the large group.
>
> Participant A – Tor core developer

Through my research, I have separated out these discourses into self-consistent perspectives, or social worlds. This set of three core social worlds at the heart of Tor, how it is understood by its community, and its position as a site of social action, forms the main analytical framework which underpins this thesis.

## Privacy worlds

Tor is an attempt to realise particular visions of society, the internet, and privacy in practice through material infrastructure. As an infrastructural project, Tor draws together different kinds of people engaged in different types of work which are embodied in different kinds of relationship with technology. In the remainder of this chapter, I use the social worlds framework to map the complex landscape of privacy values in the Tor community. Privacy and security are at the heart of Tor's work, and form the core values of Tor. However, within the broad concept of privacy lies a heterogeneous terrain of different concepts and elements. This includes the category systems of use cases and users for whom Tor provides privacy, the adversaries against which Tor attempts to provide privacy, how privacy is understood as a feature of technical systems, the relationship between privacy and anonymity, and how privacy, security and resilience interact and balance against one another. Additionally, a further component of how privacy is constructed concerns its implication in power and politics: namely, how privacy technologies become sites of social action, and the kinds of social action in which they are implicated. In Tor, there

is a deep tension between different understandings of the links between privacy, politics, technology, and power.

Through empirical research, clustering strands of discourse from my interviews into self-consistent ways of framing Tor, I have identified three main social worlds of understanding which are rooted in different kinds of work. I describe the process of arriving at these social worlds in more depth in Chapter 5. The first of these is the *engineer* social world, which stems from the design and development work on Tor and understands privacy technology as rewriting structures of power in technical networks. The second is the *activist* social world, which is linked to the campaigning, lobbying and advocacy work of the Tor Project, and sees privacy technology as engaged in political work, and part of a social movement in its own right. The final social world is that of the *infrastructuralist*, arising from the maintenance and administration work done by the Tor community, which is deeply agnostic about the political character of privacy technology, preferring a "neutralised" ethos of service provision.

These constitute ways of understanding the work of Tor, 'universes of discourse' imbued with their own culture, practices and politics, which different actors draw on when working on the project. While these worlds appear to map neatly onto particular groups in the Tor community, in fact, as I discuss during this chapter, individuals often draw on more than one of these social worlds in making sense of the politics of privacy technology, especially when they are involved in multiple kinds of work. Thus, a particular relay operator might occasionally draw on the *engineer* or an *activist* perspective when talking about how Tor relates to other organisations, for example, but primarily identify as an *infrastructuralist* where these worlds directly come into conflict. In this section, I characterise each of these social worlds, and how they articulate different understandings of Tor's relationship to power and politics. For each world, I set out some background about how they fit into the work of Tor and detail the main kinds of work in which they are engaged. I then discuss the main discourses which together constitute the way the social world makes sense of Tor as

a site of social action, then briefly outline the points off passage through which this world exerts its influence on the material forms of Tor.

## Engineers: privacy as a structure

When Tor was first created, most of its community was composed of the people involved in designing and developing its software and encryption protocols. Tor's technological design and the rationalities which underpin it are shaped by this development work and the social world to which it gives rise. Tor now has a small core team of full-time development staff who work on the project, supported by a larger Open-Source community of volunteer developers. Their work is undoubtedly the highest-profile work involved in the Tor community and is characterised by a social world which I describe as the *engineer* perspective. In addition to this, many other projects – in particular Onion Services, which use the Tor network to provide anonymous and uncensorable web services – contribute to the broader Tor ecosystem (Tor Project 2019). Their developers, and the large community of academics who develop privacy technologies, also contribute to the engineer perspective on Tor. This perspective is the foundational social world of the Tor community:

> Uh, I think people working on Tor then were technical people. Um, so either they had computing science degrees, or, or something approximating that. The, the more inter-disciplinary aspects came later. Um… uh, like, OK, there's probably a few exceptions, so, [an early founder of Tor is] a philosopher and a mathematician, but I think he, he does computer science research, um, so I think people either doing computer science or doing computer science research at the time.
>
> Participant F - Tor core developer

Tor's engineering work bears some similarities with hacking, involving deep technical knowledge, creativity and expertise. However rather than subverting or repurposing technologies which already exist, Tor's engineers are engaged in the creation of something new: a massive, stable infrastructure which needs to be reliable and maintainable. This entails planning and software development processes, and

balancing between privacy, usability, resilience and security in design (Dingledine 2004). I describe this development work and the practices of Tor's developers in considerably more depth in Chapter 7.

Although the Tor engineers are engaged in the same debates about privacy and internet freedom (and often on the same side) as many hackers, their understanding is framed by a different set of practices, logics and goals. The engineer social world is shaped by a deep, systematic technical understanding of internet infrastructure, combined with a practical engagement with its systems through design processes. Through this work, the Tor engineers construct politics and power as enacted through the structural forms which communications systems take, mapping the 'choke points' which the topology of the internet creates and how this gives power to the particular actors who control them. This perspective frames the politics of technology, privacy and anonymity in *topological* terms:

> But the act of [running a Tor node], just like the act of creating an internet service provider where there wasn't one before, is a political act, right? It changes the landscape, and the relationship between people, and what people can do, and can't do, you know, so it's, I mean, yes, it is [political]… People who say that the choice to do this is not political are deluding themselves.
>
> Participant U - Tor relay operator

Musiani (2013) argues that perspectives like these represent part of an 'architectural' turn in internet governance discourse. In the engineer world, privacy is a quality of the structures of technosystems whose designs produce different types of privacy and topologies of power. What is distinctive about the engineer perspective is that it does not make value judgements about *who* has this power, rather it critiques the accumulation of this structural power itself:

> I see the work that I do as decentralising and distributing power. Because I think that's always a good thing. *laughs* I see that as a fundamental… like, if nothing else is true in the world, distributing power in this world is a good thing. And, so… when you're threat modelling, it's a case of, how do we take this cluster of power here… and how do we remove that from the equation?
>
> Participant Z - Onion Service developer

This perspective confines explicit value discussions to the initial goals of the project, whose consequences are worked out through engineering practices which are perceived as largely value-neutral. This is not a disavowal of the politics of technology, rather, it is an understanding of power and politics as arising from structural forms in networks. Privacy is understood through topologies of informational power, in which making the internet more private is seen as a process of redistributing power, inherently helping the weak more than the strong. Thus, Tor is seen by the engineer perspective as changing the terrain of power online through a technical 'fix' to the structures of these networks, reframing political questions about the technology in ways which can be tackled through design and development processes.

> I think privacy does level the board a bit. So, I think privacy helps weaker people, it helps people who want to enact change. Powerful people do not need privacy to the same extent, because they have other means of defending themselves against bad things happening. So, I think it is also a technology that tries to help equality.
>
> Participant F - Tor developer

The *points of passage* through which this perspective shapes Tor are its design and development processes, and hence the material and functional qualities of the Tor network. This obviously constitutes substantial power to shape what Tor is and how it works. Access to this power is, naturally, limited by the technical expertise required to understand and make informed contributions to these debates, and this can prove difficult even for members of the developer community. Tor relies on a range of different design elements, including the cutting-edge encryption protocols on which it is based, the design of the browser and the way traffic is routed around the network, and the design work which goes into shaping its user experience, among many others. Each of these in their own right requires substantial technical expertise, and as a result, the range of people whose values shape the material design of Tor is restricted by this high barrier to entry.

As I describe in Chapter 8, this is mitigated somewhat by Tor's philosophy of radical openness. Even the less technical members of the community are generally fairly

trusting of the decisions made by the Tor developers, as the Tor Project makes its source code and design freely available and open to scrutiny by independent researchers. Tor's engineers, however, are beginning to go beyond a passive model of openness, in which they simply lay themselves bare to the technical and academic elite who have the knowledge to engage in these discussions. They are now beginning to take a more active role in involving their community and users, even those with less technical ability, in these design processes. This is often led by funding, with sponsors from particular regions of the world or representing particular user communities donating money in order to make Tor more usable for particular groups or use cases. Underneath all this, however, the inherently 'structural' or 'topological' framing of social life remains at the heart of how the engineer social world makes sense of privacy.

## Infrastructuralists: privacy as a service

Design and engineering, however, is not the only work involved in Tor. As a globally-distributed infrastructure with millions of daily users, Tor relies on a substantial quantity of 'invisible work' (Star 1999). The *infrastructuralist* perspective which typifies this labour is drawn on by a wide array of relay operators and volunteer maintainers who provide this work, concerned with the maintenance and upkeep of the network rather than design and engineering. Rather than a practice of 'hacking', based around breaking, subversion and creativity, these technologists are involved in maintaining and administering an infrastructural project, which needs to be stable and robust. The relay operators are the largest group of these 'invisible labourers' and this section focuses on them. This perspective dates largely to the original release of the Tor network in 2002, though many of the sentiments, practices, and sensibilities draw from the administrators of the other anonymity networks which grew up alongside, and sometimes predated, Tor.

The Tor relay operators, who administer the servers or "nodes" which form the backbone of the Tor infrastructure, are largely volunteers. Once a node had been set up, very little effort or attention is required to keep it running, apart from occasional checks and (depending on jurisdiction) dealing with complaints from ISPs and law enforcement. These complaints can be mitigated through careful selection of a sympathetic ISP, with wikis and mailing list discussions available to document favoured providers and ones to avoid. There was considerable variation among my participants in terms of how they set up and managed their node, with one operator running a node from their home computer, one running a few exit nodes on their secondary computers and one running a bank of several Raspberry Pis, each hosting a Tor node. Most of the relay operators I interviewed had at least some background in IT, whether as a programmer, a systems administrator or a security consultant. When asked how well they understood how Tor worked, they took care to make the distinction between their knowledge of network administration (the functioning of the infrastructure, their own machines and connections between nodes), which was generally good, and the inner workings of the Tor code, which was of less interest to them. This was generally seen as the job of the core project developers and open source contributors, even by the operators with more technical knowledge:

> I do not follow the development. I think they know what they are doing and I am not a coder.
>
> Participant P - Tor relay operator

Legal knowledge, in particular the legal situation in the host's country with respect to running a Tor node, was felt to be of more use to a relay operator, especially to those starting out.

> Get in touch with the laws of your country. Read, read, read. Understand, understand, understand. And… try to have the Tor network growing… Depends on your intention – if you, if you don't have any technical background and you just want to help the Tor network, it's very important to know the laws of your country.
>
> Participant Q - Tor relay operator

While they enjoyed running relays or contributing code, they often reaffirmed the importance and the seriousness of the work they did, describing it as a 'service'. As setting up a node was fairly straightforward, one of my participants was keen to make the distinction between their approach and that of more hobbyist contributors:

> I think for someone who's doing it in the spare time or hobby, it is more like "ohh, this is spooky, this sounds nerdy, let's give it a try!" and for me as a technician, it's like, OK, I have the possibility to provide services to people which have restricted internet. I think for, uh, the free-time IT nerds it's some play stuff and if you're kind of a professional, it's like, bringing out a service. That's my opinion.
>
> Participant Q - Tor relay operator

Despite sharing practices through wikis, mailing lists and IRC discussions, the relay operator community has been rather atomised for much of Tor's history, and appears more as a collective of individuals rather than a coherent group. Whatever 'community' of relay operators exists is a fairly loose-knit network composed of individuals with their own motivations, political opinions and levels of technical engagement. None of the respondents felt that there was a strong Tor node operator community. The majority of node operators viewed their work as a hobby, a mix of charitable work, public service and a leisure time pursuit such as gardening, a practice of cultivation and contribution.

Despite the lack of a tight-knit relay operator community, many of my participants did feel that the volunteer operators running the Tor relay network had a shared perspective which extended past the operation of the Tor network and to a more general set of beliefs about security, privacy and resistance to state surveillance. The infrastructuralist social world is characterised by rather different discourses from that of the engineers, and the practices of relay operation give rise to a distinct framing of Tor as a site of social action. Part of Tor's strength is that anyone with the capacity to set up a server can contribute, no matter their motivations. This allows for collective action without the need for shared political allegiances, and a large, broad-church community of contributors.

> I think [Tor works] probably because it's easy to work together. We don't actually have to work together! The Tor Project has made it so simple to start a relay and just run it, and not actually interact with anyone... they've made it so easy to, to act like a big community when actually, we're not really, I think we might be a bunch of individuals…We don't have to co-operate with each other, apart from running the same software.
>
> Participant R – Relay operator

The social world which arises from this is deeply agnostic to Tor's relationship to power, and anxious to 'neutralise' the politics of their work as much as possible. Coleman describes a similar sensibility in the Free and Open Source Software community, which she terms "political agnosticism" (Coleman, 2004). Coleman describes this as an expression of the interaction between the liberal values and technical practices of 'hacker' culture: "what grows out of this particular life world of intense, lifelong programming and networked sociality is an overt aesthetic dislike for politics and a culturally embodied experience of freedom that conceptually shuns politics."(Coleman, 2004, p512).

Within this agnostic view of Tor's politics lies a common commitment to deeply political values: the vision of a privacy-focused internet where the flow of information, capital and communication proceeds without surveillance or censorship. The infrastructuralist world expresses these 'hacker ethic' values through forms of practice more rooted in infrastructural labour than hacking, framed around an ethic of service provision rather than creative breaking. This frames Tor's relationship to power and politics through a 'neutralised' variant of technoliberalism.

> I think most of us believe that we want to provide the tools so others can exercise their powers and their influences. People that understand society better, maybe. And we are just the infrastructure providers. Right? I think that's a notion that a lot of hackers have, is that ultimately they don't want the political influence, they just want to provide the infrastructure. For democratisation.
>
> Participant L – Tor core contributor

This is distinct from the *engineer* perspective. Where the engineers see Tor as a political attempt to redraw the maps of informational power online, infrastructuralists are more agnostic about Tor's relationship to power,

understanding privacy as a service they provide to users, who engage in political action themselves. Getting involved in normative conversations about how the network is used becomes a dangerous game, and so this perspective strongly resists any attempts on the part of the organisation to decry or promote particular use cases, legal or illegal, or to claim that Tor itself represents any specific set of values outside a neutral service for protecting data in transit. By constructing themselves as apolitical actors, they shift the moral character of the network onto the users, allowing them to contribute without feeling responsible for the traffic which their relay serves.

The key point of passage through which the infrastructuralist perspective shapes Tor is the infrastructure of Tor itself: the relay network. Although the operators are not involved in the code, and hidden voice, they are crucial to the success of Tor, and together shape a lot of how the network is run. While they by and large do not consider themselves a community in the sense that the Tor activists and core team appear to, they wield considerable consensus power as the infrastructural backbone of the project. However, the dispersed, atomised nature of the relay operator community means that unless the Tor developers violate the fundamental guarantees of privacy and security on which the organisation is founded, in practice this group is too diffuse and heterogeneous to wield any real power to shape the direction of the organisation and its public life. Nevertheless, the Tor Project still need to keep them on side in order to maintain a robust and growing relay network.

## Activists: privacy as a struggle

Many of Tor's intended use cases involve explicit interventions in political struggles, either in the broader social movement for internet privacy or as a tool used by activists for secure communication. While this perspective, or elements thereof, has long been a part of the Tor community, it only really rose to prominence after the revelations made by Edward Snowden, which inspired a generation of activists to

nucleate around Tor, in some cases becoming deeply involved in its community. Due to the increasing maturity and professionalisation of the Tor Project organisation, there has equally been an increasing demand for HR workers, policy professionals, and fundraisers, who tend to come from other NGO and civil society groups and hence also contribute to this perspective on Tor.

> Um, as Tor grew, um, firstly, there's just people who are needed for administrative-type roles, so, just, running a project, um, getting in funders. Um, then there, there's also the recognition that there's interdisciplinary aspects of it, so you need someone who actually understands how people use the internet in order to do things better.
>
> Participant F - Core Tor developer

As a result, Tor's community includes a wide range of people who engage with civil society, activist movements and policymaking: these people develop an *activist* perspective. There is a substantial body of research on internet freedom activists, and so this section has been left brief other than a few remarks on the specific contours of Tor's activist world (Marechal 2015).

The activist social world understands Tor as part of a social movement. They see privacy technology as a site of activism, and contributing to Tor as an explicitly political act. Thus, from this perspective, privacy is often couched in the language of fundamental human rights or constitutional protections:

> I personally feel that, that Tor is political, because it enables individuals to have access to somewhat different internet, in the sense that it enables individuals to circumvent internet censorship. Circumventing internet censorship in itself is a political act of resistance. It enables individuals to, uh, circumvent, um online tracking, which is capitalist surveillance – that in itself is a form of resistance. It enables individuals to be anonymous – that is a human right, and so I feel that because of the nature of the software, in my personal opinion, is political.
>
> Participant K – Tor core contributor

This world can increasingly be seen in the public life of Tor, through strong value statements about what Tor 'stands for' and explicit articulations of Tor as embedded a specific set of values. They understand Tor as part of a long history of struggles for social justice and fight for Tor to move away from a 'neutral' understanding of

privacy in favour of one which recognises that ideas of privacy are inherently political and change for different people and in different contexts:

> The fact that many LGBTQ+ people need a private, anonymous internet to communicate with their peers or find important resources without being tracked and outed is one of the many reasons why we do what we do at the Tor Project…
>
> We are proud that our tools can serve the LGBTQ+ community. We hope that by offering a way to privately access the internet, allowing people to get online without fear, that we can communicate with one another to change the world. We all deserve to live in a world where we can express who we are without shame.
>
> Tor Project Blog, 2019

These discourses, drawn from the practices and experiences of privacy activism and working with journalists and activists around the world, frame Tor's work as explicitly political. While they are anxious that Tor not abuse its influence, they are generally happy for Tor to engage in political debates which touch directly on its work, for example, to condemn far-right users as they did following the far-right marches in Charlottesville which resulted in the death of one counter-protester, and some far-right websites proposing moving to Tor.

> We've heard that the hate-spewing website Daily Stormer has moved to a Tor onion service. We are disgusted, angered and appalled by everything these racists stand for and do… Tor stands against racism and bigotry wherever and whenever such hatred rears its ugly head. It is our work to provide everyone with the best possible security and privacy tools so human dignity and freedom can be promoted all over the world.
>
> Tor Project Blog 2017

Ultimately, the activist social world sees privacy technology as the focus of a sustained battle between authoritarian forces and surveillance capitalists on one hand, and privacy activists on the other. They see it as connected intrinsically to other such struggles and movements – whether those movements be women's liberation, LGBTQ rights, or harm reduction movements for criminalised practices such as drug-taking or sex work. While this framework is drawn on by the policy workers and activists in the Tor community, many developers and relay operators are also involved in campaigning and advocacy, drawing on the activist perspective in

understanding the broader meaning of their work. The points of passage where the activist world wields its influence are those associated with Tor's public image, which this world has a substantial capacity shape through blog posts, press releases, public talks, advertising and fundraising campaigns, and lobbying. These are important aspects of Tor, shaping as they do how it is understood in public life, and hence who uses it and how.

## Relational perspectives

The above social worlds constitute three different instantiations of liberal technopolitics, refracted through three different kinds of labour. Much like the labour practices on which they rest, these social worlds do not exist in isolation. They are *relational*, defining themselves in key ways in opposition to one another. For example, the willingness of activists to link Tor to explicit political causes can clash with the infrastructuralist perspective, and provides a foil against which they can contrast their own "neutrality". Where those who interact less with the Tor community draw heavily on an infrastructuralist perspective, they can even be sceptical that the other worlds of discourse really exist:

> I think it's neutral… I think the people behind the Tor Project, are they free of values? I'm not sure if it was marketing they put on the front page… of course every privacy project in the Internet has to put some big strong words on their front page… But I think most of the people which are connected to the Tor Project, I think they are seeing it more… as a tool. A tool for people doing whatever they want.
>
> Participant Q - Tor relay operator

While the engineers have less hostility to explicitly activist or political work, they see it as frustrating, an arena in which they are ill-equipped and unempowered and which they prefer to circumvent.

> I'm quite averse to getting involved in policy issues. And I don't know if that's something that technical people tend to share? That they look at it and they go, oh, I don't really want to touch that, I don't like making rules and things. Especially when I know someone's going to go through them and mess them all up after I've written…

> And then you have to have huge arguments with people and go, no, you really don't understand this issue… I'd rather just implement a technical fix that prevents their law from being effective.
>
> Participant D - Tor core developer

> I'm not claiming I'm unaware of anything going on geopolitically, but I guess addressing that sort of thing is just outside my bailiwick… I mean, we're certainly aware of how evolution of technology is going on in the broader world, but the specific sorts of, as you said, the Cryptowars, and other things, I don't think they directly played a role, at least for me. Whether they were important motivation for other people… perhaps, but I don't think it significantly changed what we were trying to do. Because I think that it made sense whether those things were happening or not.
>
> Participant I – Tor core developer

These social worlds represent 'ideal types', a typology which aims to differentiate and accentuate the characteristic qualities of each of these worlds, stressing commonalities within particular categories without claiming exactly to correspond with the views of any particular person or group of people (Aronovitch 2012) While the perspectives of individual people in the Tor community tend to be aligned with one of these worlds based on their role in Tor, they often draw from others, bridging between different worlds. Identities and roles in Tor are hence often multiple or ambiguous:

> I think I avoid having an identity too much. Not in terms of anonymity, but in terms of a self-image of what I am. Because I feel like that's limiting somehow.
>
> Participant C - Tor core developer

While some members of the community may only be involved in engineering, policy, or infrastructural work, many of the core team are involved in all of these to some extent. Some of the engineers also carry out a variety of maintenance work, such as bugfixes, patching and monitoring the network, and outreach or policy work. This means that many of the core developers, while primarily viewing Tor through the *engineer* lens, draw on framings from the *activist* or *infrastructural* perspectives when talking in more abstract terms about the place of Tor in the world. Similarly, there are some relay operators who see the work they do as part of their political

activism (and many of the developers and activists also contribute to the relay network), or as restructuring power relations online.

Within individual interviews, participants would often tack between different ways of making sense of Tor, drawing from different social worlds in different contexts. For example, in the following pair of responses, when discussing their broader motivations for being part of the community the participant describes Tor from an activist perspective as part of a political movement for privacy as a human right, then, when discussing the practices of operating a relay and the traffic which flows through it, describes Tor from the infrastructural perspective as a neutral tool whose politics stem entirely from its users.

> If you can see in Europe in United States, in Asia, in Russia, in Africa, there are a lot of crimes actually, against free speech, against human rights, about anonymity, you know United Nations has enlisted online anonymity as a basic human right more than a year ago… [Tor is] very important because the, yes, people have the right to think freely, to speak free, to speak from their hearts, not from fear of governments that will punish them for not being, you know, not being agreed with the official positions, for example.
>
> Participant N – Tor open source contributor
>
> Because the tool is something that helps you to do something. But uh, you know, what you will do, with this tool, is up to you. Crime happens not on the hard drive of the Bond movie producer, crime happens not on the Silk Road drug store, no. Crime happens inside people's mind… Neither Tor or other software authors, nor people who are running even exit nodes, no they're not responsible. They are not responsible for another people's thoughts and actions. They are not. Tor is just a tool.
>
> Participant N – Tor open source contributor

As Unruh (1980) describes, it is this multiplicity of membership in social worlds which forms the "glue" that binds them together. Part of Tor's success has been precisely due to the productive tension between these three perspectives (which have grown and developed alongside the infrastructure at different points), and due to the fact that many of the core team can translate between these social worlds.

# Collaboration, conflict and transformation

## Privacy as a boundary object

Despite this heterogeneity, Tor has been remarkably successful at fostering collaboration within its diverse community. In this section, I explore how these worlds coexist, and how individuals are able to bridge between them. Although they differ in their understandings of the politics of privacy technologies, these social worlds share important sites of agreement. This gives these social worlds a shared link between the diverse kinds of work they do and the animating values and goals of the project.

When asking participants about the most important use cases of Tor, they conceptualised these as falling within two distinct categories which took a common form across all three social worlds. The first of these, which I characterise here as *everyday privacy*, are everyday users of the internet. This is linked to the idea of privacy as a foundational democratic value, underpinning the rights of freedom of speech and association, and a cornerstone of free societies.

> The whole reason that Tor Browser existed is because there was a belief that privacy should be for everyone, it shouldn't just be for techie people who are able to pull together all these obscure components.
>
> Participant F – Tor core developer

This type of privacy affects the quotidian rhythms of users' daily lives. This constructs privacy through the aggregated, patterned interactions of whole populations and the personal details which can be learned about them through studying this. Many of the participants linked this to protecting democratic values, the right to free speech, and halting what they saw as a dangerous trend towards authoritarian surveillance of people's private lives.

This is contrasted with the use of Tor to protect people in cases where detection might mean imprisonment, death or other serious consequences. These high-risk users, which include political dissidents, freedom fighters, CIA field agents,

journalists, and human rights activists, tended to be much rarer activities which incurred substantial interest from powerful actors and hence needed protection through rigorous security practices. This is a vision of privacy which is more directly oppositional, allowing those in authoritarian nations (or whistleblowers and journalists in Western democracies) to speak truth to power, resist control, or create spaces where they can organise against state-backed oppression.

> [journalists] are getting people to speak to them in a truly free way that they would not in almost any other context. You know, there's no… parking garage where you can go to speak to, you know, Woodward and Bernstein any more, that's over. [Tor Onion Services] is that parking garage.
>
> Participant X - Onion Service developer

Some community members prioritise high risk use cases, while others place more emphasis on everyday privacy. For example, some of my participants were keen to emphasise Tor's use by everyday Internet users in Western democracies, while others argued that their participation in the Tor network was motivated by a desire to protect human rights defenders in authoritarian nations, rather than privacy-conscious citizens in more open societies. While individuals differ in *which* of these they see as important, they share the same system of classification: that Tor's construction of privacy encapsulates these two distinct forms.

> I think you couldn't have Tor when you didn't have all of those things. Anonymity loves company, and you couldn't have the Chinese dissident anonymity system, or the US military open intelligence gathering system, it doesn't make sense. So, I think, if there's one thing that's the most important, it would be that all of these things can interact on the same system. I'm sure everyone will have their own preferences… I'm happier that people who are trying to promote human rights are able to have their job facilitated through Tor. That's probably what I personally think, but I recognise that it would be useless to have just that sort of group.
>
> Participant F – Tor core developer

This category system arises from the design of Tor itself. Tor's predecessor, the Onion Routing project, was initially created through the coming-together of two distinct social worlds. As I describe in Chapter 2, this involved a chance collaboration between US Naval researchers and "cypherpunk" technologists wanting to shape the internet as a privacy-preserving social space. Somewhat to their own surprise, these

two groups had more aligned perspectives than they might otherwise have imagined:

> I'm very happy to see the NRL doing this research. I have no doubt that you guys have what it takes to pull this project off. I'm also happy to see that your goal is to resist serious traffic analysis (as opposed to hiding browsing patterns from your little sister). We cypherpunks have been thinking about these problems for quite some time, as they are central to our agenda, but too often we sit around and talk about them rather than actually building things.
>
> Cypherpunk, Or-dev mailing list 1997
>
> We are researchers. That is our job description. That is what we get paid to do. There are more PhD's walking around this base than some college campuses. We publish constantly in academic circles, we attend conferences, we participate in the larger academic world. Please do not assume that since we work for the government that we are uninformed, undereducated, GAK-loving idiots. What we lack is the practical experience in this area – most of what we do is theory, theory, theory...very little applied (at least in the computer security area). Thus the prototype where we've already learned a great deal about where the theoretical models break down in the real world… Please don't view this as an "us vs. them" environment...we want the same level (and possibly even higher level) of security that you want out of this system... help us do that.
>
> US Naval researcher, Or-dev mailing list 1997

The initial development of Tor constitutes an alignment between these 'military-academic' and 'cypherpunk-engineer' worlds. In practice, the Onion Routing design represents a technological solution which brings these two strange bedfellows into a mutually beneficial relationship. The final top-level design of Onion Routing reflects a coming-together of both of these worlds, as it involves large numbers of everyday users acting as 'cover traffic' for higher-security use cases, thus satisfying the 'everyday privacy' requirements of the cypherpunks and the 'high-security' requirements of the US Naval research lab. In terms of the kind of social action they see privacy technologies as being engaged in, these two worlds also resonate: they both understand them, much as the 'engineer' social world does, as using technical fixes to reshape the topologies of power in information systems. For the cypherpunks, this removes pinch points in the infrastructure of the Internet which states can use to surveil their citizens, while in the case of the military, this

undermines non-US nations' ability to secure their communications networks against use by US military personnel.

> The old Cypherpunks and the US Navy are facing the same problem and are therefore looking at similar solutions. You need broad public use of the system to provide you with cover traffic and we want to see such a system deployed to provide the citizens with privacy. We are allies, not enemies.
>
> Cypherpunk, Or-dev mailing list 1997

The three social worlds of Tor draw their constructions of the user from the logics embedded in its technical design, which provide a common point of stabilisation between Tor's worlds. From the *engineer* perspective, this frames user categories through the patterns they trace in technical systems and envisions privacy in terms of the decentralisation of structures of power and control in the internet. The world of the *activist* understands *everyday privacy* as a civil rights movement in its own right and sees *high risk* use cases as important for activists and journalists involved in social justice struggles the world over. The *infrastructuralist* perspective resonates with the content-agnostic nature of this user classification, which classifies users according to security criteria and the patterns of their use rather than their politics or allegiances.

> That is a political question, and to date, we have tried to only deal with the technological issues instead of the political ones. As soon as we start dealing with political issues, this thing will fall apart.
>
> Developer, Or-dev mailing list, 1997

In this way, privacy acts as a boundary object (Star 1989), with a shared construction of privacy in the end user providing a common element which allows individuals to bridge between otherwise irreconcilable social worlds. This has historically allowed Tor a productive ambiguity around the political dimension of privacy, leaving different parts of its community the freedom to conceptualise the links between privacy technologies and power differently. Until recently this détente has proven remarkably resilient, helping Tor has to navigate these conflicts and draw on the interpretive power of these different social worlds.

## Cultural change and boundary breakdown

Boundary objects, however, are not immutable (Star 1989). Tor's productive ambiguity has proven durable for much of its life, however a series of internal crises and cultural changes have in recent years made this untenable. As it has had to be clearer about its core values and what it stands for, so too has the cultural landscape of the Tor community changed. In this section, I explore the nature of this challenge and how Tor has navigated it, how a social worlds perspective helps us to understand the deeper implications of this, and the resulting transformations in Tor's social worlds.

Following the Snowden revelations, the Tor community saw a massive influx of new members, galvanised by the social backlash against mass surveillance by the US, and a more *activist* perspective on Tor. At the same time, a shift in the broader culture of the tech industry was underway, bringing a more critical and politically engaged sensibility to prominence, and calling out a history of misogyny and abuse in these communities. This was accompanied by an increasingly critical trend in public discourses about online platforms, focused on the power and politics of the people behind these technologies. For Tor, this came to a head in June 2016, when several members of the Tor community accused Jacob Appelbaum, a member of the core team and one of Tor's most prominent representatives, of engaging in a pattern of abusive behaviour and sexual assault (Loll, 2016).

This resulted in Appelbaum being fired from the project, the replacement of the project board and the installation of Shari Steele as director. Steele led a programme of professionalization, remaking Tor into a modern NGO with more developed organisational practices and structure and a well-defined set of core values (Marechal - forthcoming). This has met with praise from some sections of the community, and considerable opposition from others, and has shaken the détente between the social worlds of Tor.

A social worlds perspective allows us to understand this crisis as not just a clash between groups within the Tor community, but as the rupture of a previously-stable equilibrium between different ways of understanding the project. From the *activist* perspective, Tor is inherently political, promoting values of liberation and democracy, so this change was a necessary part of Tor's growth as a modern activist organisation. Equally, despite their suspicion of policy work, the *engineers* seem to have welcomed this formalisation of Tor's values, especially against harassment. I contend that this is because of how this has been framed – as attempts to redistribute and decentralise power within the Tor Project.

> Tor has definitely become more open in the last year or so… And I still think they're going through this evolution of wondering where they fit in the world.... And they're getting better at addressing all these issues, they've done a lot of work in making sure that accusations of sexual assault and harassment are addressed, and, you know, opening up the power structures, and restructuring that.
>
> Participant Z – Onion Service developer

However, for some of those adopting a purist *infrastructuralist* perspective, these changes were less welcome. Asserting Tor as embodying feminist principles and attempting to transform Tor into a diverse, modern organisation with explicit values has, for some in the community, undone the political ambiguity which enabled them to feel aligned with its goals.

> This changed to, Tor is now about women's rights as well... They are probably right, with everything they say, so don't get me wrong. But Tor isn't specifically about empowering women and technology. I mean, they can do that, whatever. Take turns, do workshops, whatever. But that's not why I'm running a Tor relay. I'm running a Tor relay because there are people in Turkey and they're in jail for things they write, because people in Syria are getting killed if they are found reporting from certain areas. People in China just disappear if they are found using Tor, that's why I'm running Tor relays, Tor bridges. That's what I care about. Women's rights - fine, but, just, sorry, not my department! And saying that out loud makes people upset.
>
> Participant W – Tor relay operator

The assertion of political neutrality to rule feminist concerns out of scope for technical projects has historical precedent in hacker and OSS culture (Nafus 2012). In Tor's case, the firing of Appelbaum and the resulting organisational changes led to a

minority within the community leaving outright. The atomised nature of the relay operator community meant there were no real leaders to drive an exodus, and no strong sense of a shared social meaning (in fact, the infrastructuralist understanding of Tor itself precludes this). Many who understood Tor from this perspective were still able to see themselves in the infrastructural labour of the organisation, however where some felt unable to do so was in the public life of Tor, feeling that Tor's values now excluded their way of understanding it.

> And then with the Jake fallout and different conflicts… a bit of the dynamics changed… I mean Tor is trying to become a professional NGO. Tor Project Incorporated. And I think that's a change over the previous idea of being deeply rooted in a lot of different communities. When you want to become a professional NGO, you have to make decisions…Before, you can be very flexible, and in different situations with different people act very differently. And it's not necessarily that there were any mistakes, it's just the growth is now changing things. And also, of course, changing who… stays around and what their incentives and motivations are for still hanging around and doing this kind of work.
>
> Participant L – Tor core contributor

This is not merely the sidelining of one group in favour of another, rather it is representative of a fundamental transformation in how the Tor community understands the project on which they collaborate as the organisation has matured. Accordingly, the infrastructuralists' world has also begun to change, moving from an "atomised" model of relay operation to a collaborative one based around in-person operator meet-ups and a more engaged community with a shared sense of purpose.

> And then there's also this element of, we should all get to know each other, because we're kind of in this boat together. Uh, even if we disagree on a lot of things, like, there's clearly something that's binding us together, so we should at least meet and talk about it.
>
> Participant R - Relay operator

The engineer perspective is also transforming. Its topological understanding of power is increasingly turned on Tor itself, critiquing the developers' own "power to structure" in designing these systems. This is indicative of a broader trend in the internet freedom community, as through organisations like Tor, Tactical Tech and Open Privacy there is a concerted effort to extend this understanding of power in

network structures to specific, subjective, and local contexts rather than universalising abstractions. Open Privacy, for example, draws on Lewis' work in *Queer Privacy* where she critically unpacks the construction of "privacy", exploring how it might mean different things to marginalised communities (Lewis 2017).

The crisis in Tor around the firing of Appelbaum was a signal event, emblematic of changes which had been ongoing within the Tor community for some time. Part of this is due to Tor becoming more successful and maturing as an organisation, however it is also the result of the worlds of Tor shaping one another and changes in the broader context of information security work and Internet politics. Over the last few years, Tor has been undergoing a major shift in terms of what kind of organisation it is, and as a result, its social worlds have been changing too. As Star argues, this new détente may well require new or altered boundary objects, and different kinds of boundary work.

## Conclusions

In this chapter, I have mapped the social worlds of Tor and how they relate to one another, managing conflict, consensus, and change. Infrastructures require a range of different kinds of work to function, bringing together people, cultures and perspectives in complex ways. Tor is characterised by three main social worlds: the engineer world, rooted in Tor's development work, which understands 'privacy as a structure'; the activist world, rooted in the policy and lobbying work of Tor, which sees 'privacy as a struggle'; and the infrastructuralist world of Tor's relay operators, which sees 'privacy as a service' . It is important to emphasise that any given person in the Tor community likely draws on a range of discourses from these worlds in different situations in making sense of Tor, although some are clearly more firmly rooted in a particular world than others. Equally, as I describe in this chapter, these worlds are not static, but change and shape one another over time.

In navigating the boundaries between these worlds, Tor has for much of its life used the concept of privacy as a boundary object to unite the community around a shared sense of the meaning of their work. Through a common category system of the *users* in their construction of privacy, they were able to afford the place of privacy technology in relations politics and power a productive ambiguity. This enabled many of the core team to bridge and translate between these worlds and has been largely successful in allowing Tor to persist. As the context of Tor changed through the Snowden revelations, the increasing prominence of the activist perspective, and broader cultural changes in the information security community, the tension between these worlds began to come to the surface, erupting in the firing of Jacob Appelbaum and the professionalisation of Tor. The result of this has been the tentative formation of a new détente, reflecting changing understandings of politics, power and practices in each of these three worlds. How it navigates this will be deeply consequential for the kind of organisation Tor becomes and its role in struggles over privacy, politics and power online.

Tor's engineers constitute the foundation of the organisation, and although other worlds have grown up around Tor, theirs was the initial framing which shaped its development. The engineer world and the design practices to which it is connected are therefore of particular interest, and I focus on this in the following chapter – where this world came from, how it developed, and how it shaped the foundations of Tor's design and its vision of the world. Tor therefore constitutes an explicit, conscious attempt by its engineers to 'do politics through architecture', rather than simply a military tool or software project: to realise a particular vision of society through technical design. In the following chapter, I explore how they actually attempted to do this in practice through design and development work.

# chapter 7
# growing onions: Tor, values and design

## Introduction

Having mapped out the main social worlds of Tor and the different facets of its visions of a private Internet, I now explore how the discourses and ideas underpinning Tor's social life shape the technology itself. Of the three social worlds I characterise in Chapter 6, the engineer world is the one with the closest connection to Tor's design. Focusing on the design and development processes of Tor, I explore the relationship between the engineer social world and the material design of Tor, and hence how this vision of the world becomes embedded in the category systems, technical paradigms, and frameworks of representation which characterise Tor as a material artefact. Although Actor-Network Theory has been more commonly used in understanding how different visions of the world become embedded in material artefacts (Latour, 2005), I instead use the social worlds framework, which focuses on collaboration, multiplicity, and communication (Star and Clarke, 2008). In doing so, I draw both on my interviews and extensive archival research in the Tor Project's mailing list and design archives, mapping values, category systems and frameworks of representation and how they shape Tor's material form.

In this section, I first sketch out the kind of privacy envisioned by Tor's design, and the key values and constructions of privacy which underpin this. I then outline how Tor implements this design in practice, the privacy properties this confers on users, and the design decisions the Tor developers had to make. I highlight a particularly important decision: the decision not to include 'padding traffic' in Tor's design to

protect against adversaries with a global view of the Internet. In doing so, I also map the development of the engineer social world through a process of convergence, in which Tor's design and development practices at once create, through iterative, non-linear processes, both a coherent social world and a material design for Tor. Finally, I discuss how development practices in Tor and the social world of the Tor engineers have changed over time, and the consequences this bears for making sense of Tor's implication in power.

## Onion Routing: a technical design and a value system

Tor is based on the Onion Routing design, where users' Internet traffic is bounced around a network of volunteer-operated servers (known as 'relays') around the world in order to disguise its origin and destination. First, the administrative information which routes users' traffic around the Internet is wrapped in three layers of encryption. This traffic is then sent as a series of packets to the Tor relay network. The traffic is first sent to a Tor entry relay, a server which decrypts the first layer of encryption and reveals the address of the next relay in the chain. This next 'middle' relay decrypts the next layer of encryption, revealing the 'exit' relay's address. The exit relay then decrypts the last layer of encryption, finds the final destination of the traffic and sends it on. Thus, no part of the network knows both the origin and the destination of the traffic, and anyone observing a particular user only sees them connecting to Tor, not which websites they are accessing. This allows Tor users to get lost in a crowd of millions of other users (Syverson, 2009, Dingledine, Matthewson and Syverson, 2004).

Onion Routing is not just a technical specification; it represents a particular social construction of privacy. The Onion Routing design was originally developed in the mid-1990s in collaboration between US Naval researchers seeking to develop a secure communications system and a group of technologists from the cypherpunks subculture, who view strong privacy protections as central to realising the liberatory

potential of the Internet. The naval researchers wanted to develop a system which would protect high-risk military traffic, requiring as many everyday users as possible to act as 'cover traffic', while the cypherpunks wanted to provide strong privacy protections for everyday users. The Onion Routing design brings the values of these groups into a mutually beneficial relationship. By protecting the everyday online lives of the general public, Onion Routing constructs privacy as a human right and a public good for all, not just those with strong technical skills.

Tor's values are anchored in a technological vision of privacy underpinned by the properties of the Internet. This frames privacy as the product of engineering decisions in information systems, the administrative traces left in communication networks and the geographies of informational control in global IT infrastructures. It is deeply oppositional in character, with its goal being the greatest practical anonymity at the technical level, leaving the social negotiations of sharing personal information up to the user. As such, it aims to neutralise any architectural features of the Internet which compromise users' privacy. Onion Routing frames users as topological types. This means that its developers design around particular patterns of use and the information structures they leave in the network, rather than designing for particular user groups. I explore the importance of this framing and how it developed in detail in subsequent sections of this chapter. This allows people with fundamentally opposing views to use the system while only sharing a concern for privacy (Dingledine 2006). Thus, people using Tor to access far-right websites, those using it to access LGBT advocacy charities, and law enforcement using it to collect intelligence all contribute to one another's protection.

> Well, you know, the technology's cool, and it's nice to make something that's actually going to be useful and help people, but one of the really nice things about it is that you… you build something which by its very nature takes people who think they ought not to trust each other and work together at all, and forces them to collaborate in order to get the results that you want. And I just like the idea that you are forcing people who thought that they should never work with these other people to do so.
>
> Participant I – Tor core developer

This creates a collective of individuals who act together without a single shared worldview or centralised control, strongly shaped by a techno-libertarian, US-grounded view of privacy based around individual choice, agency and freedom. It is both deeply individualist, framing users as singular owners of their data, and paradoxically communitarian, with privacy reliant on the protection of a 'crowd' of these atomised users who underwrite one another's protection as a swarm of connected individuals. Fundamentally, it constructs privacy through the idea of topologies of informational power, mediated by the structures and design of the Internet.

## Implementing Onion Routing - Tor's construction of privacy

The privacy which Tor provides is the product of the design decisions made by its developers. In implementing Tor's design in practice, its developers could not make it impervious to all possible adversaries and usable for all use cases. These practical considerations make the development of an anonymity system different to more theoretical cryptographic research:

> The problem with anonymity is that we can build such threat models, stronger than any adversary, but then we don't know how to build a system that actually works, or, at least, is usable in that case. So, the threat models in cryptography are quite different from the threat models in anonymity, not just in what they are, but also in how they're developed. So, we would like to be in the situation where we can come up with a threat model that covers everyone, but I think, in anonymity, there's a trade-off between threat models, and then other design requirements. So, if we started off with a strong threat model, then that will naturally lead to design choices that will bring us to high-latency, and then we get something that drops usability. So, I think, what probably more happens is that there is some estimate of what attackers can do, the design consequences are worked out, and then there's iteration. In order to work out what is actually useful to people, that feeds into that process, you're right, it's hard.
>
> Participant F – core Tor developer

Tor's privacy properties are shaped by three key design decisions. First, its network is structurally decentralised: the core team which design Tor have minimal control over

its volunteer-run infrastructure, and it has no centralised mechanism for censoring user traffic. This is vital for a tool designed to subvert censorship and surveillance, but makes it harder to mitigate any harms arising from its use by malicious actors. Secondly, it is low latency: fast enough to use for everyday Internet browsing (Dingledine 2006). This widens its potential for social good, and for harm. Finally, it sacrifices some protections against a class of very powerful attacks in the interest of maximising usability and speed. These 'timing attacks' are theoretically available to powerful enemies who are able to collect and process vast amounts of the world's Internet traffic: by doing this, they can time the signals travelling around the Tor network and trace them back to their origins. This means that extremely powerful enemies, such as the signals intelligence services of the Five Eyes nations, may be able to deanonymize some users of Tor (Dingledine 2006).

Tor did not begin the design process with these properties; they are a particular practical implementation of the Onion Routing framework developed over a period of months through careful experimentation and discussion. Although they began with the Onion Routing design, implementing this necessitated making difficult decisions about which users and use cases Tor should support, and against which adversaries they should attempt to protect these users. The remainder of this section maps the background to these decisions, and the different categories of adversary and user around which they attempted to design.

When Tor was being built, the developers had very little knowledge about state surveillance capabilities, and, given the fast-changing nature of surveillance in the wake of the 9/11 attacks, they needed to build a system which was capable not only of subverting current practices, but those which might arise in the future. Today, the information security community knows far more about the practices of nation state security services, often thanks to the dedicated efforts of researchers, leakers and whistleblowers:

> That's one of the very challenging aspects to a project like this, same with Tor, is that… you know, to quote a questionable strategist, there are 'known knowns', you know, *laughs* we can read news articles, uh, we can look at the Vault 7 release and

> get an idea of what's currently in practice. We can talk to former whistleblowers and get their feedback, people that have been on the inside and understand how these systems work.
>
> Participant X - Onion Service developer

By contrast, the developers began their initial design work on Tor with very little information about adversary capabilities. As such, Tor's category system of adversaries is not based around specific real-world actors, such as the Chinese or Russian governments. Adversaries are instead conceptualised as a set of abstract categories based on how much of the network they can observe, and the power they can exert in different places. These categories include the global passive adversary (an adversary which can passively monitor traffic between all users and servers), the global active adversary (an adversary which can actively interfere with or otherwise modulate traffic between all users and servers), and the roving adversary (an adversary which has a subset of nodes which it controls which changes over time). Global adversaries are particularly problematic for Tor. These adversaries, with a view of the whole Internet, are able to observe the timings of the 'cells' of information sent around the Tor network, then use these to trace traffic around the network and deanonymize users through 'timing attacks'. In the original Onion Routing design discussions, this attack is thwarted by using 'padding traffic' to complicate this traffic analysis (Dingledine 2006). However, these defences often slow down the system, and hence reduce Tor's usability and suitability for everyday Internet browsing.

The Onion Routing framework distinguishes between two kinds of users. This stems from Onion Routing's technical design, which relies on attracting a large set of everyday users to provide 'cover traffic' for high risk users for whom deanonymisation has more severe consequences. In the original design discussions for Tor, the developers often draw on examples to illustrate different kinds of users:

> "Somebody is watching cnn.com, say some guy in China."

> “A road warrior who is logging into his home enclave with OR on the OR firewall. Nobody is likely to be watching his connection to the network because they don't expect him there.”
>
> “Someone is gather[ing] intelligence on some web site owned by the adversary.”
>
> “Alice has a hotmail account 'foo at hotmail.com', which she logs into periodically via the onion routing network.”
>
> “A group of CIA agents are deployed around the world, and check back with the cia.gov site periodically.”
>
> “Amnesty International allows anonymous story submission. Reporters risk their lives going to rural Asian countries, and surface every so often to submit a story, to pass back lists of contacts, etc.”
>
> “Dedicated political dissidents in the United States check an online bulletin board for a list of upcoming peaceful protests and recent news. When actually participating in the protests, they use masks to maintain anonymity while exercising their rights.”
>
> “Anne logs in every day and checks these 4 news sites; it would make Anne unhappy to not be able to use our system for that”
>
> Selected quotes from developers, tor-dev mailing list, 2002

Whether the user is a CIA agent, an Iranian journalist or a privacy-conscious member of the public, these use case categories constitute either everyday privacy, with sensitive information inferred through observing the patterns of everyday life, or high-risk, where detection relates to the observation of a small number of particularly recognisable traces. In order to protect the security of the high-risk users, Tor needs to be usable and fast enough to attract a large number of everyday users: usability is not just desirable, but in fact one of its core security properties (Dingledine, Matthewson, and Syverson, 2004). The diversity of users and the innocuous nature of much of the traffic means that use of the system itself is not incriminating. Thus, Tor takes the tension between developing a high security anonymity tool and a mass-use privacy infrastructure and makes these apparently-contrasting aims mutually supportive.

## Exploring the development process in Tor

Balancing between protecting against global, nation-state surveillance and maintaining the greatest usability possible is crucial to Tor's design. In working out how to implement their privacy values in practice, the developers needed to make a number of decisions about Tor's technical features. This section explores the initial design of Tor through one of these decisions: whether to include padding traffic in the Tor protocol to protect against a global adversary. First, I lay out the context of this design discussion and the various ideas the Tor developers drew on. Then, I map the processes by which the Tor developers came to a decision by refining and evaluating these ideas. Finally, I explore the consequences for Tor's privacy values and privacy properties.

### Decomposing privacy values and reconstructing privacy properties

In 2002, the developers of Tor came together on a mailing list to begin work on a practical anonymity system, following previous attempts to develop test networks as proof-of-concept for Onion Routing. These developers included academics, military security researchers and others, drawn from the initial Onion Routing project and other early anonymity systems. They began with a high-level assumption that some form of padding ought to be included to defend against the global passive adversary. In tension with this were the other core values underpinning the Onion Routing paradigm, as its technical design explicitly links privacy to usability and speed. This made the padding decision anything but certain in these early stages. The developers needed to work out the tension between the core values driving the project through exploring the practical consequences of different potential designs.

The way these decisions were made looked rather different to the traditional picture of 'inscription', in which different groups of actors compete to inscribe their own more-or-less coherent sets of values and understandings into an artefact. Rather, in

Tor's case, there was remarkable consensus around goals, and Tor's vision of privacy (as practically realised in particular design decisions) was fairly amorphous, only stabilising across the course of a substantial amount of work. Tor's vision of privacy was as much shaped by these design processes as the nascent 'value system' with which the developers began.

> When you were saying, did you do this, or did you do that… I was going to say, yes! Because I do think that it evolved over time. I know, sometimes, security research goes where somebody has a very well thought-out, theoretically analysable, mathematical argument for something, and then they try to design a system that meets that. But for us I think the idea of what security we wanted, and how to reason about it, and the system design, all kind of grew up together. And I think that actually makes sense, because if you're doing something that's really new you don't know what makes sense, and you could start with the abstract model, but you have not so much reason to think that that model is the right one. I mean, we went back and forth, and people do analyses, and then argue about the nature of the properties that are useful. And I mean, sometimes we were aware of things on an abstract level, but the data changed things.
>
> Participant I – Core Tor developer

In practice, this constituted a long period of experimentation with different potential padding regimes. The developers engaged in this in the absence of any real knowledge about how users were going to use their system, or about the capabilities of the extremely powerful adversaries against which they were designing. As a result, they were forced to reason about the properties of their system by breaking down and refining the abstract user and adversary categories with which they began. Through working out their practical consequences for the system's privacy properties, they were able to implement those that fit, and discard those which didn't.

To do this, the developers needed to be able to reason about threats and risk in a way which brought social, technical and mathematical factors into conversation with one another. While the developers began with mathematical and technical representations of the anonymity provided by the system, they quickly found that they needed to represent social factors in these discussions as well. They needed to develop a common language which could translate between these three domains.

This involved transforming social factors, such as properties of users and adversaries, into technical representations by mapping them as topological patterns of information, power and risk in the system.

> Informally I think [the roving adversary] reflects the capability of an attacker to root several machines very quickly but can't hold on to them for very long (sysadmin having a late night and figures out something is going on or some other form of [intrusion detection system] etc).
>
> Developer, tor-dev mailing list, 2002
>
> But, what is reasonable in [the roving adversary] is the partial compromise of the network. An adversary has a budget, and short of a systemic vulnerability, he must compromise individual network elements or set up his own.
>
> Developer, tor-dev mailing list, 2002

This allowed the developers to assess the practical consequences of different implementations of padding traffic for usability, resilience, security and a range of other system factors. In the following quote, the developers translate social factors in this way to reason about how long it would take to deanonymize different kinds of user:

> * If there are more users, it may take longer.
>
> * If Alice's behavior isn't very odd (that is, if she behaves similarly to other users), it may take longer.
>
> * If other users are online more often, or Alice is online more often, or Bob is online more often, it may take longer.
>
> * If Alice sends requests to a bunch of people besides Bob, it may take longer (or it may not improve anything at all -- wouldn't it be neat to be able to show that.)
>
> * If Alice refrains from talking to Bob as often, then it may take longer.
>
> Developer, tor-dev mailing list, 2002

In these discussions, users and adversaries were abstracted into categories based on the informational traces their activities map in the network. Crucially, this frames social factors through the *formalisation* of patterns of human behaviour (Musiani 2013). The everyday human interactions which Tor protects are intrinsically patterned; people want to speak to the same people repeatedly, have long-term,

linkable relationships and regularly visit the same websites. This can be modelled and reasoned about; how unique particular 'patterns' and the activities which correspond to them are, and how expensive or attractive they will be for an attacker to compromise.

Once these representations were formalised, the developers could engage in 'attack brainstorming', iteratively attempting to work out the consequences of different kinds of attack, adversary, or use case.

> It's like, someone presents a solution to this problem. And then usually what happens is that a bunch of people think through this and then come up with attacks to it. Um, and it's like, hey, what if someone did this, what if someone did this, what if someone did this? And you kind of iterate on it until you come to a point where all of the attacks you can think of in this space fail against your solution. I mean, unless someone comes up with something that's completely different, or comes up with an attack that completely subverts that, that is your working model of how things are going to be.
>
> Participant Z - Onion Service developer

In doing this, the developers built a *topology of risk*, mapping each threat and its defence as part of the internal logic of the system. They interrogated each of their core adversary and user categories in this way, mapping different potential geographies of information and control, and the consequences this bore for Tor's users in each case.

This reframes social issues in ways which can be solved by engineering practices and reasoned about in the language of technical systems. In turn, the 'values' of the developers became translated into material features of the system as the outcomes of particular design choices; choices which constrain or open up the ways in which Tor works, the uses to which it can be put, and the protection which it offers users. Those user and adversary categories or system properties which didn't fit were discarded, and those which did were stabilised in the high-level design of Tor. As they worked through these different scenarios, refining their abstract user and adversary categories, they came up against two irreconcilable material constraints.

Firstly, the everyday types of online activity which they were trying to protect are inherently patterned. The administrative traces left by these activities are extremely distinctive and provide attackers with a wealth of different ways to characterise individuals and deanonymize their Tor traffic. As they mapped these patterns in practice, they realised that protecting against traffic analysis attacks would require a degree of padding so onerous that the network would become unable to support everyday browsing:

> Here's my point about padding. Right now I'm not convinced there can be padding/throttling regimen that is both useful and practical, or maybe even either useful or practical.
>
> Developer, tor-dev mailing list, 2002

Secondly, as they refined their adversary categories, they realised that the idea of the global passive adversary was both too weak, and too strong. In practice, a global view of the Internet is extremely hard for even nation states to attain. Equally, they realised that any adversary who is able to maintain a global view of the Internet passively will have access to a range of other, 'active' attacks, such as delaying or modulating signals entering and leaving Tor nodes, which padding does nothing to stop.

> I have a basic problem with the idea of global passive adversaries. As an academic exercise, it seems fine, but it is hard for me to imagine an adversary that is powerful enough to be global but weak enough to be entirely passive... The global passive adversary is a fairly clean notion so perhaps it should still be pursued for abstract analysis purposes, but I need way more convincing than I've seen to design against it.
>
> Developer, tor-dev mailing list, 2002
>
> In the end, what we said was… because it's so easy to do the end-to-end timing correlations, we weren't going to bother to add overhead of any… padding, until somebody could come up with a design where we thought that it was reasonably helping to raise the bar. You know, so that it was actually worth it.
>
> Participant I – Tor core developer

This led the developers to make the decision to remove padding traffic from the design of Tor. This was deeply consequential, enabling Tor to provide a relatively fast

network which was usable for everyday browsing of the Internet. This has continued to the present day, where Tor is able to be used even for file transfer and video streaming. By maximising speed, Tor removes a potential restriction on the kinds of activities for which Tor can be used. For example, had they kept Tor a medium-latency network by adding padding, it could be used for email, hosting forums, and slow text-based browsing, but not easily for file sharing, video streaming, real-time chat, or commerce. This would undermine its claims to provide 'everyday privacy', restricting its users to those who require high security and don't mind extremely slow connections, thus reducing the anonymity provided by the system and making use of the system itself far more suspicious. Tor, as a result, has the widest possible spectrum of use cases for an anonymity network which also offers high levels of security against all but the most well-resourced attackers.

## Growing a social world

Through this process, the developers pulled together a design for the infrastructure, of Tor, but also a social world. The two precursor worlds of Tor, the cypherpunks and the military researchers, provided a range of conceptual resources for this process. The developers began with a range of ideas, thoughts, values, category systems and design elements from these worlds, which constituted shared conceptual resources on which they could draw. These began in the abstract and needed to be pulled into focus around a design for Tor through development processes. Through working out the practical consequences of different design decisions, they translated these values into the hard language of engineering and into the specific context of Tor, discarding those which didn't fit the material design or clashed with other key values, and iteratively sharpening and refining those which did, arriving at a coherent social world which was stabilised in the material infrastructure of Tor. These development practices themselves perform a particular understanding of privacy technology in two key ways.

Firstly, technical elements which ended up being incorporated into the design (and those which didn't) corresponded to particular components of Tor's construction of privacy. The users of Tor won out over the adversaries in this discussion: Tor firmly retained its commitment to a low-latency design, and although Tor's remained a platform with formidable security properties, it prioritised its commitment to a privacy which is open to everyone over its status as a high-security tool. Secondly, the logics of the design process itself became an important part of this social world, underpinning the way they frame the relationships between privacy technologies, politics and power. As they engaged in these design processes, the Tor engineers performed and reinforced an understanding of Tor as doing politics through architecture, working through their privacy values and design elements as structural forms in technological networks. Tor's engineers frame their vision of privacy through patterns of power and control in the structures of technical systems, making it tractable to design and engineering processes. This topological construction of privacy is one of the key elements of the engineers' social world, as described in Chapter 6.

The coming-together of Tor's design and the social world of its engineers I describe in this article is not linear. It bears, rather, some similarity to what Star describes as "convergence", the gradual converging of the category systems embedded in infrastructures and those of the people who use them (Star, Bowker, and Neumann, 1998). Here we can observe a similar process taking place during the creation of a new infrastructure and a new social world. Milan (2016) describes a related process, arguing that the practices and community structures within technological activist communities and the ethics and values of the technologies themselves exist in a dialectic, fusing through the process of design. Tor's design constituted an iterative, non-linear process through which pre-existing cultural forms, working practices and design frameworks, were brought together, refined and stabilised as a Tor-specific world of discourse. This entailed the creation of a form of knowledge very different from that imagined by more 'scientific' models of engineering, where a pre-made theoretical model is realised in a material form. Instead, the Tor engineers were

engaged in the production of a much deeper form of material knowledge, iterating back and forth between abstract understandings of the system's values and the practicalities of technical design and social factors. I argue, therefore, that design processes constitute a special case of 'convergence', through which infrastructures and social worlds mutually create one another.

This social world has changed in recent years. Tor is not, and could never be, separate from the wider political context of the Internet. The infrastructures and platforms of the Internet are increasingly clashing with the reality of social differences and political power around the world, with generic, one-size-fits-all systems increasingly encountering tension and resistance (Gillespie, 2018). Equally, an explosion in the volume of information which security researchers have about threat actors and user behaviour has shaped Tor's approach to design and the underpinning logics and values of the Tor engineers' social world. As Tor has grown, becoming implicated in a wider range of people's lives across the world, its core values haven't changed, but its practices and systems of understanding have been refined. As more real data about users and adversaries has accrued, it has been worked into this *topological* understanding of power, shifting it from an abstract, globalising picture to a collage of local contexts, mechanisms and constructions of privacy, still understood through topological patterns in the network.

## Revisiting Tor's design in a post-Snowden world

### The return of padding

The initial design discussions for Tor took place in the aftermath of the 2001 attacks on the World Trade Centre in New York. Across the next twelve years, the US and other nations ramped up their surveillance capabilities, building systems to collect huge amounts of data about domestic and foreign citizens' use of telecommunications. In 2013, a defence contractor, Edward Snowden, released a

trove of highly classified documents which laid bare these arrangements, and for the first time allowed security researchers material intelligence about the actual capabilities of US security services. This marked a sea-change for systems like Tor, and a series of leaks, disclosures, and research since have further refined this picture of intelligence agencies and other threat actors, such as organised crime groups, around the world. Despite the revelation of a vast worldwide traffic metadata collection effort which looked very similar to a global adversary, a much-cited Top Secret NSA slide from the Snowden leaks still declared Tor the "king of high-secure low-latency anonymity – there are no contenders to the throne in waiting" (Ball, 2013). However, in August of 2015, the developers were made aware of a particular surveillance mechanism which was potentially being used to mount these traffic analysis attacks on the Tor network. The developers began to discuss ways in which they could thwart this, eventually deciding to implement a light form of padding. By briefly comparing this with the initial design discussion, this section analyses how the social world of the engineers has changed since the early days of Tor.

Tor received news in 2015 that the US may have been attempting to collect the information necessary to perform timing attacks on Tor users. Alternative media site BoingBoing had been running a high-traffic Tor exit node for several years, and, as reported by Cory Doctorow in a post on their site, they received a subpoena from the FBI, asking them to "testify before a federal grand jury in New Jersey, with all our logs for our Tor exit node" (Doctorow 2015). In a comment on this story (later deleted), a university-based exit relay operator related their own experience of being subpoenaed by Homeland Security to produce three months of records for the IP address of their Tor exit node. This indicated to the Tor developers that these "netflow" logs commonly collected by internet service providers were being actively sought by law enforcement in the US:

> I would expect most US universities to be logging netflow in the very least. Even if the Tor operator isn't keeping logs, it seems safe to assume the network operator is.
>
> Developer, Tor-dev mailing list, 2015

Netflow logs are administrative logs collected by internet service providers from routers – they provide timestamps for activity, indicating when a router is inactive and when it is sending information. This is particularly damaging for Tor, as information on the timings of signals sent to and from Tor routers is exactly what is needed to perform the correlation attacks imagined in the padding discussion.

> I think for various reasons (including this one), we're soon going to want some degree of padding traffic on the Tor network at some point relatively soon, and having more information about what is typically recorded in these cases would be very useful to inform how we might want to design padding and connection usage against this and other issues.
>
> Developer, Tor-dev mailing list, 2015

The developers asked the mailing list for any expertise from people working at ISPs, or other work dealing with netflow capture about the technical details of these collection mechanisms. This collected a fantastic level of mechanical detail, down to the variation in the lengths of netflow timers in different router models, and the precise formats in which the records are stored. The developers, by mapping this information, realised that they could reduce the resolution of this timing information substantially at a very low cost by introducing a small amount of 'netflow padding' traffic into the network. The developers arrived at this though similar attack brainstorming practices to those they used in the initial design discussion, but using real, material intelligence about what adversaries are doing and how, instead of decomposing abstract categories as they did before. The proposal itself even named a specific adversary, in contrast to the 2002 discussion.

> It is also likely that defenses for this problem will prove useful against proposed data retention plans in the EU and elsewhere, since these schemes will likely rely on the same technology... Nonetheless, it is still worthwhile to consider what the adversary is capable of, especially in light of looming data retention regulation.
>
> Netflow padding protocol specification, Tor Project website

The developer in charge of leading this discussion designed an initial padding implementation, then uploaded this as a patch in progress. Roger Dingledine, the lead developer on Tor, suggested that this could be taken as an opportunity to

explore broader padding schemes for Tor, revisiting the earlier design discussion in its entirety, however the developers decided that this fix should be restricted to a specific, small-scale change designed to thwart this particular collection mechanism rather than revisiting the core design assumptions of Tor with a more abstract discussion. Following this decision, Tor now includes a limited form of padding traffic for the first time.

The practices on which the developers draw in this design process have evolved substantially since the early days of development. They now need to achieve consensus between a much larger number of people, and have instituted more formal processes of code review, change requests, proposal systems and project management. This inherently shapes the ways that decisions are made. As it has become a more mature technical project, this has also changed the *kinds* of decisions involved in Tor's development work. As Tor grows, and development work continues to build on earlier elements, so too does a form of inertia arise at the heart of the Tor design. This means that changes in the fundamental ways in which Tor works become increasingly hard as more systems are built atop them, and more people come to rely on them. The risk associated with changing, and potentially breaking, fundamental aspects of how Tor works means that design work now focuses more on higher level implementation questions, rather than the paradigms underpinning Tor itself. Despite the changing sensibilities in the engineer world, important aspects of its initial visions and frameworks of understanding, therefore, are largely permanently stabilised in Tor's infrastructure.

## A shift in the engineer social world

This discussion reveals a change in the social world of the Tor engineers as well as in Tor's design. As the knowledge and intelligence available to Tor's designers has changed, so has this shaped its social world, leading design to shift from breaking down abstract categories into hypothetical patterns to engagement with specific

mechanisms of surveillance (and hence specific adversaries). This has shaped how the Tor developers understand the world, evolving their fairly high-level understanding of Tor as redistributing topologies of informational power online. This still understands power as topological, but it is far more concerned with engaging with these novel information sources about actual mechanisms and capabilities.

There has been a complementary shift towards collecting this information themselves where necessary, as demonstrated in the padding case but also through a variety of more formal projects. Firstly, they have accepted that the ways in which they understand privacy may not match those of their users, and this has led them to conduct a substantial programme of user research, outreach work in the global South and East, and devoting substantial development time to improving usability and accessibility for a wider range of users:

> A lot of the problems that the Tor Project faces are similar to other companies – promoting user growth and user retention. Currently, our product works in a way that can be confusing. The main difference in terms of UX development is that the Tor Browser doesn't collect any information or data about you or how you use it, so they miss out on a big resource that other companies have in seeing how people use their product. This means that they need to rely more on user research and conducting experiments with volunteers and staff.
>
> Participant B - Core Tor developer (paraphrased)

This has led to the developers not just making improvements to Tor's usability, but in fact to developing new category systems for understanding and representing their users, beyond the dyadic 'everyday privacy versus high security' category system which has been at the heart of Tor for so long. This work, beginning as mapping out 'user journeys', is still in its early stages, however Tor have moved on to more formal categorisations, distilling their user research into an initial series of 'personas' which act as 'ideal type' examples of potential users of Tor. This is a way of organising the substantial amount of information which Tor has been gathering through outreach and interviews about its current and potential users around the world. The initial set of "user journeys" and personas developed by the Tor Project form the beginnings of a prospective category system for their users going forward.

This initial set includes five personas: Jelani, an LGBTQ activist in Uganda, Fanisa, a person experiencing domestic abuse in Russia, Fernanda, a women's rights activist in Colombia, Fatima, a political researcher in Egypt, and Alex, a journalist in the US. As can be seen, this is immediately reflective of the kinds of user on which the activist social world in Tor might focus, embodying a vision of Tor which promotes its use for activism, journalism, and social justice. These package up and quantify a range of factors, including levels of risk, technological proficiency, their trust of Tor, background, income, connectivity, the languages they speak, the censorship regime in their country, and the devices they use. These are both an attempt to democratise and decolonise Tor's design processes as well as a statement of Tor's changing values. The documentation around these describes them as a "vision for who we are designing for".

This is very different to the abstract reasoning and attack brainstorming I describe earlier in this chapter, explicitly packaging up ideas about particular use cases and people Tor is for, rather than beginning with abstract structural ideas about traffic patterns. Instead, while these personas are still tractable to engineer mappings of structures and power, through the inclusion of these different components, they are a much more open attempt to develop a framework for systematically reasoning about the 'human' side of the design process, which allows more direct links to be drawn between these structures and the particular political salience and values to which they are connected. This is a direct attempt to address Star's (1990) problem of outsiders in categorisation systems, ensuring that in future design work these under-represented people do not fall through the cracks. This change in the engineer world is reflective of the broader prominence of the activist social world in Tor, and the way in which it is shaping the engineer world. As I explore in more depth in Chapter 10, this also represents the beginnings of a transformation in privacy as a boundary object at the heart of Tor, and has important consequences for the social role it is attempting to inhabit.

Feeding into this user research, the Tor Project increasingly contributes to subprojects like OONI, a team operating under the Tor Project umbrella, who develop and deploy software to collect information about internet censorship around the world.

> Yeah, so that's actually something that we're trying to strengthen, and make OONI a tool that is also useful for Tor developers or people researching about the Tor network to understand better what is happening. And to that end we do have some tests that are, for example, checking to see if Tor is blocked, and I guess currently it has been more of a reactive approach, where somebody from Tor says, ah, we suspect that there's something weird going on in this country, or we saw a drop in users from Tor in this country, can you look in the OONI data to see… Um, but yeah, I think the end goal is to reach a point where we're able to do this in a way that is a bit more proactive.
>
> Participant H - Core Tor developer

Finally, they make use of whistleblowers and leaks to collect more information about the capabilities of Tor's adversaries.

> I think in terms of what capabilities they have, we rely a lot on the various whistleblowing and leaks that come out of them. I was reading through some of the documents from the CIA stuff [the Vault 7 leaks] last night, which *laughs* there's a lot there. … the most… minute comment on a page could change how you use different tools when they come from sources like this.
>
> Participant A - Tor core developer

In Tor's case, the core values of the engineers have not changed, but the maturing of the organisation, the rise in prominence of the activist social world (as I discuss in Chapter 6), the incorporation of new people and perspectives, and major changes in their understanding of the threat landscape and user behaviours have reshaped their understanding of exactly how Tor 'does politics' through architecture (Musiani 2012). As the developers are exposed to this growing pool of information, so too do they begin to realise that their apparently-universal abstract categories are in fact not sufficient to cover all cases, and embed their own subjective values and assumptions.

> I think as an outsider it's quite hard to understand what the peculiarities of a certain country are. And I think there are for sure some common principles, and things that motivate our work, which is, you know, we believe in the right to privacy… and that

> in the end, people should have the right to access all information, but at the same time trying to not get too much into complex socio-political issues in a particular country. And trying to balance that, so that we can ensure that those that give colour to the things that we promote are actually the people that are from that country, that have a better understanding of what is happening there.
>
> Participant H – Tor core developer

The social worlds of privacy technologies, their material privacy properties, and the working practices through which their developers build them in practice are interconnected, mutually shaping one another. Tor's engineers still view privacy technology as redistributing power, but now recognise that power manifests in infrastructures in practice in complex ways shaped by different contexts. They now attempt to reshape this terrain through a deep understanding of particular local contexts rather than through broad, simplifying abstractions. This amounts to a transformation in the practices of the engineer world which reflects their changing ways of making sense of Tor as a site of social action.

## Conclusion

In this chapter, I have discussed how Tor's values and its design shape one another. I have outlined the vision of privacy which underpins Tor design, and its complex relationship with the privacy properties of Tor as a technology. In mapping the interplay between meaning and materiality, I have chosen to focus on a single world of Tor: that of the engineers. In these early years of Tor, before the rise of the Tor infrastructure and its growth into a larger community, the engineer world was the main force in shaping Tor's design. In fusing the precursor worlds of the cypherpunks and the military cryptographers, the engineer world actually arose across the work of developing Tor, forming as part of the same process which formed Tor's material design through iterative tacking-between ideas, technical practices, experimentation, and creation. The engineer social world which formed embodies a set of understandings of privacy which are framed through the organising logics of the design practices the developers used, which translate human factors into

structural patterns and paradigms in information networks. I have explored this through the study of a particularly important design decision (though one of many): the decision not to include padding traffic in Tor.

Tor's worlds, however, are not static, and as the organisation has changed from a tiny development team working on a mailing list to a modern tech NGO with a sizeable community and an infrastructure used by two million people every day, so too have its design and development practices and the social world which underpins them begun to change. As I discussed in Chapter 6, Tor's engineer world has seen a transformation in recent years, shifting to a more reflective and critical perspective on their own power to shape the world through design. Partly shaped by the increasing prominence of the activist world, partly by broader changes in the culture of information security research, and partly by the maturing of Tor as an organisation and the increased information which they have about user and adversary capabilities, this has led to a change in development practices. As I discuss in Chapter 10, this is of profound importance to Tor's relationship with governance and power.

However, as Star (1999) argues, processes of design are not the only important factor in understanding infrastructure. These cannot shape the world alone: they rely on a range of different kinds of hidden work to materialise and perform the ideas, category systems, and frameworks of representation which they embed in infrastructure. In the following chapter, I explore this hidden work and its salience to Tor as a site of social action.

# chapter 8
# open secrets, hidden work

## Introduction

Understanding the work of design and development is crucial to making sense of infrastructures as sites of social action. It is on this kind of work which much scrutiny has been focused in critiquing power and control in online platforms and infrastructures, and this has the capacity to surface important aspects of how design features of infrastructure shape society and social justice. However, in moving from a prototype or proof-of-concept to a system which spans the world, design needs to be materialised as infrastructure, and hence pulls in a range of other considerations and kinds of work which often remain hidden. In my research, I found that Tor relies on a great deal of this hidden work to realise the different design visions embedded in its technology and its community, and it is this hidden work which I explore in this chapter.

While Tor is a home for many kinds of hidden work, I focus in this chapter on the different kinds of *resilience* work on which Tor relies, as this also ties into Tor's relationship with the mechanisms used by law enforcement to establish control over the Internet infrastructure. I focus particularly on how Tor understands and attempts to resist 'high policing' (which I discuss in Chapter 3) (Brodeur, 2007), attempts made by secret services to undermine or compromise Tor and its community. In doing this, I aim to explore the relationship between design and its realisation in Tor and draw out the links between its three social worlds. First, I discuss Tor's attempts to 'design-in' resilience to its community. This draws on the 'structural' understandings

of the engineer social world, which aims to use openness and decentralisation to cultivate resilience. I then explore how this design is actually negotiated and realised in practice, and the hidden work involved in balancing the different considerations which come into play. In the next section, I turn to the resilience of the material infrastructure of Tor itself, and the hidden work of the relay operators which underpins this. Finally, I discuss the practices of maintenance and bugfixing which, although often ignored, are vital to ensuring Tor's security, and an important site where values are negotiated and performed.

## Technosocial threats and designing a community – resilience through openness and decentralisation

As a security technology, resilience is a fundamental quality of Tor's design, written through every decision the developers made about the project when working out how it was going to work in practice. This resilience design work extends well beyond the technological components and protocols of Tor into the human infrastructure of the Tor community. Tor is a *technosocial* system: its technical components depend on human factors which could prove either fatal weak links or key sites of resilience. For example, those wishing to attack Tor could either devote substantial technical resources to overcoming its protections or could far more easily target a developer or relay operator through threats and blackmail to introduce a vulnerability into the system. This makes the community on which Tor depends to develop its code, manage its finances, administer its networks, and make the case for it in public as important to protect as the technology itself. The ways in which Tor attempts to guard against these social threats draws largely from its *engineer* social world, turning the same rationalities and logics which the developers use to secure Tor's technological design on the community itself. In this section, I explore this conceptualisation of resilience and how it has shaped the Tor Project's attempts to defend itself against a range of social threats.

The ‘social’ threats which Tor faces are lurid in their scope and seriousness. In particular, Tor is deeply worried about compromise by security services. Tor’s potential adversaries include a range of organisations (for illustration, this includes but is not limited to nation state secret services and organised crime groups around the world) with massive budgets, advanced intelligence capabilities, and a long history of espionage, infiltration, and disruption targeted at resistance groups. These nation state adversaries have the capacity to engage in a range of actions against Tor as an organisation, ranging from high policing to active espionage or disruption (BBC, 2019). This goes beyond hacking and wiretapping to include attempts to compromise the human side of the organisation. Many of the conventional infrastructural organisations and platforms which support the Internet come to some sort of accommodation with security services, in which liaison groups or individuals are set up who can respond to requests for data on particular users or entire populations for crime fighting and security purposes (Lyon, 2014). This can even extend to pressuring organisations to install backdoors in their software, either covertly or overtly (BBC, 2018). This use of liaison contacts extends further, to the police and NCA, and facilitates inter-organisational collaboration. The Tor Project understandably refuses this kind of co-operation entirely, and as a result feel the need to defend themselves against more forceful strategies.

In understanding how to design for resilience in the Tor community, the engineers adopt very similar approaches to those which they use to reason about Tor’s code. To an *engineer* view, social factors like friendships, hierarchies, organisational structure, working practices, communication, and social interaction can be reasoned about as structural patterns of power and information which can be arranged to promote resilience. This leads them to turn their design practices on the community itself, explicitly engineering its social structures in ways which are protective. Underpinning this community design work are the principles of *radical openness* and *decentralisation*.

## Radical openness

The first design strategy Tor uses to counter this, paradoxically, is the opposite of the secrecy which one might expect from such an organisation. Instead, Tor designs its community around a principle of *radical openness* to minimize any concentrations of secret information within the organisation. This openness takes traditional open source software values and turns them into the primary resilience design principle which protects their community (Berry, 2008).

Tor extends this openness well beyond what might be expected of a privacy project, putting an enormous amount of other information in the public domain, from the names and email addresses of most of the key members of their communities, to financial records, to the full internal mailing lists and design discussions of their development team in addition to Tor's source code. This means that Tor's source code, financial details, internal bug-tracking and work-tracking systems, design discussions, internal mail, meeting minutes, and the majority of its developers' identities are published openly on the Web. Tor's developers see structuring their community around 'radical openness' as protecting them from a range of sociotechnical threats: ways to undermine the technology of Tor through the people embedded in it. I identify here four core threats against which they feel this defends: *infiltration*, *coercion*, *misinformation*, and *disruption*.

First, they are worried that malicious actors will try to *infiltrate* the Tor community. As imagined, this would involve a hostile agent attempting to become part of the Tor Project, becoming a developer or attaining another position of influence, reporting back secret information and attempting to undermine Tor's technology. This means that Tor needs to be careful in managing who contributes to the project, and how. On the other hand, they also don't want to have barriers to new people: as a small organisation dependent on volunteer labour to survive, Tor get a lot of their power and vibrancy from the constant flow of new people, skills and ideas into their community. They see radical openness as an elegant solution to this problem, as having the code open source allows them to get the measure of putative

collaborators and build trust, and allows those with an interest in Tor the opportunity to follow the development and propose their own changes which can be scrutinised by the community.

> Tor as, as a project is something that's, I think it could not… maybe it would exist, but it would not be able to do all the things that it does if it were not for the huge community that we have around it of people that just show up and are aligned with our ideals and believe in what we are doing, and contribute as just a labour of love to the project and to what we are doing. Like, I think, uh, without that we would definitely be much, much weaker and be able to do much less than what we do. So that I think is definitely something that would not be possible if, if we were to have a much more… closed and siloed approach to development discussions and whatnot.
>
> Participant H - Tor core developer

This also allows them to punch above their weight as a relatively small organisation. Academics at the top of their fields from all over the world are able to contribute to Tor in ways which would be impossible if the code was closed-source. The proposal system means that ideas from the community are subject to the same scrutiny as the rest of the project's work, making it more likely that malicious changes will be spotted and helping to build trust with potential new members. This also helps Tor reckon with its own power to shape people's lives, as they can bring more people into the design discussions, allowing Tor to be more representative.

The second threat with which the Tor Project are concerned is blackmail or *coercion* of its developers. There is a perception within the Tor community that there is a risk of external actors blackmailing or coercing individual members to compromise the technology or pass on secret information. This is a common anxiety of the developers of privacy technologies, given the repeated public assertions by politicians in most countries that these technologies should insert 'backdoors' which allow law enforcement access. A policy of radical openness, they hypothesise, helps this as it dramatically reduces the amount of secret information which is actually held by the organisation, and hence makes it both very obvious if someone has been blackmailed, reducing the damage they can do (and their attractiveness as a target) if it does happen.

> I would say that… I take some precautions. But I think actually the biggest protection is that it is Open Source… So, if there was an attempt to, let's say, coerce me into writing a patch that would be malicious or whatever, then that would, I very much hope that would be spotted by somebody *laughs*... I mean I also hope that I would just not do it. But if there was some way that I was actually coerced into doing it, my feeling is that it's actually *sighs* there's not that much value in targeting me, actually? So if somebody did try to target me, that would probably be because *they didn't understand the structure of what I'm doing* …I think… if I had to sort of keep a lot of things… secret in general, or if we were working closed, then it would be a very different kind of threat model.
>
> Participant C - core Tor developer (emphasis added)

Third, they are particularly worried about the spread of *misinformation* about Tor, which is often referred to within the community as 'FUD', or fear, uncertainty, and doubt. This entails spreading rumours that Tor has been compromised or is fundamentally insecure, undermining trust in Tor in the broader information security community and with its potential users. This is one of the more serious threats to Tor. The media apparatus which has grown up around information security, along with Tor's prominence as an attractive target, means that the discovery of even small vulnerabilities in Tor are accompanied by significant press attention. Similarly, the money which Tor accepts from the US government and its history with the US Naval Research Institute means that there are large sections of the information security community who instinctively distrust it, and may recommend not using Tor to people who could in fact benefit from it.

> I think it's actually more dangerous, all this talk internally in, kind of, the more technical scenes, the, kind of, talk about backdoors, about US government funding, about, you cannot trust Tor, um, on various levels and with various intensity. Because I think in the hacker community, there's a growing number of people that don't like Tor anymore. Uh, or never liked it, or are now more vocal about not recommending Tor… that of course when you're in a technical crowd and you can have these conversations, and you can say, OK there's certain, kind of, downsides to this technology, and certain risks that replace other risks… But what ends up happening is that people who ask their friends, and they ask their tech guys, and they say no, don't use Tor, then people end up using something that is worse for them. Um, and that's in some respect, for me, more dangerous, to kind of lose this core group, and I think it's the most relevant group because it spreads the knowledge. Um, it's like, if you don't know shit, you will ask the person you know that knows a bit more, and it's like a cascade that will end up somewhere in the hacker scene. And that guy says "oh no, Tor is shit", over a beer or something, and then this will have consequences for users.

Participant L - Tor core contributor

Openness helps in part to mitigate this, as it cultivates community trust and legitimacy. Tor's code is sifted over by large numbers of computer security professionals around the world, and this makes it in theory 'trust-neutral', so users don't need to trust the developers in order to use it. This also turns the natural scepticism of the information security community into an asset: the discovery of a vulnerability in Tor is a route to high-impact research and widespread media reporting, and thus this encourages this community to work on finding and fixing these vulnerabilities, increasing the scrutiny of the code, improving Tor's security, and hence its legitimacy with its users.

The fourth and final way in which the Tor developers understand the protective value of radical openness is possibly the most important of these: *disruption*. The state security actors against which they are attempting to defend have a long history of skilfully disrupting undesirable activist or resistance groups through stirring up internal conflict and stoking paranoia. This poses a particularly serious threat to Tor, as given the well-trodden history of activist community dynamics, this also has the potential to occur even without external provocation. Openness helps this as it encourages positive social dynamics rather than an economy of secret information which they see as easily exploited by outside actors.

> Uh, so it kind of, it, you know, I mean I think you see this in organisations where they, they keep things secret, not just from the outside world, but because they're keeping things secret from the outside world, they end up being secret from eachother too, and it makes it harder for them to, you know, work, work together smoothly.
>
> Participant C - Tor core developer

This *radical openness* has been part of Tor's design since its precursor projects in the US Naval Research lab. In order to attract the everyday users in countries around the world and hence generate enough cover traffic to protect high-security users, the system has to provide genuine, demonstrable protections which do not rely on trusting the US government, and so a radically open design is necessary:

> [Tor has said from the start that] this can't be a Navy-only system, it can't be just [Navy] stuff, or it won't have the protections you need. Um, and so you need to carry traffic for other people…and then following on that, you also can't say, oh, here's this binary blob of code we wrote, you know, we're the Navy, trust us, it's great! Um, you need to have it be Open Source, you know, in order for people to know it's OK, and not just Open Source, which is, you know, I guess originally we were probably just thinking that, but, uh, evolving a bit we realised, OK, not just Open Source, but it has to be well-documented, and you have to encourage various researchers to, to pound on it, and then publish anything that they find. And, so, the point is, the idea that you need to have Open Source, freely-available, uh, system design, and code, was in from the very beginning, and… that was part and parcel to the security protections you wanted the system to provide.
>
> Participant I - Tor core developer

This has been particularly successful, as it resonates with the values of the Open Source hackers and liberal, libertarian, and anarchist community members who have joined along the way. This is equally the case for its second community design principle: *decentralisation*.

## Decentralisation and non-hierarchical structures

The second design principle through which Tor attempts an *engineer* approach to community resilience is *decentralisation*, minimising concentrations of power and influence, and distributing key responsibilities among separate groups. This operates in two ways: the separation of Tor's volunteer-run infrastructure and its developers, and the adoption of an anti-hierarchical approach within the Tor Project itself.

The infrastructure of Tor is not administered or controlled by the Tor Project or its developers, in fact, they minimize their involvement with the network as much as possible. Instead of centralised provision, the Tor network is owned and operated by a community of volunteers around the world who purchase servers, set them up as Tor relays themselves, and make a range of decisions about how they work and the kinds of traffic which they carry. This means that *trust* in the network and the *risks* of supporting Tor are spread among a wide variety of different actors. There is no central authority for police to subpoena for traffic records, and it is impossible for

anyone in the Tor Project or Tor network to provide useful information on its users to law enforcement. It also means that users don't need to trust the Tor Project, and as Tor's design means that its anonymity protections improve with larger numbers of more diverse users, opening its use up to people who don't trust the US government is particularly useful.

> But if we're the only ones running the system, then the only people you're going to get is the people who are inclined to trust us. You know, and so maybe it's not quite as narrow, but it's still probably limiting in a way you don't want…So, you need to let diversely trusting people run different parts of the infrastructure. And that actually also underscores its security, because if they're running it, and it's run by different entities, which are perhaps, you know, might have, be reputable, but are still not ones that you would expect to fully co-operate if somebody wanted to pull this apart. Uh, that goes into it. So, you need to let mutually mistrusting people run different parts of the infrastructure.
>
> Participant I - Tor core developer

The other key way in which the Tor Project attempts to decentralise power within its community is within the structure of the core Tor Project organisation. Tor are concerned with the ability of malicious actors to concentrate power around themselves, either as an active measure of disrupting Tor by its adversaries, or through internal issues which arise without the intervention of hostile external actors. As a result, while some aspects of decision making are fairly centralised, they try to keep as much as possible a balance of power within the organisation, with individuals having a great deal of control over their own projects and the things they work on, rather than a strong centralised hierarchy, and broader decisions being made through consensus.

> Yeah, well I think one of the things that's quite good about Tor, especially these days, is that we don't have kind of a really strong personality cult or something like that, where, you know, I think that Wikileaks partly suffers from that. I think, you know, any one person could have an issue or whatever, but it doesn't necessarily undermine the whole organisation… So you're more, I think it's more fragile [when power become concentrated], because it's really much more exposed to the mistakes of one person, let's say. I mean, Wikileaks might also be an example. But I think in Tor, it's not that there's no hierarchy, but there's a general feeling, I mean, we talk about a "do-ocracy" in Tor *laughs* which is, I don't think originates from Tor, I'm not sure where it comes from, but basically, like, you know, if you want something to happen, you just do it. And, and you don't have to ask permission for

> things, to do things, and generally speaking, people will respect you for the effort of trying to do something and, um… you know, and if someone does something really bad then the other people will try to fix it. It's like, there's not really a single point of failure.
>
> Participant C - Tor core developer

Tor's engineers see this decentralisation of power as both promoting positive social relationships (and hence reducing the capacity for disrupting the community) and reducing the importance of any individual within the organisation in order to avoid creating natural targets for their adversaries. Not only does this mean that compromising an individual within Tor is less useful (as no one should have undue influence or be able to overrule the collective will), it also means that if they lose a member of the community, the organisation is more able to survive.

This open and decentralised community design works in practice because it stems from the core cultural values of the Tor community, resonating both with its technical design, and with the practices and logics of the Open Source hackers who make up much of its natural constituency. These design elements of Tor's community are important, but they have realised over the years, through sometimes substantial hardship, that maintaining these community designs of openness and decentralisation relies on complex negotiation and a substantial amount of support and maintenance in practice.

## Negotiating community design in practice

These approaches stem from practices of design, and the rationales behind them imply a kind of structural determinism, where decentralised, open structures inherently 'beat' the centralised, closed structures of those attempting to attack Tor, however these structures do not operate deterministically. In fact, they require a substantial amount of hidden work to be achieved in practice and pose serious issues which need to be navigated. Striking a balance between the protective dimension of openness and the risks it brings is not easy and requires active negotiation. Similarly,

the full decentralisation of power can be somewhat elusive for a community where tough decisions need to be made quickly, and which relies on key individuals as 'translators' to bridge the different parts of the community. These structural designs are therefore negotiated carefully in practice, with an eye to pragmatic compromises where they prove in the interests of the security and safety of the organisation and its users.

For example, Tor's radical openness is not as complete as it may appear. Not all of Tor's inner workings are in practice laid bare to the eyes of the world. Some elements of the functioning of Tor are kept secret, especially the tools which it uses to detect malicious relays in its network, in order to make them harder for adversaries to circumvent. While Tor's developers minimise the amount of "security through obscurity" (Hoepman and Jacobs, 2008) which they employ, sometimes they do judge this necessary. This also includes pragmatic decisions to protect Tor's users. For example, in the event of a major vulnerability being discovered in Tor, the team have in the past practiced 'responsible disclosure', waiting until they have a patch ready to fix it before revealing its existence to the community so that its users were not exposed to unnecessary danger. This means that, rather than an absolutist approach to openness, in practice maintaining this balance requires careful judgement and discussion.

> It's a very fine line that we walk. And we basically weigh that decision at every single point and as much as possible, we publish and make available everything up to, but not including whatever information could harm the Tor network. And, finding that, that line that we shouldn't cross is… difficult, but I would say most people agree. There are certainly some people that think we should be 100% transparent, but… we've, as a group we've generally decided that it's better to be slightly closed and reap some of the benefit from that, rather than be completely open and not be able to protect the Tor network as much.
>
> Participant A – Tor core developer

Equally, not all of Tor's development discussions are carried out in the open for practical reasons. Where criticism is potentially contentious, or ideas are suggested by newer developers, discussion is sometimes worked out internally at first so as not to expose the developers to unnecessarily harsh criticism without carrying out

internal scrutiny first. The Tor developers don't feel that this undermines their commitment to open development, as the result is still put out to the community for open discussion, but some of the messiness is redacted to help the discussion proceed in a constructive way. Equally, given the often-toxic culture of the information security community, there need to be mechanisms for newer or less-experienced developers to express opinions, get things wrong, or ask questions without being subject to abuse. As a result, some internal discussions are kept private so that developers can learn and work in a collaborative and productive environment.

> I guess I would say, I think there is scope for, like, private advice on occasion. Um, so maybe that's a slightly… I don't know, that's an interesting one. Because pretty much, almost everything I do is public, and I do get a certain amount of like… um, ridicule *laughs* for the things I say. Or, like, or harsh criticism. I mean there's definitely a certain, like, culture, at least among, I mean obviously online there's a culture of abuse, right, but, you know, even just among, particularly security people I've noticed…I mean, I don't know how to put this politely, but there's a lot of know-it-alls basically *laughs* right? Who like to sort of, demean people who ask them questions or whatever… But there is a little bit of exposure there and so it is true that sometimes I try not to expose other people that way. Like, I'll say something privately to them rather than saying it, you know, our ticketing system. Because of course we're all just human beings and nobody knows everything, so…
>
> Participant C - Tor core developer

Another problem with a truly open design is that it potentially opens Tor up to being steered in directions it doesn't want to go (for example, prioritising too much security over usability), and coordinating actual debate about decisions with a huge community is difficult. In practice, a set of natural exclusionary mechanisms, particularly the complexity of the Tor technical design and the cryptographic protocols on which it depends, reduces contribution to a manageable level. This also helps maintain the separation between the roles of developer and infrastructure maintainer, as it dissuades the relay operators from seizing control of the project, or leaving to form a splinter group (what Open Source organisations call a 'fork'). Most of the Tor community is largely happy to let the developers do their own thing, as long as it is open to expert scrutiny, and the complexity of these discussions means that public debate is often fiercest around the less important areas. While the

developers are happy to explain their decisions and engage with the community, they are also well able to push back where they feel that a design decision might endanger their vision for Tor.

> Um, what colour do we paint the bike shed? *laughs* If it's an easy question, everyone has an opinion. If it's a more technical question then less people have an opinion… If people have strong opinions about the way it should be done they'll come forward and they'll argue it out, but it'll be a shorter discussion and you'll have less people involved.
>
> Participant D – Tor core developer

Similarly, decentralising human social structures is not always easy in practice, and relies on a degree of pragmatism. Many of Tor's users depend upon it in potentially life-and-death situations, and so its design processes require stability and careful judgement before radical shifts in design are made, in case these users might be endangered. A rigidly decentralised structure could potentially open Tor up to entryism, or to well-meaning new community members banding together to push through a change which inadvertently put Tor's high-risk users in danger. As a result, in practice, a few key people within the organisation have ultimate veto over the direction Tor takes, even if this operates more as 'institutional conscience' than the 'benevolent dictators' which lead many Open Source software projects (Ljungberg, 2000). Other people can fork the code and set up their own projects, but internal trust is a key factor in whether something actually gets integrated into the code, or becomes an official Tor Project project.

> In terms of the community, it's kind of interesting how projects become 'official' Tor projects as opposed to just community projects. Generally, it's if the project is created by someone who is already… viewed as a core 'Tor person', an integral Tor person, then it's kind of by default, their project then becomes kind of a Tor Project project, whereas if it's someone in the community, then that just kind of like a community project. Unfortunately, not all core Tor people… necessarily write the best, you know, create the best projects, whereas some community people may make much better projects, but it's just… the core person… I think, their projects hold more weight. And so, it's just by default we kind of trust them more I guess – for better or for worse.
>
> Participant A - Tor core developer

> But it's, there within the Tor Project it's not easy to do any takeovers because it's the main core developers. And I don't see why Nick Mathewson would have a change of opinion in how he thinks about Tor. Or Roger. Ultimately, I mean Roger's very accepting and very, kind of, trying to stay out of decisions now. And, kind of, secretly, I think, if there was something happening in that respect that would endanger, kind of, how everything is working technically, uh, they wouldn't accept that. So, I don't think there's a threat there or even a possibility of manipulation or anything.
>
> Participant L - Tor core developer

This decentralisation has in itself proven problematic. Known within the information security community as the 'rock star' (Honeywell, 2016) problem, there is a well-documented tendency in disruptive tech organisations like Tor (and in activist communities), which often grow from small, agile beginnings, eschewing formal HR and workload management processes, to attract abusive, manipulative individuals who seek to concentrate power around themselves for personal gain. For much of its history, Tor has attempted to cultivate decentralisation and anti-hierarchy 'by default', eschewing formal mechanisms and assuming that not imposing structure would lead to a decentralised structure in practice.

This was shaken by a crisis when one of Tor's developers was fired. Jacob Appelbaum was accused by several members of the Tor community of sexual assault, rape, and abusive behaviour. These community members described Appelbaum as having abused Tor's lack of formal structure to cultivate his own informal power structures within the Tor community, stealing others' work, and presenting himself as the face of the organisation. After firing Appelbaum, the Tor Project brought in a new board, including a director who had substantial experience in the NGO sector. This led to a restructuring of Tor, with formal processes being developed with an aim to help maintain this decentralised structure, prevent harmful informal hierarchies developing, and work through issues as they arose. There is, in practice, a serious difference between 'structurelessness' and decentralisation of power: structureless communities often form informal hierarchies over time, while true decentralisation of power requires reflection, maintenance, and formal negotiation (Freeman, 1972). This was a major part of the Tor Project's attempts at professionalisation, inscribing

these structures into their organisation actively by, for example, ensuring a regular rotation of speaking engagements among the core team. This led to more formalised community structures rather than the previous approach, which was characterised by a *lassiez-faire* structurelessness which assumed that a lack of formal hierarchies would be enough to prevent informal ones developing.

> I think these organisations come together, and there's all this idealism, and things that come in. And then there's personality types that, not necessarily trolls per se, but… where the, the goal is much more, sort of, self-centred, that kind of undermine the original ideals and things, but because by its nature it's, sort of, open and accepting, and then they basically, it doesn't take many of them to break the organisation apart. Unless it has, sort of, structural things in place, and has community management and HR and whatnot, so that that's less likely to be an issue. Uh, I'm sure you're aware, Tor's had some horrible things, and, uh… you know, that was, that was excruciating. That was awful. Um… it's hard to use adequate terminology about, about some of those things. And it's not the only thing but having… ways to deal with that, and not have it pull the organisation apart is important, and I suspect that if it had, you know, happened, I don't know, hard to say, but if it had happened five years earlier, maybe it, it would have, you know, just pulled everything apart.
>
> Participant I – Tor core developer

Navigating the complexities of 'designing in' openness and decentralisation in practice goes beyond design work, and the Tor Project has relied on a different set of sensibilities and expertise in negotiating this: the *activist* world. This stems from the practices and perspectives of the activists, HR people, policy workers and NGO workers, many of whom (though not all) have joined the community since the Snowden revelations. The *activist* world sees privacy technologies as explicitly political, driven by strong values which have a discursive power of their own. Thus, they see Tor as part of a social movement and with a responsibility to intervene in public discourse about privacy and other political arenas. In navigating the issues which arise when these design elements enter the world, the *activist* perspective aims to draw on shared values to shape how they make these decisions in practice, how open is open, and whose projects and suggestions get approved.

In doing this, they seek to actively cultivate, reflect upon, debate, and critique a set of values within the community which they can use to guide them through these

decisions. This has occasionally proven contentious: the Tor community is characterised by a range of different perspectives, values and understandings, and so attempting to find a set of common values has in the past proven difficult. The recent social contract drawn up by the Tor Project is one example of how this has progressed from Tor's originally more lassiez-faire approach. Following the crisis around Appelbaum's alleged behaviours and expulsion, there was a concerted effort within the organisation to assert Tor's values as a feminist organisation and embed this into formal structures, such as the social contract. Drawing these practices into the terrain of debate, politics, and values may be difficult, however (as I explore in the following section) it has a range of benefits for Tor's community and its technical work. It allows essentially structurally conceived values such as openness and decentralisation to be brought into conversation with other political questions and ways of thinking, ultimately reshaping the ways decisions are made in Tor.

While community and human factors are often portrayed as the "weak link" in security engineering, the Tor Project is an example of how they can become a powerful site of resilience. As the Tor Project have attempted to 'design' their community, they have realised that although these strategies are effective, they require a lot of active negotiation in practice. I argue that this negotiation constitutes a form of hidden work which is crucial in maintaining the human infrastructure of Tor and 'performing' the ideas of openness and decentralisation embedded in the design of its community structures. In navigating these issues, the Tor Project have found the need to draw on other ways of understanding resilience and community, drawing on a more *activist* perspective which pulls these issues and decisions into the realm of value discussions. While this holds true for these 'community design' issues, these problems of how to move 'beyond design' are also important for the technologies of Tor themselves, which I discuss in the next section.

## Technical threats and the hidden work of Tor: administration and maintenance as resilience practices

In addition to attacks on the Tor community, there are a range of ways in which it attempts to defend against more technically-focused attacks. I explore Tor's technical design in the previous chapter, and there are a wealth of papers by the Tor Project and others which set out the technical ways in which Tor is engineered for resilience and security by design (Dingledine, Matthewson, and Syverson, 2004). As one might expect, the *engineer* world is foundational to this technical design work. The way in which Tor's technology is designed is important in conferring on it resilience properties, however (much like the community design elements I discuss above) these design effects similarly require a substantial amount of supportive work to be produced in practice. Tor relies on a huge amount of invisible work, not only from the infrastructural workers who administer its infrastructure, but also from the developers who carry out maintenance work on the code.

There is plentiful evidence, from reporting, leaks, and research, that the security services of nation states around the world are attempting to compromise the technological functioning of Tor in order to develop the capacity to identify its users (Lyon, 2014). As Tor has remained firm against any attempts to create 'backdoors' in its code to allow access to state security services, this has involved a certain amount of subterfuge. There are three primary ways in which Tor's *design* is subject to attack. Firstly, they can target the infrastructure of the Tor network, as Tor is vulnerable to 'traffic analysis' attacks, through which adversaries compromise relays or Internet Service Providers, or surveil enough of the global internet traffic to get a full view of the Tor network, allowing them to time the signals travelling therein and trace them back to their origin.

The second involves adversaries setting up their own relays and spying on traffic (a practice Tor counters through the Bad Relay Team which removes suspicious relays from the network). The third is targeted at the users themselves, and involves either

compromising the computers of Tor users through spreading large amounts of malware on citizens' computers (so-called bulk equipment interference), or exploiting bugs and oversights in the implementation of the Tor Browser in order to leak small amounts of information about the target when they visit these pages. In this section, I explore a by no means exhaustive selection of examples of the hidden work beyond the design of Tor itself through which Tor defends against attacks on its network and users, and the rationalities which underpin them.

## Beyond design: hidden work and the Tor infrastructure

The first domain of technical 'hidden work' on which Tor relies is that undertaken by the people who run and administer Tor's infrastructure. As I describe above, Tor's infrastructure is not run by the Tor Project, rather it is in the hands of a community of volunteers around the world. Anyone with sufficient resource to rent a private server can set up a Tor relay. This involves downloading some free programs from the Tor Project website, installing them on either one's home machine or on a rented server, and running them. Although this infrastructure is dependent on maintenance and administration practices for its resilience and stability, it too is underpinned by design principles shaped by the *engineer* world. For example, the relay network is structured to spread the risk of carrying potentially-illicit traffic around everyone in the network, and has a range of features which allow individuals to tailor their own individual engagement with this risk. Operators can choose to run entry, middle, or exit nodes, with middle nodes carrying very little risk (as they just pass traffic through the Tor network), and exit nodes accruing more (as they make the final request to the destination, so risk law enforcement attention). Equally, operators are allowed to set their own 'exit policies', blocking certain commonly-known abusive services or certain types of traffic (such as email or Internet Relay Chat), depending on what they are comfortable carrying through their relay

As important as these design considerations are, though, the work of relay operation is in itself important for the resilience of the network. The day-to-day of running a node involves a small amount of basic maintenance, such as updating relays when new patches come out, however this is more akin to gardening than hacking: they mostly just sit in a box or on a virtual server. This means that relay ops don't feel obliged to get deeply into the politics of Tor, and similarly the commitment is small enough that anything less than major scandals or value conflicts don't usually stop operators from running nodes. Additionally, the level of involvement is enough to provide a sense of satisfaction, much like gardening or volunteering, but not particularly arduous. This sensibility is linked to (but based around a different set of practices from) classic "hacker" sensibilities, and encourages experimentation and the development of clever and creative administrative practices to get the relays to work better, which are shared between the operators in documents, wikis and mailing list discussions.

> I've begun to realize that running a fast Tor relay is a pretty black art, with a lot of ad-hoc practice. Only a few people know how to do it, and if you just use Linux and Tor out of the box, your relay will likely underperform… In the interest of trying to help grow and distribute the network, my ultimate plan is to try to collect all of this lore, use Science to divine out what actually matters, and then write a more succinct blog post about it. However, that is a lot of work. It's also not totally necessary to do all this work, when you can get a pretty good setup with a rough superset of all of the ad-hoc voodoo. This post is thus about that voodoo.
>
> Relay operator, Tor-relays mailing list, 200X

This hidden work all promotes the resilience of the Tor network, underpinning its stability. As Star argues, this kind of hidden work is vital to all infrastructures, allowing them to become "transparent" to the user, and appear to operate smoothly and reliably, becoming visible (to the user) only on breakdown. These practices are crucial in underpinning the *infrastructuralist* world in Tor.

This hidden work also includes a range of strategies for undermining 'high policing' attempts to compromise the Tor relay network. Among the practices shared and developed by the Tor relay operator community is the strategy of 'relay diversity'. If all Tor relays run on Windows, and a serious vulnerability in Windows is secretly

discovered, this allows hostile actors to spy on or take down all Tor relays. Equally, if all the worlds' Tor relays are concentrated in Europe, this allows European nations to block or surveil them easily. Hence, a key part of the administration of the Tor network is encouraging relay diversity by hosting them in a variety of different countries, on a variety of different operating systems, and in a variety of different configurations. This aims to make the relays of the Tor network as heterogeneous as possible, running on different kinds of computers, operating systems, in different countries, and through different kinds of organisation, in order to minimise the damage to the network if GCHQ's hackers find an exploit for a particular type of system, or if a particular country decides to seize or surveil all its Tor relays.

This hidden work is not only vital to Tor's survival, but also itself performs a distinct vision of Tor as a site of social action. This vision of resilience isn't *structural* like that of the engineers, or *value-driven* like that of the activists, it is *agile, creative,* and '*hackery*', driven by the confluence of pragmatic practices of administration and a subversive hacker ethic. Rather than negotiating the reality of Tor's design through values or structure-writ-large, the *infrastructuralists* do so by attempting to find clever loopholes, creative, partial, 'edge-case' solutions, and through a focus on keeping the technology working in practice. This work is therefore important not only in 'maintaining' Tor's infrastructure, but also in 'maintaining' and performing the infrastructuralist social world's values and frameworks of understanding.

## Maintenance as resilience practice: "is this going to be a stand-up fight or another bug hunt?"[24]

The final area of resilience practice I discuss herein concerns the code of Tor itself. Code is the implementation of design: people can come up with understandings of how the system works and is structured at different levels of abstraction, but this is

[24] Quote from Cameron, J. (1983) *Aliens*, 20th Century Fox

materialised in practice at the level of code. However, this code is not static - information technologies and infrastructures like Tor are not frozen in time at the moment of their creation, rather they need constant development, revision, updating, and a myriad of much smaller maintenance practices which all constitute the ongoing processes of development which enable them to continue to function. These maintenance practices, such as fixing bugs or finding loopholes in the code are in themselves part of the implementation of Tor, and hence sites where a multitude of small but important decisions need to be made. In this section, I briefly describe these maintenance practices and how the developers understand and navigate them in practice.

Although much-mythologised, the work of "hackers" attempting to compromise information systems rarely involves the often-costly development of pathbreaking new attacks which undermine the very way a system is designed. In fact, much of what is exploited in practice are edge cases, bugs, and blind spots which inadvertently allow the attacker to gain control of the system, or in Tor's case, to cause information about the user's identity to be leaked or tracked. The often-tedious work of bugfixing and code maintenance is therefore enormously important for Tor's security. Accordingly, the Tor Project recently ran a large fundraising campaign to raise additional funds for bugfixing work.

> I mean the design, of course, uh, it's, it's kind of fundamental to the whole thing, I mean the thing about this is, like, so it started with a very simple idea of the Tor network. Of how to, which, OK maybe is not super simple, but, I shouldn't even call that simple, but at least the, you can describe the idea in a few sentences, what it does, let's say, in broad terms. But then the resulting work, you know, they have dozens of people working on it over many years, and… you know, and it turns out that you don't just have to fix the network, you also have to fix the browser in many ways, because even though the network is… protecting your privacy in one way, that doesn't help if you're not protecting privacy in all the other ways it can be lost. Uh, that's kind of the thing about privacy is that it's like you're securing a house, right, and you have to lock all the windows, you can't just lock some of the windows *laughs*. Um, so that's where the kind of initial design is not enough, because we have to constantly be going through and looking for, what are all the privacy holes, what are all the problems? What are all the sort of, like, corner cases and so on
>
> Participant C - Tor core developer

The practices through which this kind of work is done are far from the "structural" vision of design work, and involve systematically combing through edge cases, exhaustively testing how the Tor browser and network perform in a myriad different conditions and environments, and hardening and fixing tiny, subtle aspects of the implementation of Tor.

> Um, I also have another project in mind, that I haven't gotten to, where I want to go through every single [call in an API framework with which Tor interacts] and just manually go through every one of them, I think there's probably, you know, several hundred, um, and just see if there's anything we're missing. I think we're covering pretty much, I mean anything that people are using. I wouldn't be surprised, though, if there's something that we've missed. That everybody, kind of, has missed.
>
> Participant C - Tor core developer.
>
> Yeah. I mean my goals and the goals of the [Onion Service project] for the next, like, three months are basically just clean-up. Um, to reduce technical debt and… get things on a more solid footing in terms of testing and quality assurance, kind of like boring stuff *laughs*. Like, a lot of people want new features in [Onion Service project] and I'm just like "no, no, no" *laughs* "that sounds great, but we're not going to be doing that!" *laughs* Um, just because, you know, as we want to evolve things and move things forward, we need to make sure that the foundation is as solid as possible. And so we've spent a lot of time, and are continuing to do things like making sure that we have good test coverage, that the kind of cludgy bits of the code are rewritten.
>
> Participant X - Onion Service developer

This work is taken up by Tor developers working in a range of teams across the organisation, each specialising in a different part of Tor, such as the browser, the encryption protocols, or the network. Given the volume of this kind of work, this leads to a huge sea of micro-decisions which would be impractical to subject to full community scrutiny and debate every time, unlike the top-level design of Tor. As a result, these developers need a way of making these decisions in practice. Surprisingly, despite the "maintenance" nature of this work, the developers I interviewed did not view this through an *infrastructuralist* sensibility, but rather understood the salience of this work through the cultivation and curation of mutual trust, based around a shared set of values between the core members of the Tor Project.

> I guess that's where the values come in, because, you know, we have to trust eachother, that we're all doing the right thing in each detailed case, that we don't necessarily at all, I mean I don't follow every ticket on our ticket tracker, by any means. Uh, I follow probably one percent of the tickets, so all the other people who are working on other privacy leaks, like, basically I have to trust they're locking those windows when I'm locking this window over here. And so it's this general principle, we know, like… basically what are we all trying to do, we're all following that principle, to fix it everywhere. So I guess that's where the… *it's more of a value than a design thing then, in that respect, maybe*. Um, and that, you know, it's a fairly clear principle, I think, actually, for Tor. I feel like it's less clear for somebody like Mozilla, what are your guiding principles. I mean they have a list of them, but… those are sometimes competing with eachother, those values… So we're lucky, we're lucky in that way, maybe, that we have kind of a… a fairly clear purpose, I think.
>
> Participant C - Tor core developer (emphasis added)

This is deeply thoughtful explanation of how these decisions are made. It is important to highlight how this conceptualises the links between resilience and trust: the hidden, solitary nature of this work means that, as opposed to a 'structural' approach, these micro-design decisions in fact rely on a shared set of values and sense of community and purpose. This kind of trust and its role in resilience is very different to the 'trust-neutral' approach through which Tor's *engineer* rationality understands resilience – that through radical openness and decentralisation, no user of the system should have to trust any individual member of the Tor Project or relay network by design, or its sponsors or developers. It is also very different to the *infrastructuralist* perspective, which is deeply suspicious of any attempt to develop, assert, or even discuss a shared set of values for Tor, preferring to exist as an autonomous collective of individuals. This *activist* sensibility takes these hidden development practices, which are worked out through tedious, isolated, and systematic work, and connects them to a broader arena of values where they can be debated, disagreed-out, and linked to more political discussions. This means that these maintenance practices are seen not only as sites where the initial values and design of Tor are *maintained*, but active sites where they can be contested, reflected upon, and evolve with the organisation.

## Conclusion

In this chapter, I have taken the picture of the *materiality* of Tor's infrastructure (in both its human and technical components) and moved it beyond the perspective of design into the hidden work and resilience practices which allow it to realise its visions of privacy in the world. However, these practices are not simply vehicles through which the logics of design are realised, but also give rise to their own means of understanding Tor and its vision of the world. They are important sites at which values are performed and negotiated, and at which the worlds of Tor meet one another.

Tor faces a range of threats, ranging from the quotidian to the extreme, necessitating resilience design in the human and non-human elements of Tor's infrastructure. However, the 'structural' view of the engineer world, although worked out in meticulous and nuanced detail in practice, leans on ideas about the inherent primacy of open and decentralised structures, over others. In fact, realising these structures in practices involves a range of complex negotiations, balancing between different priorities, and conflicts in domains outside design. The hidden work which is required, both within the community and in working with the technologies of Tor, to realise these visions is vital to making sense of Tor as a site of social action. This hidden work draws not only on the *infrastructuralist* social world, as might be expected of maintenance practices, but in some cases also draws on the *activist* social world. This is reflective of the broader shifts within the social worlds of Tor, and the increasing prominence of the activist perspective, which I discuss in more depth in Chapter 6.

In the following chapter, I conclude the presentation of the results of my research with an exploration of the problems which Tor faces in practice in realising this vision, in particular, with crime, harm, and criminal justice. This uses the social worlds framework and the rich maps of Tor's meanings and materiality which I have

sketched across the course of the thesis to make sense of the problems with crime, power, and governance which Tor faces, and how it tries to navigate them.

# chapter 9

# allergic to onions? Tor, crime, power and harm

## Introduction

All Internet infrastructures and platforms, from Google, to Facebook, to internet service providers, face problems with crime. These problems arise from the different ways in which people use these platforms but are also shaped by the decisions made by the developers of these technologies at the design stage, the continuing processes of development and administration, and public perceptions of the technology. How these infrastructural organisations and platforms approach and make sense of these issues plays a crucial role in shaping the salience of these infrastructures to crime, power, and harm. In this chapter, I address my final research question, exploring the crime problems which Tor faces, the different ways in which it makes sense of them, and the strategies through which it attempts to navigate them.

Having mapped out the main social worlds of Tor, how they shaped its design, and the hidden kinds of work which allow Tor to 'perform' this design in practice, and to survive and thrive despite its powerful enemies, we are now equipped with a rich set of maps of Tor as a site of social action. These are a powerful resource for exploring other questions about Tor and its place in the world. In this final results chapter I bring these maps to bear on more criminological subjects. In doing so, I endeavour to demonstrate the value of a social worlds approach for criminological research on the Internet and its infrastructures, and for understanding crime and control in contemporary societies.

This chapter is divided into two halves. In the first, I discuss the problems with crime, harm, and criminal justice in which Tor becomes caught up when its attempts at 'infrastructural politics' meet the forces of power and control which they are trying to subvert. I begin with a brief discussion of how Tor has become implicated in online crime and harm. I then move onto the findings from my own research, exploring the ways in which Tor has become tangled up in the processes and mechanisms through which crime on the Internet is governed. I discuss the consequences which this has for the Tor community and the broader ways in which Tor plays a role in global power relations. In the second half of this chapter, I use my mapping of Tor's social worlds to explore the often-contradictory ways in which Tor attempts to navigate these issues, characterising in turn how the *activist, infrastructuralist*, and *engineer* worlds make sense of them and their strategies for negotiating this terrain.

## The Darknet, crime and moral reaction

The design of Tor explicitly attempts to frustrate mass surveillance. As I describe in more detail in Chapter 7, the design choices made by its developers, through maintaining low latency and designing out any opportunities for control over how people use it, make it a powerful tool for privacy-conscious citizens, activists and journalists, but also potentially for harmful and illegal conduct. Tor has become associated in the public eye with a wide range of use cases unintended by its original designers. The way that Tor builds circuits through its anonymity network is designed to protect user browsing information, however, Tor can be used not only to *access* web services anonymously, but also to *host* them anonymously through the creation of Onion Services . These websites are extremely difficult to shut down or censor, and can only be accessed through the Tor network. While this has obvious utility for journalists seeking to take submissions from whistleblowers or news organisations looking to circumvent censorship (with the New York Times, the BBC, and the Guardian all hosting Onion Services, and SecureDrop providing one as a platform for

whistleblowers), it has also been adopted by those looking to commit crime, access illegal materials, and trade in illegal goods. Tor has also received substantial media attention as a tool for organisation by terror groups and child sexual abusers, and for hate speech and other harmful conduct.

Where countries exercise an ethos of centralised state control of the Internet, Tor is often illegal, prohibited by legislation which often also criminalises the use of VPNs and other technologies. As of 2018, Tor was prohibited or blocked in Bahrain, Belarus, China, Iran, Iraq, Oman, Russia, Saudi Arabia, Turkey, Uganda, the UAE, and Venezuela. Russia notably made the news in 2017 for the imprisonment of an exit relay operator (The Register, 2017), and China has banned Tor use, engaging in a wealth of complex technical mechanisms to prevent people from accessing it. Blocking Tor is in principle easy for nation states: a list of all Tor relays is published online, and so they can simply find these and block them. Tor implements a wide array of circumvention technologies to get around this, including bridges, which provide alternative, secret routes into the Tor network, and pluggable transports, which disguise Tor traffic as other kinds of signals.

In 2014, journalist Jamie Bartlett published a book with the title *The Dark Net: Inside the Digital Underworld* (Bartlett, 2014; Gehl and McKelvey, 2019). This documented the rise of, among other things, the early cryptomarkets, anonymous marketplaces for illegal goods and services hosted on the Tor network. This was part of a wave of media accounts which brought Tor to the attention of the public in a form which was far more easily communicated than the technical complexities of anonymity networks. The deviant connotations suggested by the name 'Dark Net' and Tor's radical ability to undermine surveillance even by nation states online proved irresistible for narratives about online crime, conjuring an image of an online demimonde (Maddox, 2016). Depicted vividly as a 'Wild West' in which hackers, paedophiles, terrorists, and drug dealers operated with impunity from law enforcement, Tor became a proxy for broader anxieties about the internet, with many of these depictions echoing anxieties about the rise of the Internet circulating

in the 1990s. The rise and fall of the Silk Road, a particularly prominent illegal anonymous marketplace for drugs hosted on a Tor Onion Service, was reported widely in the press, along with romanticised descriptions of its owner, the self-styled Dread Pirate Roberts (Munksgaard and Demant, 2016). This has led to stories in the press and political statements which seek to whip up popular sentiment about criminal activity found in Tor Hidden Services:

> The so-called 'dark-net' is increasingly used by paedophiles to view sickening images. I want them to hear loud and clear: we are shining a light on the web's darkest corners; if you are thinking of offending, there will be nowhere for you to hide.
>
> David Cameron, UK Prime Minister, 2015

Criminological work has largely followed this characterisation, focusing on cryptomarkets and crime rather than the broader implications of anonymous browsing, censorship circumvention, and liberal challenges to authoritarian trends in internet governance. As a result, the term 'Dark Net' has now become synonymous with online crime in public discourse, used both to refer to Tor and other anonymity networks, but also as a general term for crime online, encompassing even illegal activity which occurs over the regular internet rather than Tor. This association with crime has caused problems for Tor, putting off new users who could benefit from its protections, causing problems for its relay operator community, and dissuading potential funders who would allow it to move away from US government funding.

In more recent years, the counter-narrative to this depiction of Tor has emerged more strongly, framing Tor as a potent moral force in condemning and resisting mass surveillance. Since the Snowden leaks (Lyon, 2014), the alleged interference by Russia in the 2016 US election (Mueller, 2019), the Cambridge Analytica scandal (ref), and a range of other widely-reported cases (Cadwalladr and Graham-Harrison, 2018), the harms associated with surveillance by governments and social media platforms have become equally the focus of public scrutiny. This has given Tor an opportunity to reframe its public image. Tor is an increasingly important actor in these debates, on the frontlines of the struggle between attempts to control

cyberspace and attempts to liberate it, between anxieties about harm and order, and anxieties about authoritarianism, control, and exploitation.

## Tangling-up in technologies of control

Tor's developers aim to redistribute online power, 'flattening' the topologies of the Internet and its technologies of control through its design. In reality, when Tor comes into contact with these technologies of control this does not occur smoothly. While Tor is remarkably effective in achieving anonymity and censorship circumvention for its users, it faces a number of obstacles in practice. Even in nations which do not criminalise or block Tor, it experiences consequences for its attempts to subvert control. This amounts to a kind of *partial* or *indirect* criminalisation which stems from its entanglement in the administrative processes through which nation states and private companies attempt to govern the Internet. Tor has little effect on governments' attempts to carry out physical targeted surveillance, to intercept packages, or to cultivate human intelligence, and has similarly little effect on the way in which Facebook and Twitter monetise the personal data provided willingly by their users. Rather, it aims to subvert a specific mechanism of control: the mass-scale tracking, surveillance, and censorship of populations. Tor's tangling-up in these mechanisms both protects its users and brings with it this partial criminalisation. This occurs in two main ways: firstly, through action by non-criminal justice actors who have been devolved responsibility for governing parts of the Internet, and secondly, through the ways in which Tor comes into contact with policing investigations.

The first technology of control in which Tor becomes entangled lies outside the formal criminal justice system. The primary rule enforcers for online conduct for most of the Internet's history have not, in practice, been the police, but the infrastructure providers who maintain the technologies of the Internet (Gillespie, 2010; Kohl, 2013). Chief among these are the owners of large-scale platforms such as Facebook and Twitter, and Internet service providers who manage users' Internet

access. The view which Internet service providers have of the Internet is an essentially administrative one. They run banks of servers which host web sites and services, manage requests from users of the Internet, and keep extensive records of all of this activity. This makes them the first point of call for the various automated complaints generated when users of the Internet illegally download copyrighted films, send abusive messages, or commit other kinds of crime online. For traffic originating from Tor relays, these complaints are then served to the operators. This generates what can be a large amount of tedious work for operators responding to complaint notices, and has been a problem for Tor since its early days:

> I came home today to find a rather unpleasant e-mail sitting in my inbox. It was a DMCA Complaint from the MPAA, for "CHRONICLES OF RIDDICK, THE". I scratched my head for a few minutes, trying to figure out if I had downloaded that movie on my server. I was really quite sure that I hadn't downloaded it, or any movies at all. I wondered if they might have misidentified a legitimate torrent. Then it dawned on me - with the recent talk about BitTorrent over tor, it probably was someone using BitTorrent over tor… I'd very much like to continue running a tor server, but I can't afford to do it if I'm going to receive DMCA Takedown notices. Has anyone else had this problem? Any suggestions?
>
> Tor-talk mailing list, 2004
>
> Lately, more and more, systems are set up to send out notifications if there was some kind of [hacking] attempt like scanning all ports or scanning URLs for like, the typical exploit stuff… So when there's filesharing stuff happening, you are required to reply, and that could mean, basically what we do is, is respond and say sorry, we can't identify the customer. So, last time I looked we get a thousand DMCA complaints every day… Um, but a lot of ISPs don't like that workload, when they see a lot of these emails. And they are not really happy about putting you in the abuse contact, because they don't know how you will deal with the more severe cases.
>
> Participant L - Tor core contributor

Once these build up, this becomes a nuisance for Internet service providers. IP addresses, the identifiers which allow information to be routed around the Internet, are in fact a relatively scarce resource. A proliferation of abuse complaints by a relay, if not properly handled, can lead to the blacklisting or banning of many of the IP addresses held by the Internet service provider. This can result in either the relay operator's accounts being punitively banned (and the loss of paid subscription money for the operator), or even the implementation of wider policies prohibiting

relay operation with that service provider. As a result of this, relay operators are finding it increasingly difficult to find ISPs who are willing to host a Tor exit node.

> It can generate flak *laughs*. And, I mean, my basic idea is, my basic position is, and always has been, is it's none of my business what people use their Internet access for. Right? They want to run a Tor node, they want to do, you know, whatever *laughs*… that's my basic position, but there's two caveats with that. One is, you don't do things that harm the ability of other people to use the network. And you don't do things that cause me excessive work *laughs*… Uh, and running a Tor exit node will get… first of all, if that's what you're doing, because, it will generate complaints and things, and I need to be able to respond to these complaints, so, I should know, let me know, right? Um, ideally, deal with your own complaints.
>
> Participant U – Tor relay operator and ISP sysadmin

> So there's different kinds of ISPs, right? You know, residential ISPs, I would be surprised if any of them liked [Tor relays] at all. Right? … So you'll more want to put them in places where you can… rent a server, co-locate a server, something like that. Now those providers are going to be worried about the reputation of their addresses. What they don't want is to get on blacklists and things, and sometimes the blacklists can be a little bit heavy-handed, and you might suffer collective punishment, and they might say, well this entire [range] of addresses is going in the blacklist, and not just this one address that's a Tor exit node… And that's a risk. I mean, addresses are scarce, you don't want them to become unusable, because that means the people adjacent to you have trouble using the network, right? So that sort of breaks that rule of causing other people problems. It's manageable if the ISP knows what's going on. They have to know what's going on and also be willing to do the extra work to manage it. And whether they are or not…
>
> Participant U – Tor relay operator and ISP sysadmin

The second technology of control in which Tor becomes entangled is the formal investigative processes of criminal justice systems. This is the result of rule enforcement against Internet crime more generally, rather than directly targeted action against Tor. In particular, the operators of the "exit" relays described above face substantial exposure to law enforcement action in practice. Tor provides privacy for its users by obscuring the administrative traces of Internet browsing, requests to visit particular sites or speak to particular people, from law enforcement and Internet service providers. The consequences of this for the relay operator are that these administrative traces become associated with them, rather than the user. When a police officer or intelligence analyst is investigating crime online, they rely on these administrative records: they go to the Internet Service Provider, request the

records, and follow the trail of suspicious activity back to the user who appears to have made the connection. If the offence is serious then they may request the details of the rest of their browsing history and communications. Equally, as policing the Internet becomes increasingly automated, and algorithms scan for attacks, requests to illegal websites, and other criminalised activities automatically and flag up suspicious patterns, Tor relays can appear to be particularly potent generators of these patterns. To anyone who looks through the administrative records, it appears that every abusive, illegal, or unpleasant action undertaken by Tor users has been committed by the person running the exit node. For a Tor relay operator, this can lead to substantial difficulties, including arrest and seizure of equipment:

> Because the moment where, kind of, if there's a small police, law enforcement office somewhere and they get an IP address and they ask the ISP who was the customer who was using that IP address, and then they get a customer record, and then some small town policemen go and get some small town court to, say OK, and they come to your door, it's already too late. Like, you have to kind of sit back and allow them to, basically, take all your hardware, and then later argue that there's enough proof that you weren't related to the crime.
>
> Participant L - Relay operator
>
> It is actually a terrifying experience. Um, I wouldn't wish that to my worst enemies… They wake you up, at five minutes to seven in the morning, after, with my sleep cycle, I'd had two hours of sleep that day… And then, uh, ding-dong, welcome… we have a… search warrant, yes, that's it. Um, and they're standing at your door, with four people, and once you open the door, there's a foot in the door.
>
> Participant W - Relay operator

A number of my participants reported having some level of conflict with law enforcement as the result of running an exit relay, and most of the relay operators identified it as a source of anxiety for them. For one operator, involved in a particularly high profile case which involved an attack on critical national infrastructure, this had particularly serious consequences.

> In my case [a major company], classified as "vital importance company" in [my home nation] (but apparently without any basic security practices...), was infected by [a ransomware virus] After infection, [this virus] try to contact its [command and control server], which is a Tor hidden service. So infected machines starts a Tor client, which connect to guard nodes to established Tor circuit to the [command and control server]. After infection, the IT service flag all outgoing traffic as evil, and

> complaint to [law enforcement] about hacking. 24h later, [all of the] guard nodes joined by an infected computer was seized by the [law enforcement agency]. The main problem is [law enforcement] ask for a gag order around my case, and I officially have no information at all of what are charges against me or what I risk on this case. No warning at all. Machines vanished without reason a Sunday morning, no information from my provider during two days, before agreeing to tell me that I had legal action against me.
>
> Participant T - Tor relay operator

Tor's design disrupts a particular set of strategies employed by law enforcement in controlling crime online. It is crucial to emphasise that these law enforcement processes are not directed actively at Tor. Rather, they are the result of the particular administrative traces generated by a Tor relay and how these become entangled in criminal justice attempts to take enforcement action against online crime more generally. By shielding its users from these processes of enforcement, Tor itself becomes subject to the disciplinary power wielded against their illegal online activities. This has a number of consequences for the Tor community.

## Stigma and the tarnishing of the 'free Internet'

In many ways, Tor has been quite successful at resisting mass surveillance and mass censorship on behalf of its users, but, as I describe above, it faces a number of challenges in practice. In this section, I outline the consequences of these for Tor. The threat of law enforcement action is a particularly worrying issue for Tor. Relay operators employ a wide range of strategies to avoid this, which I describe in more detail in a subsequent section of this chapter.

Despite these mitigation efforts, smaller or less experienced operators can still receive a lot of unwanted attention. Recent police raids on a relay operator organisation in Germany suggest that anxiety over police action may be well-founded even where mitigation efforts have been attempted. Although there has been a lack of successful prosecutions, this can result in substantial stigma for the people involved:

> Even if… once you've had a police raid for child porn, that's, you can't burn your name more than that. Something always sticks.
>
> Participant W - Tor relay operator

> I have some people asking me "Hey, some weeks ago you told about Tor Browsers and something, what are you doing there? Are you buying drugs, are you buying guns?" And I told them, no – I was looking for some alternative, uh, news and I visit some websites, I don't want to leave any footprint. That's my reason I'm going there. And they all asked "Huh? I thought myself it's just for buying guns and abusing children!" and I said to them "no! it's just an Internet without Google and Facebook."
>
> Participant Q- Tor relay operator

Even for those who claim to brush this off, it can still lend a "deviant" air to Tor, which undermines its self-image as a force for good:

> It feels like you're wearing an Anonymous mask and it feels like you're doing a little… you're a bad guy. That's the feeling when going there, yeah… It's more an excitement. It's like being in your car and, know you are going a little too fast now or something. It's like, it's like having a joint, going to the park and smoking, yeah?
>
> Participant Q - Tor relay operator

This stigma, and the broader association of Tor (and hence, themselves) with crime, are a problem, as relay operators and the network itself rely on not being culpable for the content of the communications which their Tor nodes carry. Combined with the administrative issues with ISPs, this produces a sizeable barrier to running the valuable exit nodes on which the network depends. As Internet hosting becomes more centralised, with smaller providers coming under the auspices of larger corporations, they are increasingly bound to follow restrictive policies as these corporations are less sympathetic to the complaints generated by Tor nodes. In practice, this means that a lot of exit nodes are concentrated around a few cheap and tolerant hosting providers. There is speculation within the Tor community that this may have ultimately dire consequences, making it possible for hostile actors to shut off large parts of the Tor network by targeting a relatively small number of providers.

> So OVH is a French company, has, uh lots of European data centres, and they have very, very cheap virtual servers. Um, so there's lots of fast, fast relays, but they're all

> in the same network and this isn't really adding any diversity. Even though there's maybe four, five hundred people running them, um, they're all, maybe even in the same rack. Which is *laughs* sub-optimal.
>
> Participant D - Tor developer

As an attempt to realise a particular vision of the world, it is problematic for Tor if others, such those who use it for illegal or harmful activities, or those who wish to paint it as criminal, attempt to subvert this. Similarly, its use for harm, especially deeply emotive issues such as child sex abuse imagery, terrorist organising, and racist hate crime undermines the utopian vision of the society it is meant to be creating. This stigma limits the growth in Tor users, and hence the spread of its vision of the world. Its tangling up in mechanisms of control only compounds this, adding further stigma and association with crime.

While Tor's reputation as the 'Darknet' is a problem for attracting more users and funders, it is largely ignored by the people in the relay operator community, who view this as scaremongering. What limits the size of the relay network and the resilience of its infrastructure in practice are these ancillary mechanisms of tangling-up: the secondary, administrative consequences of Tor becoming implicated in illegal activities. All-in-all, this amounts to a weakening of the Tor network, rather than full criminalisation. This is one way in which the politics-through-infrastructure imagined by Tor's design meets challenges in practice, spilling over into other domains separate from the power structures built into the design of the Internet, such as public opinion and fine-grain mechanisms of administration and enforcement. But this tangling-up not only occurs where Tor conflicts with mechanisms of internal state power, rather, it also happens at the points of concordance at which Tor's vision of the world and that of powerful nation states overlap.

## Broader stages of power

Tor acts not only on power relations and technologies of control within nation states, but also between them, in the terrain of global power (Moore and Rid, 2016). Tor becomes tangled up in these rather differently, becoming implicated in questions of geopolitics and sovereign power in ways which may illuminate further why most liberal democracies (and the US in particular) have largely not attempted to formally criminalise its use. Tor was originally developed by the US government's Naval Research Laboratory and has received substantial funding and expertise throughout its life from the US state. As well as fulfilling its original purpose to allow field agents in hostile nations to communicate with their handlers over the regular Internet without raising suspicion, its broader adoption around the world potentially operates in the interests of US soft power.

In this framing, Tor (much as the Internet more generally) becomes one of the many efforts made by the US globally to spread its culture, way of life, and model of society (Nye, 2004). By broadening access to information and communication, Tor allows the everyday citizens of more 'closed' societies access to the global internet without censors' determining what information is fit for them to consume, and allows political dissidents, freedom fighters, and activist groups to communicate and organise. It is therefore no surprise that the nations which have attempted to formally criminalise or block Tor are largely more authoritarian states with adversarial relationships with the US. Some extremely powerful actors with little interest in preserving the right to privacy have set up sites on Tor, with the Onion Services set up by Facebook and the CIA perhaps the most telling examples of these attempts at the co-option of Tor in the interests of existing power structures. This contradiction is keenly felt by Tor's developers:

> I think one of the main challenges at the end of the day is that the incentives of private companies are oftentimes not necessarily that much aligned with the incentives of the public. And so it's sort of hard to push for something that is going to significantly damage the business model that they are based on. So I think… the sad truth is that in the end, on the Internet, unfortunately, still the prevalent

> business model is based on advertisement. And advertisement depends on being able to collect as much personally identifiable information as you can, from everybody. So… I mean, sure, Facebook has made an important step in terms of… you know, running their own Tor Hidden Service... but I'm… I'm not sure that is necessarily that much of a big win, in terms of the information that they still are able to gather and collect about them and how Facebook uses this.
>
> Participant H - Tor core developer

This is, oddly, an area in which Tor's vision of the future and that of the US government have historically overlapped, with the Internet cast as a force for liberalisation, breaking down the barriers between nation states, facilitating free trade, political organisation, and freedom of expression. As abortively realised in the discourse around the Arab Spring, there has long been a tendency within US global policymaking circles to have faith in the capacity of the Internet to play a role in exactly this structural redistribution of power which Tor seeks: moving societies from 'closed' to 'open'. While the developers of Tor are very much alive to this critique of their infrastructure, they also accept that many of their own visions of Tor's role in the world overlap with this 'democratising' sensibility.

> I think some Tor people maybe disagree with this view, but… so, one of the things that Tor gets its funding for is helping dissidents in countries with repressive governments. Like, Iran is an example. And… I actually agree with the idea of doing this, and it can sound a little, maybe… colonialist, and I see that point of view, but on the other hand we're not forcing anyone to use this tool. This is a tool for individuals and an individual anywhere in the world is allowed to use it, so I'm quite enthusiastic about, let's say, translating it into whatever language, Farsi or whatever. Localising it for people from… whatever country, and so that's part of our funding, and it comes from the US government. And I think it's a valid thing to do.
>
> Participant C - Tor core developer
>
> I think there are for sure some common principles… but at the same time trying to not get too much into those that are complex socio-political issues in a particular country and trying to, sort of, balance that, so that we can ensure that those that give colour, in a way, to the things that we promote are actually the people that are from that country, that have a better understanding of what is happening there.
>
> Participant H - Tor core developer

This presents a somewhat counter-intuitive but crucial challenge for Tor: it needs a way to distinguish its vision of the Internet from that of the US state, and prevent itself from being co-opted as a technology of power.

## Navigating crime and power as a rebel infrastructure

Having set out some of the main issues of crime, harm, and power which Tor is facing, I now explore the ways in which the Tor community makes sense of this 'crime problem', and how they attempt to navigate it. Each of Tor's social worlds frames crime and harm rather differently: in my interviews, adopting different strategies to deal with it. As will be seen, these strategies are often opposed and mutually-exclusive, which is reflected in the often-conflicted way in which Tor has attempted to deal with these issues over its history.

Most Internet infrastructures have three avenues in which to engage in dealing with crime, harm, and abuse of their services. The first of these is the route of design, making changes to the design of the technology in order to shape its affordances for its users and the kinds of action and interaction which are possible. This is effectively an 'online' version of Situational Crime Prevention techniques, making changes to the built environment in order to alter opportunities for criminal offending, or to increase possibilities for guardianship (Reynes, 2010). There are many examples of this, including automated detection systems which scan messages on social media platforms for hate speech or child abuse images and remove them, systems for collecting information on users' real identities, and more subtle changes which can be made to the user experience to 'nudge' people away from abusive or illegal behaviour (see for example, Reynes, 2010; Pothineni, 2014; Blackwell et al., 2017; Suzor et al., 2019; ).

The second approach involves moderation and administration, including a range of techniques through which platforms directly police user behaviour. Many platforms make use of moderators and administrators to handle abuse reports, make decisions about suitable sanctions, such as posting restrictions or exile from the platform, and some adopt a more community-based approach, with moderation of norms and conduct left up to particularly well-established users. These processes effectively set up internal policing and governance mechanisms and systems of sanctions for the

users of the site through which behaviour is observed (by automated systems, paid administrators, or community members) and unwanted behaviour sanctioned.

Finally, as I discuss in Chapter 8, platforms can engage with the formal institutions of law enforcement and criminal justice. This involves storing and collecting user data which can be used as evidence in investigations, the establishment of reporting mechanisms where illegal behaviour is detected, and either replying to subpoenas for user data or, on occasion, developing more active collaboration regimes with secret services (Lyon, 2014). As revealed in the Snowden leaks, and as has become increasingly prominent in discussions about the operation of contemporary criminal justice systems, this kind of collaboration has only been deepening, with some exceptions where companies, such as Apple, have tried to assert the rights of their users against state intrusion (Schulze, 2017).

Tor, however, has deliberately limited its ability to engage in any of these. Its design deliberately removes any of the control points through which user behaviour might be surveilled, and its foundational design decisions, based around maximising the number of use cases in which it can be employed, all seek to design out control rather than designing out crime. This is both as a matter of principle, and to prevent the people who run its infrastructure and design its code becoming targets themselves. By extension, it has also 'designed out' its ability to administer or moderate user behaviour to a large extent, and this, and the anti-authoritarian sensibility of its community, makes collaboration with law enforcement both a technical impossibility (as the infrastructure collects no useful data on its users) and escheded as a matter of principle. This makes it a particularly interesting case to study. In the following half of this chapter, I explore how issues of crime and harm fit into each of Tor's social worlds, and the strategies which arise from these ways of understanding these problems.

## Privacy as a struggle: the *activist* world and reclaiming Tor

For much of Tor's life, the Tor Project has avoided making strong public commitments to a particular set of values other than a dedication to privacy, preferring to frame the technology itself as neutral in order to permit the widest possible community of contributors and users. This in fact goes back to its original design, when the US naval researchers who developed it envisioned it as enrolling the largest and most diverse possible user community to provide effective cover traffic in which US military agents could disguise themselves. The rise of the activist social world, however, has caused a reorientation of this strategy, and Tor has become much more engaged in public discussions about the values it represents.

The *activist* world views privacy as a struggle, and privacy technologies as part of a political movement for civil rights, wielding political power, and embodying a coherent set of values of their own. Asserting these values in public is therefore, for this world, an important way in which privacy technologies exert power and shape societies.

> Tor is not just software, but a labor of love produced by an international community of people devoted to human rights… We advance human rights by creating and deploying usable anonymity and privacy technologies. We believe that privacy, the free exchange of ideas, and access to information are essential to free societies… We are not just people who build software, but ambassadors for online freedom. We want everybody in the world to understand that their human rights -- particularly their rights to free speech, freedom to access information, and privacy -- can be preserved when they use the Internet… Our vision of a more free society will not be accomplished simply behind a computer screen, and so in addition to writing good code, we also prioritize community outreach and advocacy.
>
> Excerpts from the Tor Social Contract

The problems of crime which technologies face, accordingly, are also framed as stemming from questions of public image and perceived values. In this framing, technologies like Tor attract crime problems (and the attention of the criminal justice system) when they become associated with crime and deviance, and legitimate users become dissuaded. Hence, they feel that Tor's reputation as a 'Dark Web' full of illegal content is the prime factor in shaping its use for crime, and if it becomes

known as a tool for free speech and liberal democracy it is likely to attract a wider range of more positive use cases. Promoting Tor's socially beneficial use cases, and encouraging more journalistic organisations to set up Onion Service versions of their websites is a large part of this effort at changing Tor's image. The activist social world is also the only one of Tor's social worlds which is occasionally (though not always) willing to condemn Onion Services outright, arguing that they pose too great a risk of abuse, unlike Tor's capability as a browser.

> I'm not really a fan of onion services myself. I think it's nice from a technology point of view. It's nice if you can think about systems, and that's kind of the classical thinking that I was used to before all this public visibility. That kind of, the technical community accepts that it's currently all crap, and all shit happening on the Darknet. Because it's technically so neat… I'm not sure that just because there are potential worlds where Hidden Services would save the planet, um, it's maybe not the world we live in.
>
> Participant L - Core Tor contributor
>
> I think it's an absolute disaster… Tor's public perception has been really bad… I think the most important thing they could do is, like, rebrand, and have a decent PR person… like, if you look at it from the outside, it feels like some underground, dodgy, like, drugs trading thing. My really specific recommendation to them is to separate Hidden Services, because this whole, like "Dark Web" bullshit has come about from the fact that Tor enables Hidden Services, means that Tor gets lumped in with Silk Road. And that's not helpful, and I think the Tor Browser could really do with a rebrand… Tor Browser is about browsing without censorship.
>
> Participant R – Tor advocate and relay operator

This conceives of privacy technologies as possessing substantial power to act as moral agents, shaping public debate and influencing policy and legislation. The activist strategy is to engage directly in these public debates, making explicit cases for Tor as possessing intrinsic political values, and being intended for particular uses and political causes. In doing this, they seek to reclaim Tor as not about crime, but about control, itself at the vanguard of a wave of moral reaction against mass surveillance and authoritarian attempts by powerful groups to control the internet. By engaging in these public conversations, they attempt to get governments, institutions, and public opinion on their side. This involves promoting particular positive use cases of Tor, making the case that Tor 'isn't about' the cryptomarkets

and illegal pornography (and arguing that this represents a very small percentage of Tor's actual users). Rather, they claim that Tor was designed for a particular set of intended uses – namely, for journalism, human rights work, and the protection of everyday internet browsing from mass surveillance.

> You need to be working out how to present the good use cases along with the bad ones. Um, I think they're still learning as an organisation how to do that, they've not really had to do that for the last decade, because they've had a bunch of government funding, and they've been able to tailor it to what they want to do. Now that they're more reliant on people and outside organisations for funding, well it looks like it's going to be that way, especially in the next few years, they have to get better at selling the technology as a whole to society.
>
> Participant Z - Tor Onion Services developer

As a result, they articulate a vision for Tor which is rather different from the neutral status Tor has asserted over the years, or the structural change through engineering imagined by its designers. This world of discourse is more likely to accept publicly that harmful uses of Tor are a problem, and to condemn particular use cases of Tor, especially those which are associated with crime or the far right:

By explicitly allying Tor with other social movements, such as women's rights, LGBT liberation, civil rights, they attempt to ensure that the social meaning of Tor becomes steered by its community and *reclaim* Tor's values. They do this by promoting particular use cases, allying with particular causes, and partnering with the particular groups which the activists choose to train in how to use Tor. This has the advantage of empowering Tor to use its substantial clout in lobbying for privacy as a political cause, and shaping public perceptions of Tor to improve its image. This, however, faces problems in practice, clashing with *infrastructuralist* sensibilities in the Tor community who are both unused to acting in the domain of public discussion, and deeply suspicious of associating technologies with an explicit politics.

## Privacy as a service: the *infrastructuralist* world and becoming invisible

These attempts to assert Tor's values and engage in public debates over the politics of privacy come up against the strategy on which Tor relied for much of its life: to assert itself as a neutral facilitator of the actions of its users in order to build as broad a community of contributors as possible. This sensibility is particularly embodied in the *infrastructuralist* world, which stems from the various practices of maintenance, network administration and invisible work on which the Tor network relies, giving rise to an ethic of "privacy as a service". In contrast to the value assertions of the *activist* world, the *infrastructuralist* world aims to denude Tor of explicit values, withdrawing it from public conversations about politics and social meaning as much as possible.

This perspective baulks at the assertion that Tor it should take any view at all on the particular types of things for which it is used. The majority of the relay operators whom I interviewed felt this way, often comparing Tor with a knife or similar tool, with no intrinsic politics or values. This amounts to an assertion of 'technological neutrality', the argument that technologies themselves possess no agency, and are mere conduits of human action.

> It's like, *sighs* it's like having a knife – with a knife you can cut an apple and with a knife you can kill a man… so the Tor network is just a knife which is laying on the table without anyone touching it. That's my opinion.
>
> Participant Q - Tor relay operator

> Because the tool is something that does, something that helps you to do something. But what you will do with this tool is up to you. Crime happens not on the hard drive of the Bond movie producer, crime happens not on the Silk Road drug store, no. Crime happens inside people's mind. The criminal mind is a way of thinking. It's actually confirmed even by psychiatry and medicine. Some maniacs have special genetic markers or special protein markers that these potentials can be identified from just a newborn child. It's true… Neither Tor or other software authors, nor people who are running even exit nodes, no they're not responsible. They are not responsible for another people's thoughts and actions. They are not. Tor is just a tool.

> Participant N - Tor relay operator and open source contributor

This framing has a practical purpose. While Tor is not explicitly criminalised in many countries, it does become entangled in criminal justice processes, which brings it into conflict with the technologies of control through which states maintain online order. This is primarily experienced by Tor's relay operators, as I describe above. These practical concerns and risks, and the intrinsic distrust of politics of this world, leads them to a set of strategies which I characterise as 'making Tor invisible', a powerful set of tactics for enabling Tor to sit under the radar, and untangle themselves from the criminal justice processes which put them at risk. This resonates with hacker sensibilities about oppositional technologies, using clever tricks, loopholes and creativity to slip the infrastructure of Tor through the cracks and edge cases in the law and police procedure, rather than attempting to change people's minds through political debate:

> Problem: immunicity takedown. Solution is to do the exact same thing without "encouraging an offence". Answer: let people choose their own websites to proxy… Problem: Internet Connection Records. Solution: An unsurveillable ADSL connection… Answer: overlay network out of the operators control… Problem: ISPs take down Tor exits because they are scared of abuse complaints. Solution: Be your own ISP… I'm a professional problem solver, government attempts at controlling the Internet is a problem. As I've said many a time: I can innovate faster than they can legislate.
>
> Participant S - Relay operator

To mitigate the problems with administration and law enforcement I describe above, relay operators cultivate a range of practices which attempt to allow them to slip between the cracks. Prospective relay operators are advised to avoid running a Tor relay from their home connection, instead setting it up in a datacentre on a rented server. These servers tend to be clustered within countries and service providers who are sympathetic to Tor, don't bother to ban nodes over abuse complaints, or have jurisdictions where investigating foreign cybercrime cases is not a police priority. Although successful prosecutions are rare, especially as Tor provides a service which allows investigators to establish proof that the traffic originated from their Tor relay, rather than their personal computer, operators understandably try to

avoid getting caught in this process to begin with. For ISPs who host Tor nodes on their network, the experience with law enforcement is very different:

> The NCA contacted [the Internet Service Provider we run] and said, preserve this Tor node! *laughs* It used to be the case that whatever police, wherever, that was dealing with a thing would like, oh, it's an Internet thing, I'll call the ISP and not really understand what's going on, and ask them for ridiculous stuff. Now, that kind of communication needs to be funnelled through the NCA. And they have a group, a specialised group that understands how the Internet works, and what Tor nodes are, and these sorts of things, and so you know… that's good. Right? Because, I mean, it means that when you do, as an ISP, at least, interact with law enforcement, you're interacting with people who know what they're dealing with … Like, literally, the only contact I have had with them is on that kind of level, where somebody is doing something bad on the Internet, oh, it's a Tor node, oh, OK, we know what that is, we'll… go find evidence some other way! Right? *laughs* Um, and that's kind of the way it should be.
>
> Participant U - Tor relay operator

> We need to advocate companies and ask them to run more exits by covering costs (infrastructures, bandwidth...) and troubles (abuse, seizure, law enforcement requests...).
> Exit nodes are currently too risky for a single person without a structure (company or association) above.
>
> Participant T - Tor relay operator

As a result, Tor's relay operators have attempted to mitigate this threat through the cultivation of fairly sophisticated mechanisms to de-intersect Tor from the particular parts of these administrative processes which result in trouble for its operators, while keeping it interposed between the users and state technologies of control.

Relay operators draw on the classic hacker techniques of social engineering to shape the way Tor appears to the world through the use of what relay operators call 'legal entities'. Tor's operators have realised that having a relay in their own name operating from a home internet connection appears very different to less technically-minded police than a relay owned by an Internet Service Provider hosted in a private datacentre. Accordingly, Tor's exit operators often set up small companies or charitable organisations which they register as a service provider and use to host their relay. This means that when police look up an IP address associated with illegal activities, they find what appears to be a company providing hosting for

its customers, rather than an individual's home connection. For the relay operator, this is the difference between a dawn raid for child pornography charges, including the seizure of computers and a potential court case, and a polite letter informing them that one of their customers has broken the law. Relay operators are now actively advised by the Tor Project to avoid running an exit relay on their home connection, and a range of organisations exist which can help new operators get set up safely.

> That's why we always try to teach everyone to get them listed in the whois records, so you are not the end user, you are not the customer, but you are looked at as an intermediary."
>
> Participant L - Tor core contributor

> When I run an exit, I want it to be owned by a legal entity that's not me. And that's for the risk of it being, if someone uses that, when someone uses that exit for something bad, and some police investigation happens, which unfortunately might happen, I want the chain of, I want it to go to the company that owns it, and then at least it'll mean that they'll ask a question before they bash my door down…. I want it to be obvious when a police investigation is happening that this is a proxy, and so incorporating it is essential for me – I'm not going to run it in my own name.
>
> Participant R - Tor relay operator

Tor is designed specifically to preclude any mechanisms for censorship on the basis of content, allowing Tor to take advantage of laws which offer 'mere conduit' protections, and absolving them as service providers from responsibility or liability for the actions of their users. This legal and moral neutrality is very important from the people who run the Tor network, given the content which flows through their servers. The reality of Tor is that as well as providing substantial social benefits, it also facilitates (as is common with any infrastructure) a range of activities which are unambiguously harmful. Although the relay community justifiably defends their decision to help Tor, they do need ways to reconcile this tension, and the stigma it brings. This makes taking a view on user traffic of any kind is dangerous, preferring to recuse themselves from any moral judgement or articulation of Tor being 'about' one particular use case or another.

> Under European law I am not allowed to alter the packetflow. As long as I am pushing packets from A to B I am protected as a ISP. Would I like to kick the botnets out? Yes! Am I allowed to do this? I don't think so.
>
> Participant P - Relay operator

Adopting this way of understanding provides them with a way of coming to terms with this reality. The more diverse groups which use Tor, even including the police, or those who use it for criminal purposes, the more its relay operators feel they can abrogate responsibility for the traffic which flows through and maintain their 'neutral' status: as soon as they begin to take a moral view on this traffic or try to shape how Tor is used, they risk becoming culpable. The dissonance at the heart of this understanding, which tries to square a deep distaste with over politics with the explicitly political act of running a Tor relay, is reflective of the complex ways in which Tor becomes implicated in structures of power.

## Privacy as a structure: the *engineer* world from subversion, to standardisation, to sovereignty

The foundational social world which underpins the design of Tor and the core of its attempt to "do politics" through architecture is that of the engineers. This engineer world began with the researchers and developers who first set out Tor's design, and views power as a function of the topology of technical networks. They see the design of the internet, in particular, the traceability of internet traffic, as concentrating power in "choke points" in these systems, and privacy technology as flattening this terrain of structural power. When its attempts to reshape this power run into challenges in practice, Tor's engineer world has its own distinct understanding of these issues of crime, harm, and control, and its own strategies for reclaiming Tor's vision of the world.

From this perspective, conversations about the crime, deviance, and harm with which Tor is associated are a red herring. Their understanding of these concepts

mirrors that of critical criminologists such as Box (2002), arguing that "crime" is in fact constructed and enforced by and in the interests of the powerful, designed to distract the public from real questions of power in society. They see crime and harm as an unfortunate but unavoidable consequence of disrupting these vested power interests - rather than promoting positive or negative use cases, Tor works in the interests of those without power over those with power.

> It's kind of a bit like MP3, where you say, OK, society might not be ready yet and we will kill a lot of stuff and, and… video killed the radio star! And it's like, technology comes first and then there's a struggle in society on how to restructure itself to be able to cope with that change. And I think a lot of the hacker ethos is about seeing what would be possible with technology. And, and seeing that there's all these forces that drag down the change, because they want to survive… All these structures are becoming more and more stale and static and, and, uh, the only way to change them would be to break them. And I like fluid systems. I like, this kind of structurelessness and, and chaos, and I think that's a value by itself, and… maybe that's the way to go, is to build these systems and then say, OK, maybe we will be fucked for thirty years because of these systems, and everything will go to shit, but afterwards we will rise again and a new society will evolve that is much better than the old one! I don't know.
>
> Participant L – Tor core contributor

> If Tor were to go away tomorrow, the bad people would not really be inconvenienced very much… I think the only people who'll be significantly inconvenienced by the lack of Tor will be the, the relatively vulnerable people who aren't able to run their own network, and they'll be the people who don't want to break the law. So, I think, in that sense, Tor is, is overall positive. Um, regardless of how people are actually using it.
>
> Participant F - Tor core developer

*Engineer* discourse is not as anti-policing as might be expected, and in fact many expressing this perspective were in favour of the use of targeted police powers to tackle crime. What it opposes is the adoption of engineering and architectural solutions for social control. They argue that policing through automated mass online surveillance is a dangerous and authoritarian centralisation of power to the state and the unelected software developers who build these platforms, and that social issues should be tackled through democratically-accountable institutions.

While the *infrastructuralists* seek to master administrative processes in order to de-intersect Tor from them so that they can run it smoothly, the *engineers* seek to undermine the strategies of control more fundamentally through disruptive technological innovation. Tor began as an attempt to 'fight fire with fire', using the same engineering techniques to redistribute this power back to everyday Internet users. As I describe above, however, they soon find that these engineering design techniques promote change in unexpected, unpredictable ways, and run into problems in practice. Tor's performance of these values relies on people using it and it working smoothly: its negative public image, association with crime, and tangling-up in criminal justice processes undermine its practical attempts to redistribute power. As a result, the *engineer* world adopts a range of strategies to steer Tor's efforts and reassert its attempts to "do politics" through architecture.

## From subversion to standardisation

This entails a conceptual move from subversion, creating a technology which undermines mechanisms of control for its users, to standardisation, fundamentally shifting the way that the Internet itself works. Rather than slipping Tor through the cracks in the criminal justice system, this involves trying to get Tor "built in" to other technologies, a toolkit for developers rather than only a tool. This has the benefit of reframing Tor's crime problems as consequences of a broader shift in the dynamics of power embedded in the Internet, rather than the result of an upstart activist technology. Tor was designed with this in mind from the beginning, much like the Internet itself. Many of Tor's core design decisions (such as allowing it to browse the regular internet) are aimed at enabling these interfaces with other technologies, and there is a substantial degree of work undertaken by the Tor Project in convincing other developers to make use of Tor in their own platforms.

> Part of [the work we are doing], does… just as a side thing, kind of, integrate Tor, and Onion Routing, and Onion Addresses more into the everyday… I see Tor and Onion space right now roughly where… web encryption was around, like 2001 or so.

> You know, back then if you, if you set up encryption for a webpage, people said, you know, what are you doing, this is, are you kidding me? You know, what are you trying to hide, this is, what kind of criminal thing do you have going on? And now it's recognised as the fundamental enabler of e-commerce... you know, ideally [in the long term], I'm out of a job, or doing something else, because this is [now] just the way the internet works.
>
> Participant I – Tor core developer

Particularly successful examples of this are the Onion Toolkit, developed by Alec Muffet, which allows anyone to easily set up an Onion Service. Onion Services (and the Tor relay network) are a key tool for developers and researchers for whom anonymity is important, and have also been built into chat messaging apps such as Ricochet and Cwytch. The whistleblowing platform SecureDrop is another example of an Onion Service technology, which has been widely used by news organisations to take anonymous submissions. Tor has become a go-to tool for security researchers who research adversarial websites as it allows them to collect information without being blocked or revealing their location.

Most importantly, Tor has also begun to try to get incorporated into other browsers, with Brave Browser recently integrating Tor into its private browsing mode, so that its users can access Tor in their browser with the click of a button. The much more widely used browser Firefox (which has 250 million users) is considering a similar move, in the meantime incorporating a range of Tor's security improvements and anti-tracking technologies. As Google increasingly becomes known for its surveillance operations, competitors to its Chrome browser are increasingly using privacy and anonymity protections as a distinguishing feature.

> Yeah. They're not all these, these drugs undergrounds. Like, the majority of them are these ephemeral things that are just in the background. And I think we're going to start seeing a lot more of them as Tor is sort of built into things in ways where you don't even know it's there… , I think this is where Tor is heading towards… things where Tor is more of a security toolbox, where you can pick and choose which features you want, um, which makes it a lot more applicable to a lot more use cases, um, and I think this is, this is what's needed to get Tor into everything as the… the underlying technology for communication.
>
> Participant D - Tor core developer

This normalisation, in this framing, would entail a reorganisation of social power which, though disruptive, would shift the ways in which power is exercised over the Internet outside the domain of mass surveillance of traffic. External factors may in fact make this more likely. A core reason that strong encryption became the norm for online technologies (despite much resistance from the US government) was not only due to the tireless campaigning work of activists, but also to the enormous security benefits which this offered to online banking and commerce. The increasing preponderance of high-profile cyberattacks and breaches against corporations, and the rise of connected homes and Internet of Things technologies, could well lead to the protections which Onion Services offer being increasingly in demand. These attempts to extend this "politics through architecture" beyond Tor itself do not only rely on engineering, however. The efforts of Tor's activists to improve Tor's public image, and of the infrastructuralists to smooth the practical realities the Tor network faces in running day to day, are both important factors in convincing the developers of other technologies to incorporate Tor into their infrastructures and platforms.

## From disruption to sovereignty

As well as its unfortunate public association with crime and the ways in which it becomes tangled up in criminal justice processes, Tor also faces challenges to realising its vision in the domain of power. This involves co-opting Tor rather than undermining it. While Tor's success in becoming a security standard is still in its initial stages, far more evident has been the growth in its users since it launched in 2002; on average, (at the time of writing) two million people now use the Tor network every day. As Tor has grown as an infrastructure, it has increasingly taken on responsibility for a global population of users the size of a small country. Tor has the power to shape the way the internet works for these users, but much of its design reflects the sensibilities and decisions made by a group of largely American engineers around the turn of the last millennium. These developers, alive to the increasingly critical turn in information security research, have engaged in the past few years in

substantial efforts to critique and understand their own place in the world and the power they wield.

Features of Tor's security design, the languages in which it is available, and the usability properties of the browser all shape who is able to actually make use of it in practice, and how it shapes their action. As Tor is a powerful technology for political actors, if its design favours one group in a conflict over another (for example, groups with a knowledge of English, or who have the technical skill to use Tor) then its developers may be making unintended interventions in power struggles. Equally, Tor has the capacity to be co-opted as a potent tool of US soft power, opening up citizens of authoritarian countries to American media, Internet platforms, and news. Leaving Tor's moves in this domain up to chance, or up to others who may have less-positive motivations, opens it up to become simply another tool of power. The growing awareness of this has led to a shift in how the *engineer* world conceives of its attempts to "do politics through architecture":

> I think that's a valid argument against Tor. That no matter how much you try to educate people to be able to use it, ultimately you are supporting the power structures. Because only they can understand and teach it. It's like… you have all these organisations that teach other organisations about encryption and how to use it. But someone is paying them, right? Someone is deciding what kind of opposition groups they will teach. They can make the decision themselves, maybe. Um, but ultimately someone has to make that very political decision. Of who will be trained to be able to use that. And in that sense, then Tor becomes a weapon against those that just don't know how to use it, right?
>
> Participant L - Tor core contributor

Tor is partly navigating this challenge through a reframing of its core values, and an increased engagement in active public discussion of what it represents, making the case for its view of the world as a set of explicit political positions. At the same time, debates around the governance of online space have shifted, and the sensibilities of the information security community have become more attuned to the political character of their work (Rogaway, 2015), so too has Tor's own role within these discussions changed. Since the Snowden leaks, the alleged interference by Russia in the 2016 US election, the Cambridge Analytica scandal, and a range of other widely-

reported cases, the harms associated with online surveillance by state actors and social media platforms have become the focus of substantial public debate (ref Coleman). This has given Tor an opportunity to reframe its public image, repositioning itself at the frontlines of the struggle between attempts to control cyberspace and attempts to liberate it, between anxieties about harm and order, and concern with rising authoritarianism, control, and exploitation. From a technology largely happy to frame itself as a neutral facilitator of the actions of its users, Tor now increasingly acts as a potent moral force and value-led community in condemning and resisting mass surveillance.

Tor's engineers increasingly believe that if they are to avoid this, they need to actively assert control over these more subtle design considerations which shape and support the lives of the people who use it. This in itself poses a serious issue, forcing them to reckon directly with the power they themselves wield over their user community and work out ways of democratising this. There is a substantial knowledge barrier to participating in Tor's development, and online privacy and security needs (and the concepts of privacy and security themselves) are very different for different people. Privacy and security are shaped by gender, race, sexuality, and social class, and are constructed differently in different cultures and situations around the world: the private protections which an abuse survivor, an activist in Iran, an LGBT person in Scotland or a videogame enthusiast in China require from Tor may differ enormously. Tor's engineers frame these more nuanced issues of design through the idea of usability:

> When I wrote my first email to tor-project as ED nine months ago, we were finalizing a long phase of work to bring a new user experience to Tor users. We put together an ambitious project to meet our users where they are to learn how to improve Tor for them. Every team inside of Tor did something to improve their users' experience…Making Tor easier to use for our dedicated user base was a big step for us, because it required the creation of an iterative feedback loop that centers the user at every step of our development process. This has fundamentally changed how we work with one another as a team and community, improved usability for our core users, and set us up to prepare Tor for mainstream adoption.
>
> Tor executive director, post on Tor-project mailing list, 2019

Unlike other web browsers, Tor cannot collect information about its users through surveillance as a matter of principle, and so democratising Tor's design properties has involved a substantial degree of outreach and user research around the world as part of an enormous recent usability improvement campaign, which has included the redesign of Tor's website and browser. These attempts to cultivate knowledge about its users and incorporate their lives into Tor's design constructs them as subjects of Tor, staking a claim over them and invoking *usability as biopolitics*, cementing Tor's status as an alternative site of authority and power. As might be expected, some who are particularly aligned with the infrastructuralist community have baulked at this shift in focus, arguing, for example, that changes to the website to make it more accessible to non-technical users are 'dumbing down' Tor and attempting to influence how it is used, rather than maintaining neutrality. This has been, however, a minority view.

As I describe in more depth in Chapter 7, an important result of this usability drive has been a reframing of Tor's user categories around particular "user journeys" and "personas" which are reflective of those users of Tor who may have been poorly-served by its design in the past, but whom the Tor Project feels are important to bring into design considerations. This constitutes both a genuine desire to democratise the Tor's infrastructure, but also in itself creates category systems and frameworks of representation which shape Tor's users and exert a form of subjectifying power. This is an important consequence of how the engineer world in Tor is attempting to deal with crime, and forms part of this assertion of sovereignty, the claim that Tor is in some important ways outside the purview of nation state control. This is also important in showing how the engineer world and the activist world have shaped one another, and how the boundary objects which supported Tor's détente between worlds are shifting. These tentative changes to aspects of Tor's user categories are reflective of a desire both to be more assertive over who and what is represented by Tor, while retaining the engineer concerns with power and structure.

## Conclusions

In this chapter, I have used the maps I have developed across the course of the thesis to answer more criminological questions about Tor and how it is coming to terms with its responsibilities for the governance of crime. While the issues of crime which Tor faces are the subject (almost to the exclusion of all others) which has received the most criminological attention, research has tended to focus on exploring the kinds of crime which Tor is used for and its affordances for criminal opportunity. Conversely, my research aims, through a more appreciative study of Tor itself, to understand the role of Tor itself as a place where visions of crime and its governance are produced.

Tor's use for crime has brought with it a number of problems for the organisation. Despite attempts to assert 'technological neutrality' in the past, the association with crime has brought with it a host of image problems for Tor, to the extent that it is now widely known as the "Dark Web" or "Dark Net". This deviant labelling is not only self-fulfilling, putting off legitimate use cases and encouraging illegal or harmful ones, but also harms Tor's efforts to grow and access funding outwith that provided by the US government. Secondly, it has brought the infrastructure of Tor into contact with the technologies of control through which the Internet is governed, and Tor's relay operators risk being caught up in criminal justice processes despite the fact that they are largely not breaking the law. Finally, Tor has become implicated in power on a geopolitical stage, and its potential for use as a technology of disruption and US soft power brings into question how, and by whom, its role in global society is being shaped.

All three of Tor's social worlds are heavily engaged in dealing with crime and its consequences. Practices of design and development, image management and administration are all implicated in how Tor is trying to deal with crime. None of these actually attempt to stop Tor being used for crime, rather they attempt to change other things: the activists try to encourage more socially beneficial use, the

infrastructuralists attempt to mitigate some of the problems which this criminal use causes for the operation of the network, and the engineers work towards the standardisation of Tor as a set of logics, standards, and protocols which can be worked, in part or in whole, into other technologies, eventually so ubiquitous that it becomes part of the fabric of daily online life and so cannot be constructed as a 'crime problem'. Each of these also entails the realisation of their social world's vision of privacy: the activists see this as realising a world where privacy values are taken more seriously by people and the national conversation on privacy is won, the infrastructuralists see the maintenance of a service which can be used by anyone for anything, and the engineers envision the wholesale structural transformation of relations of power through changing how the Internet works. Hence, as ideas about privacy are inherently bound up with ideas about power, governance, and control, they also necessarily shape how Tor deals with crime and harm.

The next chapter draws from across the thesis to fit these results into a broader view of Tor, the history of the Internet and the research literature.

# chapter 10

# discussion: technologies of power and the power of technology

## Introduction

Having set out the main findings of my thesis, in this chapter I discuss my results and their implications for criminology, STS, and digital society scholarship in depth. In doing so, I draw connections across and between my findings chapters (Chapters 6-9), pulling out the main points and contributions and fitting them back into the literature and key debates which I identify in Chapters 2, 3 and 4. Bringing all this together, I outline my explorations of the four research questions which I set out in Chapter 5:

1. What are the key social worlds of the Tor community, how do they relate to one another, and how do they come into conflict, conversation, and collaboration?
2. How do these social worlds shape the material form and design of Tor; how are these values realised as properties of the Tor network?
3. When this design is materialised as infrastructure, what other kinds of work are needed so that this infrastructure can create Tor's visions of privacy for its millions of users, especially given the considerable opposition it faces?

4. What problems with crime, power and harm arise when Tor begins to realise its visions? How do the social worlds of the Tor community make sense of these issues, and through what strategies do they navigate them?

One of the main findings of this thesis is that Tor is not characterised by a single vision of the world, but rather is composed of three distinct social worlds. These worlds are united by cypherpunk values which place privacy at the heart of realising the transformative potential of the Internet. However, these values are refracted into distinct framings of how privacy technologies constitute sites of social action and how they link to power and politics. These three social worlds package up particular practices, sensibilities, rationalities and perspectives about a range of issues. These hence constitute distinct 'visions' of privacy in Tor: the *engineer, infrastructuralist,* and *activist* social worlds, each of which involves attempting to act in one of three distinct domains. I describe these in depth in Chapter 6, but they can be summarised respectively as 'privacy as a structure', 'privacy as a service', and 'privacy as a struggle'.

An interesting and unintended aspect of these worlds is that they correspond roughly to the framings of technological political action attested by each of the three main researchers whose work I used to contextualise this thesis in Chapters 1 and 2 (something which I only realised late in the writing-up of this research): Coleman, Musiani, and Milan. Coleman (2017) is interested in the hackery, creative, often politically-agnostic world of hackers, Musiani (2012) investigates how developers try to do politics through restructuring the architectures of the Internet, and Milan (2016) understands these groups through the lens of social movements. Although a social worlds approach engages with these framings at a much lower level, exploring how different ways of making sense of technology are worked out in relation to Tor itself and its community, I draw out in this section some tentative links to these broader perspectives. Considering these different kinds of action together rather than separately shows how they influence and shape one another, how they conflict, and how the tension between them drives Tor as a site of social action. This gives us

substantial insight into the often-contradictory and contested ways in which Tor engages with the world.

Rather than simply drawing these social worlds from my research interviews and presenting them as a static map, they are in fact best understood when grounded in the history of Tor as an organisation. Mapping the early history of Tor and its design (as I do in Chapters 3 and 7 respectively) brings to the surface the 'non-linear' relationship between Tor's values and its material form, and hence between the different research questions I address in this thesis and the picture of social action which they depict. As such, this chapter does not attempt to reckon with the four core research questions of this thesis individually, rather, it draws them together into five sections framed around particular themes and findings of interest which sit across these questions. Maps of some of these relationships can be found in Appendixes E and F.

I begin with a discussion of the role of design across my results as a mediating process between meaning and materiality. I then expand this picture to the hidden work of Tor which helps to realise this design in the world, and which becomes caught up in the processes of criminal justice. Next, I discuss how Tor's social worlds have changed and shaped one another over time, and the relevance of this for how it deals with crime and power. In the fourth section, I draw these together to explore how Tor fits into wider questions of power, governance and geopolitics in contemporary societies. I reflect in a fifth and final section on what the social worlds framework might offer for criminological understanding of the Internet and its infrastructures, arguing for a programme of 'infrastructural criminology'.

## Designing privacy

The first theme I explore in this discussion is the role of design: the links between development practices, Tor's values and vision of the world, its material properties, and the broader consequences of these for crime and governance. Although this most directly addresses my second research question, in fact, as I discuss in this

section, it plays an important role in all four. Placing this design and the values it embodies in their historical context by tracking how they emerged and where they came from is crucial to making sense of Tor as an infrastructure and a site of social action.

Tor's precursor, the Onion Routing project, brought together two distinct social worlds: those of the US Naval researchers and the cypherpunks. These worlds fused together in the Onion Routing design, with the remnants of these two precursor worlds each providing one half of the shared category system of users at the heart of Onion Routing. It is this category system, which distinguishes between high security users and those seeking everyday privacy, which allowed the three main social worlds of Tor a common point with to bridge together and collaborate. The cypherpunk and military researcher precursor worlds, along with a host of other practices, discourses, abstract theories, sensibilities, frameworks, and values then went on to become the engineer world through the process of shaping Tor's design. This social world's vision of privacy views battles over privacy as inherently about battles between structures: open systems versus closed ones, centralised versus decentralised systems, and flattened topologies over those structured around control points. This vision of social action through technology corresponds most closely to the perspectives reflected in Musiani's (2012) work, through which engineers and software developers shape societies through the logics of structure, attempting to decentralise power through a technical fix to the Internet's design.

As I describe in Chapter 7, this view of Tor developed through an iterative tacking back-and-forth between attempts to represent and reason about the system and its context, discussions of purpose and values, creative design work, and implementation; a gradual convergence between meaning and materiality rather than a linear progression from a set of values to a final design (Star, Bowker, and Neumann, 1998; Williams, Stewart, and Slack, 2005). As this 'Tor's eye view' of the world was forming in Tor's design, the developers were also performing a way of seeing and making sense of the world: a set of frameworks, representations, and

category systems which become stabilised in the infrastructure as a way of understanding *and doing development work with* Tor, embodied in the engineer social world. This picture of collaboration, consensus-building and fusion between distinct perspectives is a far cry from the 'agonistic' depiction of the creation of infrastructures in Actor-Network Theory, foregrounding instead the role of communication, interpretation, and practice (Latour, 2005; Star and Clarke, 2008). It is also important to note that the 'engineer' world of Tor isn't a social world common to all engineers and developers around the world. Rather, it is a set of Tor-specific discourses, category systems, and ways of making sense of infrastructure which stem from the coming-together of particular practices and values in the process of creating Tor. While it may have commonalities with the social worlds of the developers of other privacy technologies, other infrastructures, or computer scientists more broadly, it is in its specificity to Tor that it achieves its power as an analytic framework (Star, 2010).

Tor's disruption of the mechanisms through which powerful actors control and surveil the Internet and the high-risk nature of many of its users mean that its potential adversaries are extremely powerful, and potentially capable of attacking not only Tor as a technology, but the people in its community. As a result, Tor's design practices do not stop at the technologies of Tor, extending as well to the Tor community itself. This fits naturally into the engineer world's frameworks for making sense of human and social factors in terms tractable to engineering solutions. Their approach to security, threat modelling, and design extended the engineer world's representative frameworks and design processes to the human factors of Tor's community, reasoning about them as patterns in systems. As Milan (2016) argues, these community structures are reflective of both the values and visions of communal action of technical communities as well as the ideas, in this case of openness and decentralisation, embedded in the design of Tor. Once again, however, these designs work through structural paradigms, assuming the inherent primacy of decentralised and open systems over closed ones. Hence, *the structure itself and the value it represents are mutually constitutive*.

As Tor's developers were pulling together the engineer social world through Tor's initial design decisions and processes, they were also embedding a set of rationalities about crime and control within this social world and within Tor's design. Our maps of the engineer world and Tor's initial design decisions are therefore a useful resource for understanding parts of how it engages with issues of crime and harm. As I describe in Chapter 7, Tor incorporates a range of design decisions which play an important role in shaping its potential for criminal and harmful uses, particularly its low-latency design and the decentralisation of control which is built into the network. Tor's relatively high speed and the decentralisation of its 'trust-free' network across a range of volunteers aim to maximise its usability and minimise the trust which users need to place in the Tor Project to use it. This increases its potential user base substantially to include everyday users of the Internet, which provide the 'cover traffic' for Tor's high-security users. It also increases its potential for harm, allowing it to host marketplaces, share images and files, and be used for a range of other near-real time network applications. By removing the ability to control or surveil network traffic by design, the developers also remove their ability to police the traffic which flows over the network, or to hand it over to law enforcement.

Equally, the engineer construction of privacy as about structures of power in information networks has important implications for how the developers make sense of Tor's implication in crime and harm. Their view of crime and harm is focused on abuses of power: the establishment of relations of exploitation and domination over networks, and hence the people who use them. This conjures, through the engineer world, a vision of criminal justice and control as working through the establishment of control points in network topologies (see also DeNardis, 2014, for an academic framing resonant with this).Throughout Tor's life, as these forms of governance and policing have become increasingly prominent, Tor has become more explicitly a reaction to the increasing use of these technocratic solutions. Tor's engineer social world sees its relationship with crime and criminal justice as attempt to shift governance and control into other spheres of action which are more open to

democratic oversight. They believe, drawing again from this structural view of social life, that moving towards governing societies in this 'structural' domain inherently takes societies along a path towards authoritarianism and dystopia. In a reversal of traditional Situational Crime Prevention approaches (Hayward, 2007), Tor attempts to 'design out control' through technical changes to the built environment of the Internet, rather than 'designing out crime'. In practice, it does this extremely well, reliably decoupling the administrative information which allows signals to navigate the Internet from the identity of their users and pushing law enforcement to fall back to more traditional approaches which don't rely on mass-scale surveillance: human intelligence gathering, targeting offline distribution networks, and targeted surveillance.

Practices of design are implicated in all four of my research questions, forming the underpinnings of one of Tor's core social worlds (my first research question), shaping Tor's material form (my second research question), forming an important part of Tor's 'resilience work' (my third research question) and setting the context for how Tor comes into contact with issues of crime, harm, and power (my fourth research question). Studying Tor's design, the values of its developers, and the processes through which the two converged gives us a very 'pure' depiction of Tor as a site of social action and the vision of privacy which it attempts to realise. This gives us a window into the underpinnings of Tor's attempt to 'steal the fire' through creating infrastructure (Milan, 2016). Rather than a unidirectional 'translation' of a vision of privacy into material forms, the very processes of design and development through which Tor was created were themselves important factors in shaping the values its developer were trying to embed in it: how the Tor developers themselves make sense of concepts like privacy or crime. The 'architecturalisation' of social concepts like privacy, control, and crime which I document in Tor's design work, rendering them in terms tractable to engineering solutions, is reflective of what Musiani describes as "doing politics" through architecture (Musiani, 2012). My research places design within Tor's attempt at technological activism not only as a vehicle for the realisation of values, but as a way of making sense of the world in its own right.

However, as I argue in the following section, Tor's status as a site of social action cannot be understood through design alone.

## Hidden work and hidden worlds

Hidden work plays an important role in Star's infrastructural studies scholarship, a key part of what makes infrastructures work and a home for important but neglected perspectives (Star 1999). While Musiani focuses of the hidden work of design, in fact, development work is some of the most visible in Tor. Rather, the values, visions and structures which these design processes embed in Tor rely on a range of yet-more hidden practices to be realised in the world. In this section, I explore these forms of hidden work. As with my discussion of design in Tor, although this theme focuses directly on my third research question it ties into the others as well, as hidden work in Tor contributes to its values and visions in important ways, plays a key role in how Tor's values are materialised, shapes its infrastructure, and is one of the primary sites at which its interactions with crime, harm, control, and power are worked out in practice.

As Tor began to grow, the maintenance and administration work of its infrastructure became vital to its continued success, allowing the network to function reliably and hence to materialise Tor's vision of privacy for its users. The administration of Tor's infrastructure cannot be carried out by the developers, as this would create a single point of failure, an easy target for adversaries, and be too great a centralisation of power. As a result, this vital work which allows the vision of the world embedded in Tor's design to become a reality is carried out by Tor's large community of volunteer relay operators. The relay operator community, unlike the developers, largely do not know one another, functioning as an 'autonomous collective' whose members are only united by a belief in privacy. Keeping this hidden work hidden, so that the infrastructure runs without friction for its users and blends into the background (or as Star terms it, achieves 'transparency') is a key part of how infrastructures work

(Star, 1999). This is equally true for the design ideas which touch on Tor's community structures, and many of these elements of resilience design in both the community and the technologies of Tor in fact require hidden work and careful negotiation and management to successfully 'perform' these designed-in structures (as I discuss at length in Chapter 8).

While it is interesting to note that Tor relies on hidden work, this is not a hugely productive finding in itself, as this is a common characteristic of infrastructure (Star, 1999). Rather, what is important is exploring the character of this work and how it shapes Tor in important ways as a site of social action. Despite the extremely diverse politics and motivations of the relay operator community, I found that they drew on a common way of understanding Tor as a site of social action which was rather different to that of the engineers. As I discuss in Chapter 6, this hidden work gave rise to a distinct set of sensibilities and practices of its own, and formed into what I characterise as the infrastructuralist social world as the relay operator community grew. This world is steeped in the practices of system administration and maintenance, rather than design or engineering. When refracted through these practices, the cypherpunk vision of privacy at the heart of the Internet becomes one of 'privacy as a service', with the role of the infrastructure being as a neutral enabler of the political action of users rather than a political actor in its own right. Although this work is hidden, the infrastructuralist sensibility has played a major role in shaping Tor's public life for much of its history.

This way of understanding privacy, as a service which enables the action of others, is partly a response to the particular situation of Tor and the need for the people who run its infrastructure to come to terms with the often illegal or harmful content which their relays serve. The substantial stigma which this, and the law enforcement action to which exit relay operators expose themselves, incurs is important in shaping the infrastructuralist social world, as the operators need to come to terms with the sometimes harmful or illegal content which their relays carry. This is one potential explanation for this world's sensibility of deep suspicion, bordering on

outrage, towards asserting Tor as political. However, this is not only a 'neutralisation' (Sykes and Matza, 1957): it is also a self-consistent position on Tor as a site of social action, and one which resonates with classically liberal sensibilities about a 'free market of ideas'.

Tor not only comes into contact with crime and harm, but also with the technologies of power through which the administration and governance of online crime and conduct are managed. The social worlds approach, in bringing these hidden forms of work and perspectives into view, gives us powerful ways of exploring what happens when the material forms, practices, and visions of the world embodied in Tor meet those of the dominant technologies of power which its design attempts to undermine. Although the engineer world sees this as a clash of structures, with the logics of Tor's decentralised, privacy-protecting topology coming up against the centralised structures of the Internet and doing battle, when Tor comes up against the Internet's technologies of power, these conflicts spill into other domains. Although Tor's design aims to separate identity from routing information, it achieves this through an infrastructure which needs to be maintained and administered. While Tor's infrastructure effectively produces this 'flattened' structure of power for its users, it itself sits on top of an Internet with a well-defined topology of power and control, in which these control points very much still exist. The traces of illegal or harmful activity which Tor separates from its users do not disappear, and as such the administrative and investigative processes through which the 'structures' of control are enacted (and hence through which the Internet is policed) are brought to bear on the Tor relays and their operators.

Tor can't design its way out of these problems as they aren't tractable to engineering solutions. Instead, this shifts the conflict out of the domain of network structures and design, and into that of administrative practices. Through experimentation and the cultivation of expertise, the Tor relay operators have developed a shared set of resources and practices which aim to cleverly disentangle themselves from these processes of online enforcement. This involves properly arranging administrative

information, siting relays tactically at sympathetic or hard-to-reach providers, finding clever loopholes and edge cases, and exploiting the dynamics of police investigation using 'legal entities' in order to allow Tor to slip past these processes without scraping up against them. It also involves more prosaic practices of administration, where relay operation becomes like tending a Bonsai tree: dealing with complaints properly, applying updates, and regular maintenance. This all contributes to a distinctly 'hacker' sensibility, though refracted through processes of system administration rather than coding, giving rise to a peculiarly 'hacker values'-infused ethic of 'service provision' in the infrastructuralist world.

The commitment to 'political neutrality' which is bound to this ethic of service provision also resonates with what Coleman (2004) describes as a 'political agnosticism' in Open Source hacking communities. This frames this as the result of the articulation of cultural liberalism through the logics and rhythms of hacker practices, and an analogous social process appears to be occurring in the formation and enaction of the infrastructuralist social world (Coleman and Golub, 2008). The infrastructuralist world is, in fact, a distinctly 'hacker' instantiation of cypherpunk values. Although framed through practices of systems administration rather than coding, the problems from law enforcement and other forces of control which Tor faces has led these administrative practices to take on a rather 'hackery' form, based around finding clever edge cases, social engineering, and experimentation. As an interesting parallel between the infrastructuralists and Coleman's hackers, the experience of law enforcement action and opposition from powerful state actors is an important factor in the development of a 'political' sensibility in the infrastructuralist work of Tor as well (Coleman, 2017). In this case, however, it causes them to double down on their construction of their social action as politically neutral, on which they insist with the vehemence of a deeply-held political conviction.

That this work is so grounded in the idea of neutrality, yet motivated by such political sensibilities about privacy says a lot about the ability of privacy to appear to be a

'neutral' concept when it in fact packages up deeply political values. Part of what makes this possible is that privacy in this case is being produced through infrastructure, and this technological housing makes it easier to cast deeply political social facts such as not only privacy, but also crime, as devoid of politics. This has historically been an important tactic used not only by Tor, but by other Internet platforms and infrastructures to offset questions about the crime and harm in which these become implicated. While this infrastructuralist sensibility has contributed to a broad-church community for Tor, the tolerance for working across ideological boundaries which this 'neutrality' mandates relies on shared understandings of Tor as a site of social action, and where other social worlds attempt to assert more fixed understandings of Tor's politics, it begins to break down.

Administration and maintenance are key practices through which power and values are enacted. Changing the world through architecture and realising the values and visions present in a design requires a lot of supporting work: power doesn't just operate in this structural dimension, but is realised by a range of other practices. While this hidden work is crucial in realising the values embedded in Tor's design (research question three), it also gives rise to a particular social world of its own, shaping the visions of privacy and the Internet which characterise the Tor community (research question one). As it materialises Tor's design and privacy properties for its users, the infrastructure of Tor also becomes an important site at which the problems of crime and their consequences manifest themselves, itself coming into contact with and navigating the control structures of the Internet and the technologies of power through which it is governed (research question four). Many of the problems which Tor faces from powerful actors aren't even deliberate attempts to frustrate Tor. Instead, they are the consequences of the fact that even though Tor can create this 'surveillance-free' Internet for its users, *the infrastructure of Tor* needs to sit on top of an Internet which still has these control points and topologies of power, so they become directed at Tor itself.

These forms of hidden work are therefore important places where Tor's visions of society and ideas about crime and harm are worked out, and an important part of how social facts like privacy, crime, control are 'produced' from Tor's design. Equally, this means that democratic scrutiny of technologies and infrastructures and how they shape social life cannot be limited to their design features (though these are undoubtedly important). While a wide-ranging literature argues that the design of these infrastructures are important sites where power is enacted (Winner 1999; Lessig 1999a; Musiani 2012; Coleman 2012; Milan, 2016), in addition to these, the forms of hidden maintenance and administrative work are clearly important sites of power as well, where the logics and visions in these design elements are realised in practice. I argue that these kinds of work are therefore also important forms of social action, and also deserving of scrutiny.

## Transforming worlds and the sovereign Onion

The map of Tor's social worlds which I sketch across the course of this thesis is not a static one. Rather, as I show in Chapters 6, 7, and 9 in particular, although the three main social worlds of Tor still exist, they have changed substantially, as has the relationship between them. As new kinds of work have become necessary throughout Tor's life, Tor's values have been refracted through the logics of these different relationships with infrastructure and different forms of technological practice, giving rise to new perspectives which exert their own shaping forces on Tor. For much of its life, Tor's approach to questions of the politics of privacy technology was one of 'productive ambiguity', strongly influenced by the need to square these conflicting understandings of Tor. As Tor grew (much as with other major online platforms), this affected neutrality provided a useful cover for dealing with the inevitable issues of crime and harm which accompanied its partial disruption of the technologies of control through which the Internet is governed. The rise in prominence of the activist world has begun to change this approach. It has also

begun to shape and influence the other worlds as well, holding as it does a range of skills and strategies which are more well-suited and comfortable in engaging in the discussions about values and politics with which Tor is increasingly confronted. In this section, I discuss the rise of the activist world, how the social worlds of Tor have changed and shaped one another, the implications for this for how Tor navigates its implication in crime, and how this has begun to shift Tor into a new era.

The growth of Tor and its adoption around the world has given rise to a host of 'problems of success' with which the engineer and infrastructuralist perspectives have been ill-equipped to deal. In particular, its association with crime and harm has been an increasing problem for Tor as it has grown. While asserting 'technological neutrality' may have worked for much of Tor's life, this has begun, as it has for other platforms, to cause a host of PR problems which impede Tor's attempts to grow and provide its protections to more people around the world. Tor's association with crime and reputation as the 'Dark Web' puts off potential users who might benefit from its protections, and as the organisation attempts to diversify its funding away from reliance on the US government, also harms its ability to raise funds from organisations and through crowdfunding. This is another way in which Tor's action in the domain of design 'spills out' into other domains: this time the domain of public perceptions and political values. Fortunately, the wave of contributors with a more activist sensibility and skills who have joined Tor in the wake of the Snowden revelations are more well-equipped to deal with these issues of public image and conversations about organisational values, and Tor has been far more willing to engage in these debates in the last few years. This activist social world is most reflected by Milan's (2016) characterisation of technological social action, tied directly to values, and framing privacy technologies as part of a social movement. It explicitly attempts to pull the hidden design and maintenance work of Tor into this sphere, pulling the values and visions inherent within Tor to the surface where they can be engaged in public debate.

The confluence of the three social worlds of Tor means that Tor is reliant on three distinct and contradictory ways of making sense of its construction of privacy and social action. In particular, the activist and infrastructuralist worlds give rise to directly contradictory strategies and sensibilities, arguing (respectively) for asserting and denying Tor's values and politics. The work of these worlds is not siloed, rather, they all need to work with one another. This has been successful because of key translators who have been able to bridge these worlds and do boundary maintenance work, aided by the establishment of privacy as a boundary object as I describe in Chapter 6. However, as these worlds have worked together, they have also shaped one another, and due to changes in the broader context of Tor, this détente, too, has evolved.

When I was carrying out my interviews and finishing my analysis, I had already alighted on the construction of Tor's users as a shared core between Tor's social worlds which allowed privacy to function as a boundary object between them. While Star (2010) argues that changes in social worlds often necessitate the creation of new boundary objects or the transformation of existing ones, I was yet to observe any transformations in the core 'everyday users and high-security users' category system at the heart of Tor's design and its community's understanding of their user communities. I did observe, along with a shift in the engineer world to a more critical understanding of their own power to shape the world, changes in engineer design practices associated with the increasing maturity of Tor as a technical project and the increasing wealth of information about users and adversaries which was becoming available. In particular, a major drive towards making Tor more usable and carrying out substantial global research into both its current users and those non-users who might benefit from it the most has been underway for the last few years. I predicted that as the social worlds of Tor shifted, so would the framing of the user categories at the heart of Tor's détente between its worlds, and the new push for usability research appeared to be a herald of exactly this change.

In the final months of writing up this thesis, I found that the outputs of this user research, released in a set of five preliminary 'personas', appeared to confirm that this category system (and hence, the boundary object at the heart of Tor) was beginning to change. This constituted the beginnings of a category system of ideal-type users, intended to both shape Tor's communication efforts, but also to feed into the ongoing processes of development. The content of these is clearly and explicitly value-driven, a statement of Tor's own values and perspectives as well as an attempt to be representative of its global user community. This constitutes a powerful critique from within of the limited nature of Tor's existing category systems, representing groups of people who may have been excluded from these in the past and envisioning constructions of privacy beyond those of the white Western tech elite. Tor's attempts to represent its users are part of a broader acceptance that Tor, as an infrastructure, itself is and must always be a site of governance. This means that rather than becoming the very kind of technocratic platform they are trying to disrupt, they try to democratise the power of design by bringing their users into these processes. The force of infrastructural power from an infrastructural studies approach (as I use here) is in the category systems which become embedded in these infrastructures, how they are enacted through the materiality of the infrastructure and the hidden work on which it relies, and how they subjectify populations and create outsiders who don't fit into these categories, those who, to appropriate Star's phrase, may be 'allergic to Onions' (Star, 1990).

Drawing a Foucauldian framing of power into these questions of usability is useful for understanding this dimension of infrastructural power. For the surveillance capitalist giants, this user research is more obviously a technology of governance: the collection of vast amounts of information in order to shape platforms around their users, to know them more intimately, to appropriate and exploit this knowledge for power and financial gain, and to shape them as consumer-subjects. As Tor turns to more critical understandings of its own power, its attempts to gather information about and characterise its users reflect exactly this kind of subjectifying power, imagined in the service of a very different set of governmental rationalities. That is

not to say that this does not itself create outsiders. As Star (1990) argues, where the category systems embedded in boundary objects change, they always also exclude. In fact, as this is linked to Tor's reckoning with its use for crime, these new category systems are likely to render its criminal users as outsiders, as people looking to buy drugs and guns on Onion Services, for example, are unlikely to find a place for themselves in Tor's user research publications. In blending the activist and engineer worlds to shape Tor's design around particular desired user categories and values, this is effectively an assertion of a form of infrastructural 'sovereign' power.

Although STS scholarship often frames the work of mapping or tracing infrastructure as surfacing hidden work, what is posited as the essentially hidden nature of this infrastructural work is not always a given. In fact, many of the aspects of maintenance and design in Tor are brought to the surface in more or less deliberate ways. Infrastructure inescapably has a politics, and where it becomes implicated in crime or control, it also often becomes something for which a case needs to be made. Pulling different kinds of work, material forms, people, and distinct facets of Tor in or out of visibility is a deliberate and political act in which each of these groups are engaged, and constitutes an intervention in power relations in its own right. Sometimes Tor's infrastructural work becomes visible in ways which damage the project, such as when it becomes entangled in criminal justice, whereas at other times, the developers and activists pull the hidden design work of Tor to the surface in the interest of democracy. The idea that the work on which infrastructures depend is hidden until it breaks down, therefore, places too-great an emphasis on transparency (the idea that this work is invisible to users) as a key component of infrastructure. In fact, the extent to which this work is hidden at all is reflective of the power relationships, motivations, and values at play within the organisations which create and maintain infrastructure.

In making sense of Tor as a site of social action, it is important to recognise that its worlds aren't static but shape and influence one another (research question one). This also fundamentally shapes the practices of design and maintenance which shape

the infrastructure itself (research question two), which, as they change, are also reshaping the category system of users embedded in Tor. Changes in these worlds and the relationship between them are key to understanding how Tor's approach to and understanding of crime is changing (research question four). As it enters this new phase of its life, Tor's shift to a more self-reflexively governmental approach is also fundamentally changing its relationship with power.

## Broader questions of crime and power

In this section, I explore the broader terrain of power in which Tor exists. Tor's role in contemporary societies extends well beyond issues of crime, touching on broader issues of geopolitics and power. Mapping the ways in which Tor interacts with power, meaning, and material infrastructures on this global stage is difficult, especially as I have restricted my research to the Tor community itself. Although I aim to address this broader context, I try to do so with my feet firmly planted in my empirical research, and what I can justify from analysis of my interviews and archival research. Hence, I discuss how Tor perceives these things and are trying to act, and this picture may look rather different from the vantage point of a GCHQ analyst, developer at Facebook, civil servant, police officer, soldier, LGBT rights activist, or cabinet minister. Fortunately, the Tor community is very alive to these issues, and anxieties about how Tor fits into a wider geopolitical context were a common theme in my interviews.

The globalisation of human societies, partly achieved through the creation of the international Internet infrastructure, has complicated many of the taken-for-granted boundaries between the national and international domains, and hence between how states govern crime and how they deal with issues of national security (Castells, 2002, 2004). The mass collection of personal data as a means of getting a handle on the complexity of contemporary societies and the connecting up of the communication systems of different nations have been part of the increasing

securitisation of issues of crime, with policing taking up the tools and practices which were historically the purview of espionage and national security (Brodeur, 2007; Lyon, 2014). The rise of technologies of power based around mass surveillance and censorship have therefore fixed online infrastructures and platforms as central points in the topology of the Internet where social control, the governance of populations, and relationships between nation states are negotiated (Gillespie 2010, 2018; DeNardis, 2009, 2014). As I have discussed at length in this thesis, Tor (and particularly its engineer social world) sets itself directly against this 'topological' form of power.

On a global stage, many of the most successful of these online international platforms and infrastructures are engaged in a set of apparently-contradictory movements, on one hand attempting to assert themselves in important ways as outside the purview of nation state regulation, while on the other pulling themselves to the heart of nation states' attempts to govern their societies (Gillespie, 2018, Zuboff, 2019). What ties these together is the implication of these platforms in governmental relations, not only as things to be governed but as sites themselves where governance is enacted, by themselves and by nation states as well (Foucault 2007). As I describe in Chapter 3, the curators of these platforms and the algorithms which make sense of the data which they generate are giving rise to a new set of "platonic guardians" (Loader, 2004) in the global tech elite, whose expert knowledge and neutral, technocratic, and science-based approaches to governing societies through design have been particularly attractive to governments desperate to assert control over late modern societies. These 'platonic guardians' are able to represent themselves as neutral administrators of society, bringing expert knowledge to the business of government.

As global Internet platforms such as Google and Facebook employ engineering and design-based strategies for governing their billion-strong user populations, governments in the West are increasingly using these 'smart governance' solutions based around predictive analytics to deliver and target public services and control

(Ferguson, 2016; 2019). Meanwhile, private companies like Palantir are exporting these capabilities to the rest of the world, and more authoritarian nations such as China are embedding them in the heart of their technologies of government (Biddle, 2017; Liang et al., 2018). This has allowed these 'new platonic guardians' to amass substantial power, money, and influence outside traditional mechanisms of democratic scrutiny (Loader, 2004). However, if these infrastructures are becoming central to control, they are at the same time becoming important points at which control is resisted. In the present day, and as these issues have moved to the forefront of political life, Tor has effectively become a critique of this rising global tech elite from within, part of a broader shift in the information security research community towards aiming for research which addresses and impacts social and political issues (Rogaway, 2015).

While many in Tor see themselves as explicitly fighting this technocratic form of governance, which they understand as dangerous and authoritarian, they are also alive to their own role in wielding the same kind of power. For a group aiming to protect the Internet as a home for democratic liberal values, it is potentially uncomfortable for them to be enacting this kind of structural change through design themselves. If the battle over the future of the Internet is only being fought between different factions within the US tech elite, this potentially only serves to concentrate the power to determine the Internet's future in the hands of this elite class. Tor is also open to the criticism that its values and visions are grounded in US-centric notions of privacy and essentially promote US global interests. By promoting open models of society over closed ones, establishing globally accessible tools for resistance and free speech and human rights activism, and preventing governments from censoring access to Western media, Tor is potentially a powerful tool for destabilising authoritarian regimes and promoting the rise of democratic, liberal forms of government around the world. The use of this kind of 'soft power' by the West has been criticised as a key part of how contemporary neoliberal state attempt to advance their geopolitical interests and spread a Western capitalist way of life around the world (Nye, 2002). In embedding them in infrastructure, openness,

democracy, and privacy can be masked as politically neutral concepts while embodying and promoting essentially Western liberal framings of these ideas.

As I have argued in this thesis, Tor's developers are very alive to these issues, and recent efforts to conduct user research and make Tor's vision of privacy more representative of its global user base are an important response to this critique. However, this is in itself a form of governmental power, even if a more democratised one. Even these explicit efforts to 'decolonise' the design work of privacy technologies like Tor can act as a form of soft power, taking the experiences and identities of people around the world and fitting them into Western category systems and conceptual frameworks. The paradox is that the more it tries to decolonise its framing of its users, the further it embeds itself into the lives of its global user community. Through collecting this information, Tor is in fact setting frames of categorisation, and hence power, over its users. While this is the picture in more authoritarian nations, the role which Tor sets for itself in liberal capitalist democracies is rather different. As the liberal vision of governance and democracy has been shaken by rising authoritarianism in the West and the spread of mass surveillance, Tor is in some ways acting as a resilience mechanism, part of how liberal societies are navigating the tensions and contradictions between freedom and control at their heart. This too brings Tor into the functioning of governmental power and how it is negotiated. As Guerses, Kundnani, and Van Hoboken (2016) argue, the efforts of privacy technologists to resist power themselves package up and reify forms of power and ideas about society: in infrastructural politics, governmental power is inescapable

While the controversies aroused by the revelations of mass surveillance by Western liberal governments have largely passed, the role of surveillance by private companies and in authoritarian regimes are only increasing their prominence in public debates about the Internet. Tor's commitment to privacy in a political landscape increasingly critical of surveillance capitalism is beginning to establish Tor as a powerful moral force and site of an alternative vision of governance (of a sort) in

its own right. Hence, issues of the harm and crime in which Tor are implicated are perhaps best understood in the same terms as those of other internet platforms, from Facebook and Google to the Internet backbone infrastructures themselves: as problems of infrastructural governance.

While Tor's implication in crime is undoubtedly overstated in many accounts, nonetheless, it does play host to some serious harms. This is not necessarily best understood as causing 'opportunities' for crime, rather, a more productive perspective might be to consider Tor as an infrastructure which is inherently permeable to a range of uses. In fact, Tor is only one of many ways through which Internet users can hide their IP address, and the majority of criminal services are enabled through the use of 'bulletproof' hosting services and VPNs, and are simply hosted on the 'Clearnet'. Additionally, while Tor has become implicated in harm and crime, in many ways its effect has been one of harm reduction. Cryptomarkets, although they facilitate the trade in illegal goods, have been shown to mitigate some of the violence associated with street drug dealing (Barratt et al., 2016a), and as most crime occurs on services hosted on the regular Internet, Tor has in fact become a vital tool for organisations like the Internet Watch Foundation or law enforcement for investigating online crime while evading detection by malicious actors. Equally, the Tor Brower's substantial security protections serve to protect its users from both malicious code and the now-ubiquitous attempts by most web services to track users across the Internet without consent. It also forms a vital platform for communication and censorship circumvention for some of the most vulnerable people in the world. This is not to minimise the harm caused by some users of Tor Onion Services. It is, however, to argue that whether one judges Tor to be a socially beneficial or harmful force is more a question of competing visions of future Internet societies than the weighing of costs versus benefits: the importance attached to crime as compared to harm, to freedom as compared to order, and to broader notions of social justice. The rise of the cryptomarkets is part of the same kind of phenomenon as Tor itself: just as Tor extends and subverts the infrastructures of the Internet towards its visions of

the future, so too do the cryptomarkets extend and subvert the Tor network in the service of their own.

Tor's attempts at more widespread adoption and its drives towards standardisation as a security toolkit may be more successful than might be anticipated for a technology still widely known as 'the Dark Web'. The wider currents of geopolitics suggest that Tor's security properties may outweigh its status as an irritant for law enforcement, especially as the Internet continues to splinter, and online threats from China and Russia continue to escalate. In a recent blog post, a former FBI Director spells this out, admitting to have changed their mind in favour of the social benefits of encryption technologies and arguing that their protective qualities are vital to maintaining the Internet as a viable part of human societies in the face of international threats (Baker, 2019). This is not only the balancing of national security concerns against domestic law enforcement, but part of the increasing blurring of the boundaries between these domains (Brodeur, 2007). This future vision of society is somewhat stark, involving the hardening and securitising of all areas of life and tight control over the global links between nations. Paradoxically, Tor is potentially also a counter to this isolationism. The view of the Internet which a Tor user experiences is inherently internationalising: one sees the Internet from one of a random selection of other countries (depending on the exit node selected), which can often look very different, with adverts in foreign languages, different ordering of search results, and even different prices for services. This re-establishes the 'globality' of the Internet and places it in the hands of its users as a distinct sovereign space of its own.

A suspicious reader might at this point ask (and many in the broader Tor user community have) whether there was ever a pivot in the actual purpose of Tor from a military technology serving the needs of US global power to a crusading human rights technology run by civil society groups. Is this a true case of Tor being handed over to the NGO sector as a technology of freedom, or is this simply a 'front', always part of the cultivation of US geopolitical goals? Unlike some reporting around Tor,

which presents this military connection as a 'gotcha' (see for example, Levine, 2014 and rebuttal by Lee, 2014), I disagree that these two things are mutually exclusive, or even necessarily contradictory. The developers I spoke to, from more and from less establishment backgrounds, were all deeply and passionately committed to privacy (though some were more critical than others of Tor's links to US soft power, which I discuss in Chapter 9). In fact, these two perspectives, which overlap in important ways around the importance of liberty, freedom of speech and association, and the global movement against authoritarian power are, at least as far as Tor is concerned, working in the service of compatible goals.

None of this means that Tor isn't also a powerful site of resistance. Just like the Internet itself, Tor is both part of how the Western liberal order is working through some of its internal contradictions and attempting to underwrite its vision of the world, as well as a crusading vision of freedom and escape from this order (Haraway, 1991). Equally, the anti-regulation, free-market vision of many cryptomarkets shows how Tor might be a home for yet more visions of the world, such as those with more radical libertarian, anti-government sensibilities (Maddox et al., 2016). As Haraway (1991) argues, in her 'cyborg' depictions of high technology societies, these infrastructures, often arising from the work of military research, are the sites of a vast panoply of different potential meanings, possessing the potential for both domination and liberation. Some of the Tor developers explicitly saw Tor as rekindling foundational elements of liberalism within societies at risk of being driven by Internet technologies (through the logics of capitalism, control, and colonialism) to authoritarianism, while others saw it as a path to a far more radical transformation of the social order. The multiplicity of meaning in Tor, something which the social worlds framework is particularly effective at grasping, is vital to understanding the often-contradictory ways it acts in the world. As the global vision of the Internet shows signs of faltering, Tor is in fact one of the clearest articulations of its liberal roots, with these different visions constituting distinct instantiations of liberal rationalities. The problems which Tor faces are similar to those of other major Internet platforms, and are in fact reflective of the tensions and contradictions at the

heart of liberal democracies between control and freedom; technocracy and democracy; centralisation and decentralisation.

## Infrastructural criminology

In the preceding four sections, I have discussed a set of themes which address my research questions but also bridge across them: design, hidden work, the transformation in Tor's worlds, and its broader implication in relations of power. I conclude this chapter with a discussion of some of the theoretical and methodological implications of this research for criminological study of the Internet and understanding crime and control in contemporary societies. Criminology as a discipline is particularly well-suited to exploring the power of discourse in society. Drawing from a wide range of scholarship, including but by no means limited to Foucault's theoretical work, frameworks for studying institutions and fields from Bourdieu, and symbolic interactionist approaches, there have been a wide range of accounts which study the links between particular ways of making sense of the world, the mechanisms of control and technologies of power which underpin contemporary societies, and the practices, material forms and relationships through which these are enacted. These have studied a range of professional practices, rationalities and sensibilities within criminal justice systems through deep qualitative interviewing, ethnography and archival work. However, technological infrastructures, particularly those which underpin the Internet, remain largely untouched by this kind of criminological study. Nevertheless, they are crucial sites at which governance is enacted, experienced, and resisted. Bringing the Internet's platforms and infrastructures into these explorations of governmental power is therefore an important and under-explored area of research.

One of the main contributions of this research is a reframing of Tor as an infrastructure rather than simply a tool for crime. As Becker (2008) studied what goes into 'producing' a work of art in *Art Worlds*, by exploring the conditions which

make Tor possible and the different elements and types of work which make it a site where social facts such as 'privacy', 'crime', 'justice' and 'governance' are produced, we can achieve a much deeper understanding of the role which it plays in contemporary social life. Social worlds approaches, and Star's closely linked 'infrastructure studies' scholarship provide a 'way in' for criminologists to study these processes of materialisation in technology without getting lost: what Musiani (2012) calls "a study… that isn't afraid of its subject". Foucault argues that to understand technologies of control, we need to understand the rationalities of power which underpin them: the historical currents in ways of making sense of the business of governing societies. But in fact, when the technologies of control take up position around huge technical infrastructures they accrete dense thickets of meaning and multiple different ways of making sense of the business of governing society, crime, control, and privacy. A social worlds approach allows us to connect up the wider currents of ideas and power (the Foucauldian framing of discourse) to the lower-level picture of practices, work, and materiality as they cluster around and shape particular infrastructures as sites where governance is produced. This allows us to see how these lower-level materialisations of discourse interact with *technologies of power* on a broader stage and gain insight into the apparently-random, unpredictable effects which these 'disruptive' technologies have on crime and social control.

In Chapter 4, I discuss the sociological literature on social life as 'performance', both as a way of understanding the structures of human interaction and the ways in which technologies reify the ideas and category systems which become embedded in them through design. The idea of 'performance' is a rather productive metaphor for understanding Tor as a site of social action. Social performances, much like theatrical ones, require a range of additional material elements to come off successfully: lighting rigs, curtains, chairs, a stage and audience seating (Pinch, 2010). Pinch (2010) argues that these material elements both support social performances and shape the conditions in which they occur in important ways, calling for further sociological research into the design of Internet infrastructures which shapes the

human interactions which take place within them. Turning this lens around to the 'performances' of the infrastructure itself and the values and visions which it attempts to realise through changing these material settings of human interaction, we reveal a range of other kinds of hidden work which allow these to be successful in practice; the stage hands, lighting engineers, janitors and house staff, to continue the metaphor.

A putative 'infrastructural criminology' could engage with this wide range of different kinds of work to achieve a deeper picture of Internet infrastructure as another important domain of the governance of crime and harm and the exercise of disciplinary power, alongside the traditional institutions of the criminal justice system, such as the police, courts, prisons, and community justice. It would be no more productive to focus solely on the design of these infrastructures than it would be for a criminological study of the police to focus solely on the laws they enforce. Further studies could extend our understanding of the role which infrastructures play in how governance, privacy, control, and crime are 'produced' in contemporary societies. This also opens up the terrain for more critical studies of cybercrime which do not necessarily frame themselves through dominant, administrative ways of making sense of crime and governance, and for theoretical accountings for the role played by technologies in cybercrime which actually engage with why they work the way they do, rather than getting lost in technical detail or abstracting them to a totalising 'cyberspace'. By finding the interesting criminological stories in these "boring" (Star, 1999) aspects of social life, this project might also have something to contribute to Science and Technology Studies, bringing criminology's focus on crime, governance, and power to bear on these appreciative studies of technology. By excavating the category systems, frameworks of representation, and hidden work embedded in these infrastructures, where they come from, how they change, and the visions of the world on which they depend, criminology can explore vital questions about who is being privileged, who is left out, and how the business of governance is changing in contemporary societies.

## Conclusions

This chapter has brought to a close my social worlds study of Tor, mapping out the relationships between my research questions and the themes which straddle them, linking my results into the broader literature. Tor is in fact a remarkable site of social action which has been far more successful than any other comparable project. Reliant on the work of a very small number of people, it has survived for nearly two decades and now has a large worldwide community and over two million daily users at the time of writing. Through its life, Tor has managed to weather a great deal of change, opposition, and crisis, and has kept its diverse community together despite their differences. Tor is a site of social action around which multiple distinct, overlapping visions of privacy are enacted through different kinds of work. Making sense of this requires accounting for all these different kinds of work and how they 'produce' or 'perform' visions of privacy, justice, crime, and control. The cypherpunk visions of the world which Tor is trying to realise are multiple and changing, focused around privacy and the decentralisation of power, but refracted into three distinct social worlds. While design work is doubtless important, maintenance work, resilience practices, PR work and other forms of labour also play a key role in making its visions of privacy a reality for millions of people around the world. These forms of work also constitute important sites where values are performed and go on to shape the infrastructure in important ways.

One can imagine five potential future directions for Tor. The first of these is failure: that Tor might collapse through the increasing ratcheting-up of pressures on its infrastructure, the compromise of its development community by hostile forces or internal schisms, the rise of newer and better anonymity networks, or an authoritarian crackdown on anonymity technologies. The second draws from the activist vision, with Tor becoming more a campaigning and advocacy organisation, and the technology working in the service of this political struggle. Thirdly, Tor might retreat, as the infrastructuralists envision, from these issues of values and become a software foundation in the more classic model. Fourthly, Tor might fulfil the visions

of its engineers, evolving itself out of existence as a distinct organisation, so that it becomes a ubiquitous standard that underpins the way the Internet works. Finally, if the transformation of Tor's social worlds continues, Tor might become something more akin (in a limited way) to Facebook or Google, an international infrastructure which wields a kind of sovereign claim in its own right over its users as legitimate subjects whose lives it can shape in important ways.

To understand Tor, we need to study it as an infrastructure, a site of social action surrounded by heterogeneous meanings, practices, and material forms. Privacy technologies, of which Tor is by far the most well-known and widely-used, are both sites of resistance to authoritarian power, but also themselves embed strong ideas about crime and how it should be governed in contemporary societies. A primary contribution of this thesis is the development of a picture of Tor's attempts to wield and reckon with its own power as an infrastructure. Milan (2016) calls this 'stealing the fire', it forms a part of Coleman's (2017) 'weapons of the geek', and is crucial to Musiani's (2012) 'doing politics' through architecture, as I describe in Chapter 2. In further making sense of the technologies of the Internet and their implication in crime, governance, and control, future research might usefully explore the importance of the boring aspects of the Internet, and its hidden people and perspectives. The Internet infrastructure embeds a host of design decisions which are doubtless important to its role as a site of social action What is often lost is the role of system administrators, load balancers, maintainers, regulators, policy people, HR people and public relations experts, who are just as important and who exert real influence over the direction of these projects. These people are making decisions about the governance of crime and conduct, and the administration of large parts of our societies every day. They therefore sit at sites of vital governmental power. To understand infrastructural power, we need to understand it *by necessity* as at the intersection of a multiplicity of different perspectives, values, practices, and social worlds.

To do this, criminological and sociological research needs to engage with these hidden aspects of technology: the dense thickets of meaning which surround infrastructures and how they relate to their material forms. By engaging in appreciative, qualitative research with the people who design, maintain, and promote these infrastructures, and by understanding the different kinds of work and social action which make these infrastructures possible, we can make sense of the visions of the world which are being realised in them. These visions of the world can then be connected up to broader criminological sensibilities and frameworks at the more abstract level of discourse and power in order to tease out the ways in which these infrastructures become sites where governance, power, and control are contested and enacted. Turning to the final chapter, I conclude this thesis with a summary of its overall conclusions and some reflections on the research and its contributions, outlining some limitations of this study and potential avenues for future work.

# chapter 11
# concluding remarks and reflections: privacy worlds

## Introduction

Across this thesis, I have explored Tor as a site of social action, exploring how it has tried to materialise a vision of privacy in the world, and how it has reckoned with and become entangled in power, crime, and harm. I have mapped Tor in detail, moving from a genealogical history in Chapter 3 to a deep exploration of the different *social worlds* which underpin Tor in Chapter 6, to how these have been materialised through practices and design decisions in Chapter 7. In Chapter 8, I then described what actually happens when these materialised values meet the outside world – how Tor attempts to defend itself, and the different kinds of invisible work which are required to support these in practice. In Chapter 9, I have excavated how Tor's attempts to act in the domain of power work out in practice when they come into contact with the dominant technologies of power which they are trying to subvert. In Chapter 10, I discussed how these different elements fit together, drawing out key themes across my findings chapters and attempting to pull these together into a characterisation of Tor as a site of social action. In this final chapter of the thesis, I reflect on the broader salience of my research, its key contributions to the academic literature, and potential limitations and avenues for future study.

All infrastructures are sites of power, where material resources are controlled and category systems enacted (Star, 1990, 1999). The visions of society which are

embedded in their material forms and the different kinds of work required to maintain them exert a force over society, structuring social life and realising these visions in greater or lesser ways. In doing so, they shape the people who interact with them to conform to these category systems and cast those who cannot as outsiders (Star, 1990; Foucault, 2008). When these infrastructures become problematised as active sites of resistance, however, visions of new and alternative futures come into conflict with the visions embedded in the existing infrastructures. The Internet is a particularly fertile site for these conflicts, as it permits new infrastructures to be built alongside and on top of it with relative ease.

This makes privacy technologies powerful sites of social action, where the logics and practices of technological disruption and innovation can be repurposed to become forms of activism in their own right (Milan, 2016). The particular place of data and information in contemporary societies makes privacy, and privacy technologies in particular, a flashpoint for a wide range of political struggles. The issues which privacy touches on, of information about people and how it is controlled, governed, and who has power over it, are particularly vital due to the importance of the communications infrastructures which underpin our lives and the kinds of data they collect about us (Lyon, 2014; Raab, Jones, and Szekely, 2015). That technologies and infrastructures have become a key domain in which this battle is being fought is reflective of the ways in which contemporary societies are governed, with automated mass online surveillance and censorship at the heart of modern technologies of control (Lyon, 2014).

Making sense of Tor as a site of social action involves making sense of it as an infrastructure, mapping the different visions of the world which go into it, the kinds of work which make it possible, and the human and technical forms and structures of which it is composed, and how these interrelate. Exploring Tor's design is important, but is not enough, as this does not account for the conditions and relationships which allow it to go from an ingenious prototype to a fact of life for millions of people around the world, and hence to realise its vision of the world in practice. By

understanding the category systems, hidden work, frameworks of representation, and visions of privacy which make up Tor, we can better understand how it interacts with the other Internet infrastructures whose dominant rationalities of control and visions of the world it is trying to replace.

## Key contributions of the thesis

A major contribution of this thesis is to the body of scholarship on Tor, the Tor community, and the Tor Project. Although Marechal (2018) and Gehl (2018a) have both studied different aspects of Tor to those I cover here as one part of comparative projects which look at the broader Internet freedom milieu, this thesis constitutes the first in-depth sociological study focused entirely on Tor of which I am aware. I have attempted to characterise Tor as a site of social action, drawing on the social worlds framework to distil the dense, heterogenous and diverse discourses in the Tor community into three distinct 'ideal type' perspectives. These three social worlds, which each constitute a 'universe of discourse' do not necessarily accord entirely with the perspective of any given individual in the Tor community, but, as I hope I have demonstrated, prove a powerful framework for making sense of Tor and its role in human society.

This thesis sets out the beginnings of a potentially novel avenue of criminological research, drawing as it does from theoretical and methodological frameworks largely outside those usually employed in criminology. In arguing for an 'infrastructural criminology' approach, I have attempted to make the case for the productive use of frameworks from Science and Technology Studies in expanding criminological understanding of cybercrime, cyber security, and the Internet more broadly. I have tried to approach Tor not as an intrinsically criminal tool, but as an infrastructure deeply implicated in power, politics and governance. In some more modest ways, I have also contributed to social worlds theory, in particular using its concept of

'convergence' to frame not only how people interact with existing infrastructures, but also the processes through which they are initially designed.

Finally, I have contributed to the literature on privacy and digital society. This has drawn in particular on the work of Coleman, Musiani, and Milan in different ways to make sense of technology as a site of social action, and different visions of privacy as something which can be 'produced' through building infrastructure. In exploring the different ideas, types of work, discourses, people, and technologies which go into 'making' a particular vision of privacy, I have aimed to highlight some of the fundamental questions of values, power and justice which are implicated in these processes, often hidden or deliberately obscured. The social worlds approach, which, resonant with Haraway's scholarship, sees infrastructures as sites of multiplicity, where different meanings and visions of the world overlap and interact, is a particularly powerful framework for conducting this research.

## Reflections on limitations and avenues for future work

In this section, I reflect on the limitations of this thesis, and some potential avenues for future work. Although I managed to negotiate far greater access to the Tor community than I imagined I might when beginning, the perspective I depict here is by necessity a partial one. There were many members of the Tor Project with whom I was unable to speak, and several potentially important sites of research which I was either unable or decided not to access. In particular, Tor's regular developer meetings would have been a potentially valuable research site, and would be an obvious target for future research. However, I have generally been wary about becoming too involved in the Tor community, in particular deciding against trying to observe public IRC meetings or become part of the relay operator community. This is because many within the broader Tor community are deeply suspicious of researchers, and at a time when the Tor Project are attempting to increase participation, I was loath to do anything which might put people off from engaging

with this. Other topics I decided to avoid or not include in my analysis for reasons of sensitivity. In particular, the analysis and discussion of resilience practices in Chapter 8 could be considered to be sensitive, or exploitable by those who wish Tor harm, and as such I have thought very carefully about what I have and have not included in this section in particular. In particular, I made the choice not to present information about individuals' security practices, even though a number of them did talk about this in some depth.

In many respects, this research barely scratches the surface of Tor. It maps Tor's broader contours and delves deeper in a few interesting or illustrative areas, but there is a vast amount of ground and further interesting questions, which remain largely untouched. In particular, the mailing lists of Tor constitute a vast, largely untapped resource for sociological researchers. Some particularly interesting aspects of Tor's design, such as how it coped with its initial use for illegal downloads, the complex negotiations between administrative practices and censorship in relay operation (such as the use of blacklists and exit policies), and its attempts to cope with an expanding user base remain entirely untouched in this research. An early conflict between Tor and Wikipedia is also a fascinating example of a clash between two similar, but meaningfully distinct visions of Internet utopia which is well worth future study. As Tor has grown, the amount of data it has made available has increased dramatically, and more recent development work has been accompanied by documented changes in Tor's source code with substantial discussion and debate attached. Although I engaged in some analysis of this, for reasons of time and clarity I have chosen to leave this work for future research. Equally, the development of major parts of Tor, such as the Tor Browser and the first and subsequent versions of Onion Services are important milestones in Tor's story which merit study of their own and themselves embed important decisions about crime, governance, and social justice. Tor is in a moment of profound change, and I have been very lucky to document some of this.

Reasons of space have also limited the historical scope of this research, which is largely confined to a combination of Tor's early years along with more recent developments in the wake of the Snowden revelations. The intervening years are lightly sketched herein, but many important controversies, crises, challenges and successes are left out for reasons of space. A fuller historical accounting of Tor could offer a valuable contribution to better understanding the role it has played over the years. Equally, tracking the evolution of discourse about crime and control over the course of the mailing lists would itself be a valuable project. As Tor enters this new era, it will doubtless change and develop in yet more interesting ways. A more ethnographic study, building on this research to attempt to develop a closer collaboration with the Tor community over the next few years could be extremely productive in achieving a deeper picture of these changes.

This research is also by design limited in scope to a particular community whose voices and perspectives I wished to bring to the fore: the immediate community of people who contribute directly to Tor. However, Tor is deeply linked to a range of other communities and projects, from major international conferences such as the Chaos Communications Congress and Hackers On Planet Earth, to technical organisations like Tails and OONI, and to campaigning organisations such as the EFF. Studying these organisations and the ways in which they contribute to, criticise, and understand Tor could unearth yet more hidden perspectives, social worlds, and important forms of work. Equally, while I managed to interview some developers of the Onion Services which make use of Tor, an in-depth study of the technical foundations of these projects would be valuable in more directly connecting Tor to its wider user base and to the ways in which its visions are actually being realised, taken up, and transformed by others.

Having chosen to focus entirely on the Tor community, Tor's users and their perspectives are almost completely absent in this research. The users of technologies and infrastructures form core parts of many social worlds studies (Star, 1999) and related approaches (Brunton and Coleman, 2014). Their absence makes it

difficult to achieve a truly holistic view of Tor, or to make the final connection between values, materiality and the actual realities which are performed for and by users in practice, whose own frameworks of understanding and constructions of privacy and power are an equally important factor. Bancroft's (2017) work on cryptomarket communities and the relationship between their own constructions of anonymity and those embedded in the material properties of Tor Onion Services point a potential way forward for this kind of research. Equally there are a range of other people who interact with Tor, who develop their own distinct perspectives: the academic research community, state intelligence agencies, cryptographers, the Internet governance community, policymakers, politicians, law enforcement and Internet Service Providers. There may well therefore be important social worlds which play a role in Tor which have been missed by this research, and Tor's current re-appraisal of its ways of understanding its users make this a key an opportune site of future research.

This approach could also profitably be turned to criminological study of other important technologies and infrastructure. The most obvious of these is Bitcoin, which shares many of Tor's intersections with crime, governance and power, but navigates them in rather different ways. While Facebook and Google are unlikely to open themselves up to the extent that Tor does, there is the potential to do this kind of deep, appreciative qualitative research with other, smaller, emerging social media companies, many of whom are desperate to better make sense of the problems of crime and governance which they are facing. Some in law enforcement may be equally happy to discuss their attempts to develop mechanisms of governance and control in trying to produce 'justice' (or at least fight crime) through the Internet infrastructure. Finally, many modern cybercrime economies rely heavily on both legitimate and illegitimate infrastructure, such as botnets, payment systems, bulletproof hosting, and web services. Understanding the forms of infrastructural work and the social worlds which are implicated in these may open up new avenues of criminological enquiry to better characterise these forms of (illegal) action through technological infrastructure. The prospects for an 'infrastructural

criminology' to bring a more critical perspective into cybercrime research are exciting, and I intend to continue this programme of research in the future.

## Final remarks

This research has taken place across a period of time where questions about power and the Internet have risen to public prominence. Even as the forces of authoritarianism appear to be on the rise around the world, so too are historic resistance movements springing up to demand radical, transformative social change and liberation. The power wielded by the tech giants and social media companies is becoming both a dominant shaping force in society and the subject of increasing critique in public life, as they continue to disrupt work, democracy, policing, governance, politics, and social life. Visons of society are clashing against one another, and the Internet is a place where many of these battles over different potential futures will be fought. Possessing the potential to be both technologies of domination or of liberation, Tor and the other parts of the Internet infrastructure will play a key role in these struggles, and understanding them as sites of social action, rather than deterministically acting on society, is crucial to making sense of how our societies are changing in the contemporary era.

The role of infrastructure as a site of power is not new and has existed as long as human society. The particular dynamics of the Internet are interesting, as its capacity to be extended and built upon opens up this infrastructural power to a range of other actors, making it a site of profound social change, where relatively small groups can have enormous success in realising their visions of future worlds. If we want to build structures and societies which aren't based around domination, we need to understand the mechanisms by which power works. This extends also to the ways in which we resist power, which themselves embed forms of power and visions of the world.

Tor is a particularly striking subject to research in that it not only represents a radically different vision of the world to the contemporary Internet but has managed to make this a reality for millions of people around the world. Much like the Internet itself, it is a military technology which has become an engine of social transformation, a place where a range of different visions, meanings, and potential futures are fought over, enacted, and born. Researching Tor and the Tor community for the past four years has been a singular pleasure, and the members of that community who are striving to maintain and develop the 'Dark Web' whom I have encountered have been friendly, welcoming, and generous people fighting for privacy, anonymity, and freedom.

# bibliography


Adams, K. (2018a) Silicon Valley's Philosopher-King Jaron Lanier Envisions a Brave, New World Without Social Media, *Medium*, Retreived from: https://medium.com/@kevinsheaadams/silicon-valleys-philosopher-king-jaron-lanier-envisions-a-brave-new-world-without-social-media-1008d787bc85

Adams, C. (2018b). "They Go for Gender First" The nature and effect of sexist abuse of female technology journalists. *Journalism Practice*, *12*(7), 850-869

Afroz, S., & Fifield, D. (2007). Timeline of Tor censorship. Retrieved from: http://www1.icsi.berkeley.edu/~sadia/tor_timeline.pdf

Afroz, S., Garg, V., McCoy, D., & Greenstadt, R. (2013, September). Honor among thieves: A common's analysis of cybercrime economies. In *2013 APWG eCrime Researchers Summit* (pp. 1-11). IEEE.

Agger, B. (2011). iTime: Labor and life in a smartphone era. *Time & Society*, *20*(1), 119-136.

Akrich, M. (1992) The de-scription of technical objects, In Bijker, W.E. and Law, J. (editors) Shaping technology/ building society. MIT Press, pp. 205 – 224.

Albas, C. A., Adler, P., Albas, D. C., Adler, P. A., Altheide, D. L., Altheide, D., ... & Clarke, A. E. (2003). *Handbook of symbolic interactionism*. Rowman Altamira.

Aldridge, J., & Decary-Hétu, D. (2016). Cryptomarkets and the future of illicit drug markets. *The Internet and drug markets*, 23-32.

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, 35, 7-15.

Alfredo Filho, S., & Johnston, D. (2005). *Neoliberalism: A critical reader*. University of Chicago Press.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of economic perspectives*, *31*(2), 211-36.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., ... & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer, Berlin, Heidelberg.

Angouri, J. (2016). Online communities and communities of practice. *The Routledge Handbook of Language and Digital Communication*, 323-338. Routledge

Aradau, C., Blanke, T., & Greenway, G. (2019). Acts of digital parasitism: Hacking, humanitarian apps and platformisation. *New Media & Society*, 21(11–12), 2548–2565. https://doi.org/10.1177/1461444819852589

Armstrong, S., & Jefferson, A. M. (2017). Disavowing 'the'prison. In *Carceral Spatiality* (pp. 237-267). Palgrave Macmillan, London.

Aronovich, H (2012). Interpreting Weber's ideal-types. *Philosophy of the Social Sciences*, 42(3), 356-369.

Aycock, A. (1995), "Technologies of the Self:" Foucault and Internet Discourse, *Journal of Computer-Mediated Communication*, Volume 1, Issue 2, JCMC121,

Bachmann, M. (2012). Deciphering the hacker underground: First quantitative insights. In *Cyber Crime: Concepts, Methodologies, Tools and Applications*, 175-194. IGI Global.

Badouard, R. & Mabi, C. & Sire, G. (2016). Beyond "Points of Control": logics of digital governmentality. *Internet Policy Review*, 5(3).

Baer, W. S., Borisov, N., Danezis, G., Guerses, S. F., Klonowski, M., Kutylowski, M., ... & Sadeghi, A. R. (2009). Machiavelli Confronts 21st Century Digital Technology: Democracy in a Network Society. Available at SSRN 1521222.

Baker, J, (2019), Rethinking Encryption, *Lawfare Blog*, https://www.lawfareblog.com/rethinking-encryption

Ball, J, (2013), Silk Road: The online drug marketplace that officials seem powerless to stop, *The Guardian*, Retrieved from: https://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace

Ball, K., & Webster, F. (2003). *The intensification of surveillance: Crime, terrorism and warfare in the information era*. Pluto Press.

Ball, K., Lyon, D., & Haggerty, K. D. (Eds.). (2012). *Routledge handbook of surveillance studies*. Routledge.

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, 1(2), 176-198.

Bancroft, A., & Scott Reid, P. (2017). Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society*, *20*(4), 497-512.

Barassi, V., & Treré, E. (2012). Does Web 3.0 come after Web 2.0? Deconstructing theoretical assumptions through practice. *New Media & Society*, *14*(8), 1269-1285.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016a). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*, 35, 24-31.

Barratt, M. J., Lenton, S., Maddox, A., & Allen, M. (2016b). 'What if you live on top of a bakery and you like cakes?'—Drug use and harm trajectories before, during and after the emergence of Silk Road. *International Journal of Drug Policy*, 35, 50-57.

Bartlett, J. (2014). *The dark net: Inside the digital underworld*. Melville House.

Bartlett, J. (2016). Cypherpunks write code. *American Scientist*, *104*(2), 120-124.

Bauman, Z. (2000). *Liquid modernity*. London: Polity.

Bayat, A., Naicker, V., & Combrinck, T. (2015). Towards an Understanding of How School Administrative Clerks Negotiate Their Work in Public Schools: A Social Worlds Perspective. *International Journal of Educational Sciences*, *8*(2), 293-303.

BBC News, (2018), Australia data encryption laws explained, *BBC News*, Retrieved from: https://www.bbc.co.uk/news/world-australia-46463029

BBC News, (2019), Russian intelligence 'targets anonymous Tor browser', *BBC News,* Retrieved from: https://www.bbc.co.uk/news/technology-49071225

Beck, U. (2009). *World at risk*. Cambridge: Polity.

Becker H. S. (1963). *Outsiders. Studies in the Sociology of Deviance*. New York Free Press

Becker, H. S. (1986). *Doing things together: Selected papers*. Evanston: Northwestern University Press.

Becker, H. S. (2008). *Art worlds: updated and expanded*. University of California Press.

Becker, H. S., & McCall, M. M. (Eds.). (2009). *Symbolic interaction and cultural studies*. University of Chicago Press.

Becker, H. S. (2017). Moral entrepreneurs. In *Cultural Criminology* (pp. 11-28). Routledge.

Becker, H. S. (2018). Labelling theory reconsidered, In *Deviance and social control* (pp. 41-66). Routledge.

Benedickt, M. (1991). *Cyberspace: first steps*., MIT Press

Bennett, C. J., & Raab, C. D. (2017). *The governance of privacy: Policy instruments in global perspective*. Routledge.

Berg, M., 1998. “The politics of technology: on bringing social theory into technological design”, *Science, Technology and Human Values,* 23(4), 456-490

Berners-Lee, T., & Fischetti, M. (2001). *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor*. DIANE Publishing Company.

Berry, D. M. (2008). *Copy, rip, burn: The politics of copyleft and open source*. Pluto Press.

Biddle, S. (2017). How Peter Thiel’s Palantir helped the NSA spy on the whole world, *The Intercept*, Retrieved from: https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/

Bingham, N. (1996). Object-ions: from technological determinism towards geographies of relations. *Environment and Planning D: Society and Space*, 14(6), 635-657.

Blackwell, L., Dimond, J., Schoenebeck, S., & Lampe, C. (2017). Classification and its consequences for online harassment: Design insights from heartmob. *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW), 24.

Bloor, M., Fincham, B., & Sampson, H. (2010). Unprepared for the worst: Risks of harm for qualitative researchers. *Methodological Innovations Online*, *5*(1), 45-55.

Bloss, W. (2007). Escalating US police surveillance after 9/11: An examination of causes and effects. *Surveillance & Society*, *4*(3).

Blumer, H. (1954). What is wrong with social theory?. *American Sociological Review*, 19(1), 3-10.

Blumer, H. (1962). Society as symbolic interaction. *Contemporary Sociological Thought*, 91.

Blumer, H. (1986). *Symbolic interactionism: Perspective and method*. University of California Press.

Bogner, A., Littig, B., & Menz, W. (Eds.). (2009). *Interviewing experts*. Springer.

Boman, J. H., & Freng, A. (2017). Differential association theory, social learning theory, and technocrime. In *Technocrime and Criminological Theory* (pp. 55-65). Routledge.

Bonnell, V. E. (1980). The uses of theory, concepts and comparison in historical sociology. *Comparative Studies in Society and History*, *22*(2), 156-173.

Bossler, A. M. (2016). 3 Cybercrime research at the crossroads: where the field currently stands and innovative strategies to move forward. In *Cybercrime through an interdisciplinary lens* (pp. 51-69). Routledge.

Bosworth, M. (2017). Border criminology and the changing nature of penal power. *The Oxford Handbook of Criminology*, 373-390.

Bowker, G. C., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. MIT press.

Bowker, G. C., Timmermans, S., Clarke, A. E., & Balka, E. (Eds.). (2016). *Boundary objects and beyond: Working with Leigh Star*. MIT Press.

Box, S. (2002). *Power, crime and mystification*. Routledge.

Boyd, D. M. and Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1): 210–230.

Brannon, M. M. (2017). Datafied and divided: Techno-dimensions of inequality in American cities. *City & Community*, *16*(1), 20-24.

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, *82*(5), 977-1008.

Brewster, B., Kemp, B., Galehbakhtiari, S., & Akhgar, B. (2015). Cybercrime: attack motivations and implications for big data and national security. In *Application of Big Data for National Security* (pp. 108-127). Butterworth-Heinemann.

Brinkmann, S., & Kvale, S. (2008). Ethics in qualitative psychological research. *The Sage handbook of qualitative research in psychology*, *24*(2), 263-279.

British Society of Criminology (2015). *Statement of Ethics*, Retrieved from: https://www.britsoccrim.org/ethics/

British Sociological Association (2017). *Statement of ethical practice*, Retrieved from: https://www.britsoc.co.uk/media/24310/bsa_statement_of_ethical_practice.pdf

Brodeur, J.P., (2000). Cops and Spooks: The Uneasy Partnership, *Police Practice and Research* 1/3: 299–321, (reprinted in Newburn, T. (ed.) (2005). *Policing: Key Readings*, Cullompton Devon (UK): Willan Publishing, 797–812).

Brodeur, J. P. (2007). High and low policing in post-9/11 times. *Policing: A journal of Policy and Practice*, 1(1), 25-37.

Brown, S. (2006). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, 10(2), 223-244.

Brunton, F., & Coleman, G. (2014). Closer to the Metal. In *Media technologies: Essays on communication, Materiality, and society*, 77-97.

Burgers, T., & Robinson, D. R. S. (2018). Keep Dreaming: Cyber Arms Control is Not a Viable Policy Option. *S&F Sicherheit und Frieden*, *36*(3), 140-145.

Butler, J. (2002). *Gender trouble*. Routledge.

Butler, J. (2006). Performative acts and gender constitution: An essay in phenomenology and feminist theory. In *The Routledge Falmer Reader in Gender & Education* (pp. 73-83). Routledge.

Butler, J. (2011). *Bodies that matter: On the discursive limits of sex*. routledge.

Butler, J. (2013). *Excitable speech: A politics of the performative*. Routledge.

Byrne, M. (2001). The concept of informed consent in qualitative research.(Research Corner). *AORN journal*, *74*(3), 401-404.

Cadwalladr, C., & Graham-Harrison, E. (2018). The Cambridge analytica files. *The Guardian*, *21*, 6-7.

Callon, M. (1991) "Techno-Economic Networks and Irreversibility." In J. Law (Editor), *a Sociology of Monsters. Essays on Power, Technology and Domination*. London: Routledge, pp. 132–161.

Callon, M. (2009). Elaborating the notion of performativity. *Le Libellio d'AEGIS*, Libellio d'AEGIS, 5 (1), pp.18-29. ffhal-00460877

Cannataci, J. A. (2009). *Privacy, Technology Law and religions across cultures*.

Carlson, M. (2018). Facebook in the news: Social media, journalism, and public responsibility following the 2016 trending topics controversy. *Digital journalism*, *6*(1), 4-20.

Carroli, L. (1997). Virtual Encounters: Community or Collaboration on the Internet?. *Leonardo*, 359-363.

Casady, T. (2011). Police legitimacy and predictive policing. *Geography & Public Safety*, *2*(4), 1-2.

Casper, Monica J. (1998) *The Making of the Unborn Patient: A Social Anatomy of Fetal Surgery* (New Brunswick, NJ: Rutgers University Press).

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press

Castells, M. (2004). *The network society A cross-cultural perspective*. Edward Elgar.

Chaabane, A., Chen, T., Cunche, M., De Cristofaro, E., Friedman, A., & Kaafar, M. A. (2014). Censorship in the wild: Analyzing Internet filtering in Syria. In *Proceedings of the 2014 Conference on Internet Measurement Conference*(pp. 285-298). ACM.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American society for information science and technology*, *59*(8), 1347-1359.

Chenou, J. M. (2014). From cyber-libertarianism to neoliberalism: Internet exceptionalism, multi-stakeholderism, and the institutionalisation of Internet governance in the 1990s. *Globalizations*, 11(2), 205-223.

CIA (2019), CIA's Latest Layer: An Onion Site, *CIA Homepage,* Retrieved from: https://www.cia.gov/news-information/featured-story-archive/2019-featured-story-archive/latest-layer-an-onion-site.html

Clarke, A. (1997). A social worlds research adventure. *Grounded theory in practice*, 63.

Clarke, A. E. (2003). Situational analyses: Grounded theory mapping after the postmodern turn. *Symbolic interaction*, 26(4), 553-576.

Clarke, A. E., & Star, S. L. (2008). The social worlds framework: A theory/methods package. *The handbook of science and technology studies*, *3*, 113-137.

Clarke, A. E. & Friese, C. (2007). Grounded Theorizing Using Situational Analysis, in *The Sage Handbook of Grounded Theory*, eds Bryant A., Charmaz, K.

Clarke, A. E. (2007). Grounded theory: Critiques, debates, and situational analysis. *The SAGE handbook of social science methodology*, 423-442.

Clarke, A. E. (2007). Social worlds. *The Blackwell encyclopedia of sociology*.

Clarke, A. E. 2005. *Situational Analysis. Grounded Theory After the Postmodern Turn.* Thousand Oaks: Sage.

Clarke, R. V. (1983). Situational crime prevention: Its theoretical basis and practical scope. *Crime and justice*, 4, 225-256.

Clarke, R. V. G. (Ed.). (1997). *Situational crime prevention* (pp. 225-256). Monsey, NY: Criminal Justice Press.

Clarke, R. V., & Newman, G. R. (2005). Modifying Criminogenic Products-What Role for Government?. *Crime prevention studies*, 18, 7.

CNN (2016), Developer of anonymous Tor software dodges FBI, leaves US, *CNN News*, Retrieved from: https://money.cnn.com/2016/05/17/technology/tor-developer-fbi/index.html

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 588-608.

Cohen-Almagor, R. (2013). Internet history. In *Moral, Ethical, and Social Dilemmas in the Age of Technology: Theories and Practice* (pp. 19-39). IGI Global.

Cohn, E. G., Farrington, D. P., a Wright, R., & Wright, R. A. (1998). *Evaluating criminology and criminal justice* (No. 51). Greenwood Publishing Group.

Coleman, G., (2004). The political agnosticism of free and open source software and the inadvertent politics of contrast. *Anthropological Quarterly*, 77(3), pp.507-519.

Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, *8*(3), 255-277.

Coleman, G. (2009). Code is speech: Legal tinkering, expertise, and protest among free and open source software developers. *Cultural Anthropology*, 24(3), 420-454.

Coleman, G. (2010). The hacker conference: A ritual condensation and celebration of a lifeworld. *Anthropological Quarterly*, 47-72.

Coleman, G. (2011). Hacker politics and publics. *Public Culture*, *23*(3 (65)), 511-516.

Coleman, E. G. (2012). *Coding freedom: The ethics and aesthetics of hacking*. Princeton University Press.

Coleman, G. (2013). Anonymous in context: The politics and power behind the mask. *CIGI Series on Internet Governance*

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous.* Verso books.

Coleman, E. Gabriella. 2013. *Coding freedom: the ethics and aesthetics of hacking. Princeton*, NJ: Princeton University Press.

Coleman, G. (2017). From Internet farming to weapons of the geek. *Current Anthropology*, *58*(S15), S91-S102.

Crawford, A. (2006). Networked governance and the post-regulatory state? Steering, rowing and anchoring the provision of policing and security. *Theoretical criminology*, *10*(4), 449-479.

Curran, J. (2012). Rethinking internet history: James Curran. In *Misunderstanding the internet* (pp. 40-71). Routledge.

Custers, B., van der Hof, S., & Schermer, B. (2014). Privacy expectations of social media users: The role of informed consent in privacy policies. *Policy & Internet*, *6*(3), 268-295.

Danet, B. (1996). *Text as mask: Gender and identity on the Internet*.

Danezis, G., & Gürses, S. (2010). A critical review of 10 years of privacy technology. *Proceedings of surveillance cultures: a global surveillance society*, 1-16.

Darier, M. D. M. E. (1998). Virtual control and disciplining on the Internet: Electronic governmentality in the new wired world. *The Information Society*, *14*(2), 107-116.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, 67(1), 55-75.

Deegan, M. J. (2013). Jane Addams, the Hull-House school of sociology, and social justice, 1892 to 1935. *Humanity & Society*, *37*(3), 248-258.

Deibert, R. J. (2008). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In *Routledge handbook of Internet politics* (pp. 339-352). Routledge.

Demant, J., Munksgaard, R., Décary-Hétu, D., & Aldridge, J. (2018). Going local on a global platform: A critical analysis of the transformative potential of cryptomarkets for organized illicit drug crime. *International Criminal Justice Review*, 28(3), 255-274.

Demont-Heinrich, C. (2002). Central points of control and surveillance on a "decentralized" Net: Internet service providers, and privacy and freedom of speech online. *info*, *4*(4), 32-42.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, *11*, 763-781.

DeNardis, L. (2007). A history of internet security. In *The history of information security* (pp. 681-704). Elsevier Science BV.

DeNardis, L. (2009). *Protocol politics*, Cambridge, MA: MIT Press

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Dennis, A., & Martin, P. J. (2005). Symbolic interactionism and the concept of power. *The British journal of sociology*, *56*(2), 191-213.

De Paoli, S. (2018). The engineer–criminologist and "the novelty of cybercrime": a situated genealogical study of timesharing systems. *Internet Histories*, 2(1-2), 20-37.

DeVault, M. L. (1990). Talking and listening from women's standpoint: Feminist strategies for interviewing and analysis. *Social problems*, *37*(1), 96-116.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router*.

Dingledine, R., & Mathewson, N. (2006). Anonymity Loves Company: Usability and the Network Effect. In *WEIS*.

van Dijck, J., Nieborg, D., & Poell, T. (2019). Reframing platform power. *Internet Policy Review*, *8*(2).

Doctorow, C. (2015), What happened when we got subpoenaed over our Tor exit node, *BoingBoing*, Retreived from: https://boingboing.net/2015/08/04/what-happened-when-the-fbi-sub.html

Dodge, A., Spencer, D., Ricciardelli, R., & Ballucci, D. (2019). "This isn't your father's police force": Digital evidence in sexual assault investigations. *Australian & New Zealand Journal of Criminology*, 0004865819851544.

Dremliuga, R. (2014). Subculture of hackers in Russia. *Asian Social Science*, *10*(18), 158.

Dubrofsky, R. E., & Magnet, S. A. (Eds.). (2015). *Feminist surveillance studies*. Duke University Press.

Eckert, S. (2018). Fighting for recognition: Online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States. *New Media & Society*, *20*(4), 1282-1302.

Economic and Social Research Council (2019), Our Core Principles, *ESRC*, Retrieved from: https://esrc.ukri.org/funding/guidance-for-applicants/research-ethics/our-core-principles/

Edman, M., & Yener, B. (2009). On anonymity in an electronic society: A survey of anonymous communication systems. *ACM Computing Surveys (CSUR)*, *42*(1), 5.

Edwards, P. (1996) *The Closed World: Completers and the Politics of Discourse in Cold War America*. Cambridge, Mass.

Elliott, M. S., & Scacchi, W. (2005). Free software development: Cooperation and conflict in a virtual organizational culture. In *Free/open source software development* (pp. 152-173). Igi Globa

Ericson, R. V., & Haggerty, K. D. (Eds.). (2006). *The new politics of surveillance and visibility*. University of Toronto Press.

Escobar, A., Hess, D., Licha, I., Sibley, W., Strathern, M., & Sutz, J. (1994). Welcome to Cyberia: Notes on the Anthropology of Cyberculture [and comments and reply]. Current anthropology, 35(3), 211-231.

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.

Fairclough, N. (1992). *Discourse and social change* (Vol. 10). Cambridge: Polity press.

Farrington, D. P., & Tarling, R. (Eds.). (1985). *Prediction in criminology*. SUNY Press.

Feeley, M. M., & Simon, J. (1992). The new penology: Notes on the emerging strategy of corrections and its implications. *Criminology*, *30*(4), 449-474.

Ferguson, A. G. (2016). Policing predictive policing. *Wash. UL Rev.*, *94*, 1109.

Ferguson, A. G. (2019). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.

Fifield, D., Lee, L. N., Egelman, S., & Wagner, D. (2015). Tor's Usability for Censorship Circumvention. *InWorkshop on Hot Topics in Privacy Enhancing Technologies*.

Fine, G. A. (1993). The sad demise, mysterious disappearance, and glorious triumph of symbolic interactionism. *Annual review of sociology*, *19*(1), 61-87.

Finn, R. L. (2011). Surveillant staring: Race and the everyday surveillance of South Asian women after 9/11. Surveillance & Society, 8(4), 413-426.

Flammia, M. (1993). The challenge of getting technical experts to talk: Why interviewing skills are crucial to the technical communication curriculum. *IEEE transactions on professional communication*, *36*(3), 124-129.

Fonhof, A. M., van der Bruggen, M., & Takes, F. W. (2018, December). Characterizing key players in child exploitation networks on the dark net. In *International Conference on Complex Networks and their Applications* (pp. 412-423). Springer, Cham.

Foucault, M. (1991). *The Foucault effect: Studies in governmentality*. University of Chicago Press.

Foucault, M. (2007). *Security, territory, population: lectures at the Collège de France, 1977-78*. Springer.

Foucault, M., (2008). *The birth of biopolitics: lectures at the Collège de France, 1978-1979*. Springer.

Foucault, M., (2010). *The government of self and others: Lectures at the Collège de France 1982–1983*. Springer.

Foucault, M. (2012). *Discipline and punish: The birth of the prison*. Vintage.

Friedman, B. (Ed.). (1997). *Human values and the design of computer technology* (No. 72). Cambridge University Press.

Furnell, S. M. (2001). The problem of categorising cybercrime and cybercriminals. In *2nd Australian information warfare and security conference* (Vol. 2001).

Gandy, O. H. (2007). Data mining and surveillance in the post 9/11 environment. *The surveillance studies reader*, 147-157.

Gane, N. (2012). The governmentalities of neoliberalism: panopticism, post-panopticism and beyond. *The Sociological Review*, *60*(4), 611-634.

Gane, N. (2014). The emergence of neoliberalism: Thinking through and beyond Michel Foucault's lectures on biopolitics. *Theory, Culture & Society*, *31*(4), 3-27.

Garland, D. (1997). Governmentality'and the problem of crime: Foucault, criminology, sociology. *Theoretical criminology*, *1*(2), 173-214.

Garland, D. (2001). The culture of control: Crime and social order in contemporary society. University of Chicago Press.

Garland, D. (2012). *Punishment and modern society: A study in social theory*. University of Chicago Press.

Garrow, D. J. (2015). *Liberty and sexuality: The right to privacy and the making of Roe v. Wade*. Open Road Media.

Garsten, C., & Nyqvist, A. (2013). *Organisational anthropology: Doing ethnography in and among complex organisations*. Pluto Press.

Geertz, C. (1973). *The Interpretation of Cultures : Selected Essays*. New York :Basic Books

Geertz, C. (2008). Thick description: Toward an interpretive theory of culture. In *The cultural geography reader* (pp. 41-51). Routledge.

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society*, 18(7), 1219-1235.

Gehl, R. W. (2018a). *Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P*. MIT Press.

Gehl, R. W. (2018b). Archives for the Dark Web: A Field Guide for Study. In *Research Methods for the Digital Humanities* (pp. 31-51). Palgrave Macmillan, Cham.

Gehl, R., & McKelvey, F. (2019). Bugging out: darknets as parasites of large-scale media objects. *Media, Culture & Society*, *41*(2), 219-235.

Gibson, W., (1984), *Neuromancer*, Ace

Giddens, A. (1991). *Modernity and self-identity*. Stanford: Stanford University Press.

Gilbert, M., & Dasgupta, N. (2017). Silicon to syringe: Cryptomarkets and disruptive innovation in opioid supply chains. International Journal of Drug Policy, 46, 160-167.

Gillespie, T. (2010). The politics of 'platforms'. *New media & society*, *12*(3), 347-364.

Gillespie, T. (2018). Platforms are not intermediaries. *Georgetown Law Technology Review*, *2*(2).

Gillespie, T., & Seaver, N. (2016). Critical algorithm studies: A reading list. *Social Media Collective*.

Goedhart, N. S., Broerse, J. E., Kattouw, R., & Dedding, C. (2019). 'Just having a computer doesn't make sense': The digital divide from the perspective of mothers with a low socio-economic position. *New Media & Society*, 21(11–12), 2347–2365.

Goffman, E. (1961), *Asylums.* NY: Anchor

Goffman, E. (1963), *Behaviour in public places*. Englewood Cliffs, NJ: Prentice Hall

Goffman, E. (1967), *Interactional rituals*. NY: Anchor

Goffman, E. (1974), *Frame analysis*, Cambridge: Harvard University Press

Goffman, E. (1978). *The presentation of self in everyday life* (p. 56). London: Harmondsworth.

Goffman, E. (1983). The interaction order. *American Sociological Review 48*(1), 5-13

Goffman, E. (1986). *Stigma: Notes on the management of spoiled identity*. Simon and Schuster.

Goldschlag, D. M., Reed, M. G., & Syverson, P. F. (1996, May). Hiding routing information. In *International workshop on information hiding* (pp. 137-150). Springer, Berlin, Heidelberg.

Goodnight, G. Thomas, and Sandy Green. (2010), Rhetoric, risk, and markets: The dot-com bubble. *Quarterly Journal of Speech* 96(2), 115-140.

Grabosky, P. (1998). Crime in cyberspace. Combating transnational crime: Concepts, activities and responses, 195-208.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles?. Social & Legal Studies, 10(2), 243-249.

Graham, S., & Thrift, N. (2007). Out of order: Understanding repair and maintenance. *Theory, Culture & Society*, *24*(3), 1-25.

Graham, S., & Wood, D. (2003). Digitizing surveillance: categorization, space, inequality. Critical social policy, 23(2), 227-248.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. Macmillan.

Guardian (2013), NSA Files – Tor: 'the king of high-security, low latency anonymity', *The Guardian*, Retreived from: https://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity

Guardian, (2018), The Cambridge Analytica Files , *The Guardian*, https://www.theguardian.com/news/series/cambridge-analytica-files

Guardian (2019), The Guardian SecureDrop, *The Guardian*, Retrieved from: https://www.theguardian.com/securedrop

Gueddana, W., & Ayadi, N. Y. (2015). D4:'An exploratory Platform in the Making': Requirements for creating a partially automated analytical tool. *Network*, *23*, 02.

Gürses, S., Kundnani, A., & Van Hoboken, J. (2016). Crypto and empire: the contradictions of counter-surveillance advocacy. *Media, Culture & Society*, *38*(4), 576-590.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods*, *18*(1), 59-82.

Guttentag, D. (2015). Airbnb: disruptive innovation and the rise of an informal tourism accommodation sector. *Current issues in Tourism*, *18*(12), 1192-1

Hacking, I. (2004). Between Michel Foucault and Erving Goffman: between discourse in the abstract and face-to-face interaction. *Economy and society*, 33(3), 277-302.

Hadjistavropoulos, T., & Smythe, W. E. (2001). Elements of risk in qualitative research. *Ethics & Behavior*, *11*(2), 163-174.

Hall, S. (1986). Variants of liberalism. *Politics and ideology*, 34-69.

Hall, S., Critcher, C., Jefferson, T., Clarke, J., & Roberts, B. (2013). *Policing the crisis: Mugging, the state and law and order*. Macmillan International Higher Education.

Hand, M. and Sandywell, B. 2002, E-topia as Cosmopolis or Citadel On the Democratizing and De-democratizing Logics of the Internet, or, Toward a Critique of the New Technological Fetishism, Theory, Culture & Society, Vol. 19(1–2): 197–225 [0263-2764(200204)19:1–2;197–225;023254]

Haraway, Donna (1991) 'A Cyborg Manifesto: Science, Technology, and Socialist-feminism in the Late Twentieth Century', pp. 149–181 in *Simians, Cyborgs and Women: The Reinvention of Nature*. New York: Routledge.

Haraway, D. J. (1997). *Modest_Witness@Second_Millennium.FemaleMan Meets OncoMouse: Feminism and technoscience*. New York: Routledge.

Harré, R. (2002). Material objects in social worlds. *Theory, Culture & Society*, 19(5-6), 23-33.

Harvey, D. (2007). *A brief history of neoliberalism*. Oxford University Press, USA.

Haynor, A. L. (1989). Micro-macro integration in sociology: Whither progress?. In *Sociological Forum* (Vol. 4, No. 3, pp. 447-453). Springer Netherlands.

Hayward, K. (2007). Situational crime prevention and its discontents: rational choice theory versus the 'culture of now'. *Social Policy & Administration*, 41(3), 232-250.

Hayward KJ (2012) Five spaces of cultural criminology. British Journal of Criminology 52(3): 441-462.

Haywood, D. (2012). The Ethic of the Code: An Ethnography of a "Humanitarian Hacking" Community. *Journal of Peer Production*, 3, 1-10.

Healy, K. (2015). The performativity of networks. *European Journal of Sociology/Archives Européennes de Sociologie*, *56*(2), 175-205.

Heisenberg, D. (2005). *Negotiating privacy: The European Union, the United States, and personal data protection* (pp. 51-73). Boulder, CO: Lynne Rienner Publishers.

Hillyard, P. (2004). *Beyond criminology: Taking harm seriously*. London: Pluto Press; Black Point, NS: Fernwood Pub..

Hinduja, S. (2012). The Heterogeneous Engineering of Music Piracy: Applying Actor-Network Theory to Internet-Based Wrongdoing. *Policy & Internet*, 4(3-4), 229-248.

Hine, C. (2008). Virtual ethnography: Modes, varieties, affordances. *The SAGE handbook of online research methods*, 257-270.

Hine, C. (2015). *Ethnography for the internet: Embedded, embodied and everyday*. Bloomsbury Publishing.

Hintz, A., & Milan, S. (2017). Through a Glass, Darkly: Everyday Acts of Authoritarianism in the Liberal West.

Hoar, P., & Hope, W. (2002). The internet, the public sphere and the 'digital divide'in New Zealand. *Journal of International Communication*, *8*(2), 64-88.

Hoepman, J. H., & Jacobs, B. (2008). Increased security through open source. *arXiv preprint arXiv:0801.3924*.

Holstein, J. A., & Gubrium, J. F. (1995). *The active interview* (Vol. 37). Sage.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1-25.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20-40.

Holt, T. J., Burruss, G. W., & Bossler, A. (2015). Policing cybercrime and cyberterror. *Criminal Justice and Criminology Faculty Publications*, Paper 70

Holt, T. J., Freilich, J. D., & Chermak, S. M. (2017). Exploring the subculture of ideologically motivated cyber-attackers. Journal of contemporary criminal justice, 33(3), 212-233.

Holt, T. J., Brewer, R., & Goldsmith, A. (2019). Digital drift and the "sense of injustice": Counter-productive policing of youth cybercrime. *Deviant Behavior*, *40*(9), 1144-1156.

Honeywell, L, (2016), No more rock stars: how to stop abuse in tech communities, *Leigh Honeywell's Blog,* Retrieved from: https://hypatia.ca/2016/06/21/no-more-rock-stars/

Howard, P. N., & Parks, M. R. (2012). Social media and political change: Capacity, constraint, and consequence. *Journal of Communication*, 62(2), 359-362

Hughes, E. (1993). *A cypherpunk's manifesto.* Retrieved from: *http://www.activism.net/cypherpunk/manifesto.html*.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'Net'?. *Current Issues in Criminal Justice*, 20(3), 433-452.

Hutchings, A., & Chua, Y. T. (2016). Gendering cybercrime. In *Cybercrime through an interdisciplinary lens* (pp. 181-202). Routledge.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, *37*(10), 1163-1178.

Introna, L. D. (1997). On cyberspace and being: identity, self, and hyperreality. *Philosophy in the Contemporary World*, *4*(1/2), 16-25.

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer*, *51*(8), 56-59.

Jardine, E. (2015). The Dark Web dilemma: Tor, anonymity and online policing. *Global Commission on Internet Governance Paper Series*, (21).

Jardine, E. (2018). Tor, what is it good for? Political repression and the use of online anonymity-granting technologies. *New media & society*, *20*(2), 435-452.

Jesiek, B. (2003). Democratizing software: Open source, the hacker ethic, and beyond. *First Monday*, *8*(10).

Jewkes, Y. (2008). The role of the Internet in the twenty-first-century prison: insecure technologies in secure spaces. In *Technologies of InSecurity* (pp. 185-202). Routledge-Cavendish.

Jewkes, Y., & Yar, M. (2012). Policing cybercrime: emerging trends and future challenges. In *Handbook of policing* (pp. 608-634). Willan.

Joerges, B. (1999). Do politics have artefacts?. *Social studies of science*, *29*(3), 411-431.

Jones, S. (2017). Disrupting the narrative: immersive journalism in virtual reality. *Journal of Media Practice*, *18*(2-3), 171-185.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780.

Just, N., & Latzer, M. (2017). Governance by algorithms: reality construction by algorithmic selection on the Internet. Media, Culture & Society, 39(2), 238-258.

Kahler, M. (Ed.). (2011). *Networked politics: agency, power, and governance*. Cornell University Press.

Kamphausen, G., & Werse, B. (2019). Digital figurations in the online trade of illicit drugs: a qualitative content analysis of darknet forums. *International Journal of Drug Policy*.

Kehl, D., Wilson, A., & Bankston, K. (2015). Doomed to repeat history? Lessons from the Crypto Wars of the 1990s. *Open Technology Institute Policy Paper, June*.

Kelty, C. M. (2008). *Two bits: The cultural significance of free software*. Duke University Press.

Kim, S. (2011). The diffusion of the Internet: Trend and causes. *Social Science Research*, *40*(2), 602-613.

Kim, Y. (2011). The pilot study in qualitative inquiry: Identifying issues and learning lessons for culturally competent research. *Qualitative Social Work*, *10*(2), 190-206.

Kohl, U. (2013). Google: the rise and rise of online intermediaries in the governance of the Internet and beyond (Part 2). *International Journal of Law and Information Technology*, 21(2), 187-234.

Kozinets, R. V. (2010). *Netnography: Doing ethnographic research online*. Sage publications.

Kvale, S. (1996). *InterViews: an introduction to qualitive research interviewing*. Sage.

Kvale, S., & Brinkmann, S. (2009). *Interviews: Learning the craft of qualitative research interviewing*. Sage.

Ladegaard, I. (2017). We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets. The British Journal of Criminology, 58(2), 414-433.

Ladegaard, I. (2019). "I pray that we will find a way to carry on this dream": How a law enforcement crackdown united an online community. Critical sociology, 45(4-5), 631-646.

Laidlaw, E.B. (2012). The responsibilities of free speech regulators: an analysis of the Internet Watch Foundation. *International Journal of Law and Information Technology*, *20*(4), 312-345.

Lanchester, J. (2019), Document number nine, *London Review of Books*, Retrieved from: https://www.lrb.co.uk/v41/n19/john-lanchester/document-number-nine

Laterza, V. (2018). Cambridge Analytica, independent research and the national interest. *Anthropology Today*, *34*(3), 1-2.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Harvard university press.

Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford university press.

Latour, B. (2007) 'Turning around politics: a note on Gerard de Vries' paper', *Social Studies of Science*, 37 (5): 811–20.

Laudel, G., & Gläser, J. (2007). Interviewing scientists. *Science, Technology & Innovation Studies*, *3*(2).

Law, J., & Singleton, V. (2000). Performing technology's stories: On social constructivism, performance, and performativity. *Technology and Culture*, *41*(4), 765-775.

Law, J., & Singleton, V. (2005). Object lessons. *Organization*, 12(3), 331-355.

Law, J. (2009). Actor network theory and material semiotics. *Social theory*, 141.

Lave, J (1991). Situating learning in communities of practice. *Perspectives on socially shared cognition*, 2, 63-82.

Lazarus, S. (2019). Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework. *International Social Science Journal*.

Lee, M. (2014), Fact-checking Pando's smears against Tor, *Micah Lee's Blog*, Retreived from: https://micahflee.com/2014/12/fact-checking-pandos-smears-against-tor/

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22-31.

Levine, Y. (2014), Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government, *Pando*, https://pando.com/2014/07/16/tor-spooks/

Lemke, T. (2015). *Foucault, governmentality, and critique*. Routledge.

Levi, M., & Leighton Williams, M. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the UK information assurance network cooperation space. *Information Management & Computer Security*, *21*(5), 420-443.

Leizerov, S. (2000). Privacy advocacy groups versus Intel: A case study of how social movements are tactically using the Internet to fight corporations. *Social science computer review*, *18*(4), 461-483.

Lemke, T. (2001) 'The birth of bio-politics': Michel Foucault's lecture at the Collège de France on neo-liberal governmentality, *Economy and Society*, 30:2, 190-207,

Lessig, L. (1999a). Code is law. *The Industry Standard*, *18*.

Lessig, L. (1999b). Code and Other Laws of Cyberspace. New York: Basic Books

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263-280.

Levina, M., & Hasinoff, A. A. (2017). The Silicon Valley ethos: Tech Industry products, discourses, and practices. *Television & New Media*, *18*(6), 489-495.

Levy, S. (1984). *Hackers: Heroes of the computer revolution* (Vol. 14). Garden City, NY: Anchor Press/Doubleday.

Levy, S. (1996). Crypto rebels. *High noon on the electronic frontier*, 185-205.

Lewis, S.J., (2017), *Queer Privacy,* https://leanpub.com/queerprivacy

Lewis, R., Rowe, M., & Wiper, C. (2016). Online abuse of feminists as an emerging form of violence against women and girls. *British journal of criminology*, *57*(6), 1462-1481.

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet*, *10*(4), 415-453.

Licoppe, C. (2010). The 'performative turn'in science and technology studies: Towards a linguistic anthropology of 'technology in action'. *Journal of Cultural Economy*, *3*(2), 181-188.

Lippert, R., & Stenson, K. (2010). Advancing governmentality studies: Lessons from social constructionism. Theoretical criminology, 14(4), 473-494.

Lischka, J. A. (2015). Surveillance discourse in UK broadcasting since the Snowden revelations. *Digital Citizenship and Surveillance Society Media Stream.(Discussion paper). http://www. dcssproject. net/files/2015/12/DCSS_Broadcasting-report. pdf*.

Littig, B. (2009). Interviewing the elite—Interviewing experts: Is there a difference?. In *Interviewing experts* (pp. 98-113). Palgrave Macmillan, London.

Licoppe, C. (2010). The 'performative turn' in Science and Technology Studies, Journal of Cultural Economy, 3:2, 181-188, DOI: 10.1080/17530350.2010.494122

Liebling, A. (2015). Appreciative inquiry, generative theory, and the 'failed state prison'. *Qualitative Research in Criminology. Advances in Criminological Theory. New Brunswick: Transaction Publishers*, 251-269.

Ljungberg, J. (2000). Open source movements as a model for organising. *European Journal of Information Systems*, *9*(4), 208-216.

Loader, I. (2005). Fall of the 'platonic guardians' liberalism, criminology and political responses to crime in England and Wales. *British Journal of Criminology*, *46*(4), 561-586.

Loll, A. (2016), Power, secrecy and cypherpunks: how Jacob Appelbaum ripped Tor apart, *The Guardian*, Retrieved from: https://www.theguardian.com/technology/2016/oct/11/jacob-appelbaum-tor-project-sexual-assault-allegations

Lorenzo-Dus, N., & Di Cristofaro, M. (2018). 'I know this whole market is based on the trust you put in me and I don't take that lightly': Trust, community and discourse in crypto-drug markets. *Discourse & Communication,* 12(6), 608-626.

Luckman, S. (1999). (En) gendering the digital body: Feminism and the Internet. *Hecate*, *25*(2), 36.

Luppicini, R. (2014). Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research. *Global Media Journal: Canadian Edition,* 7(1).

Lusthaus, J. (2013). How organised is organised cybercrime?. *Global Crime*, *14*(1), 52-60.

Lyon, D., & Zureik, E. (1996). Surveillance, privacy, and the new technology. *Computers, surveillance, and privacy*, 1-18.

Lyon, D. (2002). Surveillance Studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society*, 1(1), 1-7.

Lyon, D. (2007). Surveillance, security and social sorting: emerging research priorities. *International criminal justice review*, *17*(3), 161-170.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 2053951714541861.

Lyon, D. (2015). *Surveillance after Snowden*. John Wiley & Sons.

Lyon, D. (2017). Digital citizenship and surveillance| surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, *11*, 19.

Mackenzie, A. (2005). The performativity of code: software and cultures of circulation. *Theory, Culture & Society*, *22*(1), 71-92.

MacKenzie, D. (2006). Is economics performative? Option theory and the construction of derivatives markets. *Journal of the history of economic thought*, *28*(1), 29-55.

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. *Information, Communication & Society*, 19(1), 111-126.

Mair, G. (2013). Technology and the future of community penalties. In *Community Penalties* (pp. 182-196). Willan.

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. *Deviant Behavior*, *35*(7), 581-591.

Maréchal, N. (2015). Ranking digital rights: Human rights, the Internet and the fifth estate. *International Journal of Communication*, *9*(10), 3440-3449.

Marechal (2018). PhD Thesis: Use Signal, Use Tor? The Political Economy of Digital Rights Technology

Matthews, F. H. 1977: *Quest for an American Sociology: Robert E. Park and the Chicago Schoo*l. London: McGill Queen's University Press

Marwick, A. (2017). Silicon Valley and the social media industry. *Sage Handbook of Social Media. London: Sage*.

McCoy, D. et al. (2008), Shining light in dark places: understanding the Tor network" In *International Symposium on Privacy Enhancing Technologies Symposium* (pp 63-67). Springer, Berlin, Heidelberg

McDonald, H, (2016), Boston College ordered by US court to hand over IRA tapes, *The Guardian*, Retreived from: https://www.theguardian.com/uk-news/2016/apr/25/boston-college-ordered-by-us-court-to-hand-over-ira-tapes

McGuire, M. R. (2016). Cybercrime 4.0: now what is to be done?. In *What is to Be Done About Crime and Punishment?* (pp. 251-279). Palgrave Macmillan, London.

McIlwain, C. (2019). *Black Software: The Internet and Racial Justice, from the AfroNet to Black Lives Matter*. Oxford University Press, USA.

McLaughlin, P. (2016). Crypto Wars 2.0: Why Listening to Apple on Encryption Will Make America More Secure. *Temp. Int'l & Comp. LJ*, *30*, 353.

Melvin, A. O., & Ayotunde, T. (2011). Spirituality in cybercrime (Yahoo Yahoo) activities among youths in South West Nigeria. In *Youth culture and net culture: Online social practices* (pp. 357-380). IGI Global.

Mead, G. H. (1934). Mind, self, and society: From the standpoint of a social behaviorist (*Works of George Herbert Mead, Vol. 1*). University of Chicago Press

Mead, G. H. (1964) "The Objective Reality of Perspectives," in A.J. Reck (ed), *Selected Writings of George Herbert Mead* (Chicago: University of Chicago Press): 306–19.

Milan, S. (2013). *Social movements and their technologies: Wiring social change*. Springer.

Milan, S. (2016). Stealing the Fire. Communication for Development from the Margins of Cyberspace. *Voice & Matter. Communication, Development and the Cultural Return, edited by Thomas Tufte and Oscar Hemer, NORDICOM*, 59-70.

Milan, S., & Van Der Velden, L. (2016). The alternative epistemologies of data activism. *Digital Culture & Society*, *2*(2), 57-74.

Milan, S., & ten Oever, N. (2017). Coding and encoding rights in internet infrastructure. *Internet Policy Review*, *6*(1).

Milivojevic, S. (2019a). 'Stealing the fire', 2.0 style? Technology, the pursuit of mobility, social memory and de-securitization of migration. *Theoretical Criminology*, *23*(2), 211-227.

Milivojevic, S. (2019b). *Border Policing and Security Technologies: Mobility and Proliferation of Borders in the Western Balkans*. Routledge.

Minárik, T., & Osula, A. M. (2016). Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law. *Computer Law & Security Review*, *32*(1), 111-127.

Mohanty, C. T. (2013). Transnational feminist crossings: On neoliberalism and radical critique. *Signs: Journal of Women in Culture and Society*, *38*(4), 967-991.

Mol, A. (2010). Actor-network theory: Sensitive terms and enduring tensions. *Kölner Zeitschrift für Soziologie und Sozialpsychologie. Sonderheft*, *50*, 253-269.

Monsees, L. (2019). *Crypto-Politics: Encryption and Democratic Practices in the Digital Era*. Routledge.

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. Survival, 58(1), 7-38

Moore, M. (2016). Tech giants and civic power. *Centre for the Study of Media, Communication and Power." King's College London*.

Moore, M., & Tambini, D. (Eds.). (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. Oxford University Press.

Monteiro, E., & Hanseth, O. (1996). Social shaping of information infrastructure: on being specific about the technology. In *Information technology and changes in organizational work* (pp. 325-343). Springer, Boston, MA.

Mueller, R. S. (2019). Report on the investigation into Russian interference in the 2016 presidential election. *US Dept. of Justice. Washington, DC*.

Munksgaard, R., & Demant, J. (2016). Mixing politics and crime–The prevalence and decline of political discourse on the cryptomarket. *International Journal of Drug Policy*, *35*, 77-83.

Murdoch, SJ & Danezis, G. (2005). Low-cost traffic analysis of Tor. In *2005 IEEE Symposium on Security and Privacy* (S&P05) (pp. 183-195). IEEE

Murdoch, J. (1998). The spaces of actor-network theory. *Geoforum*, *29*(4), 357-374.

Murdoch, S. J., & Kadianakis, G. (2012). Pluggable transports roadmap. *The Tor Project, Tech. Rep*, 03-003.

Murphy, E., & Dingwall, R. (2001). The ethics of ethnography. *Handbook of ethnography*, 339-351.

Musiani, F. (2013). Network architecture as internet governance. *Internet Policy Review*.

Musiani, F. (2010). Privacy as invisibility: pervasive surveillance and the privatization of peer-to-peer systems. *TripleC*, *9*(2), 126-140.

Musiani, F. (2012). Caring about the plumbing: On the importance of architectures in social studies of (peer-to-peer) technology. *Journal of peer production*, *1*(online), 8-p.

Musiani, F. (2015). Practice, plurality, performativity, and plumbing: Internet governance research meets science and technology studies. *Science, Technology, & Human Values*, *40*(2), 272-286.

Musiani, F., Cogburn, D. L., DeNardis, L., & Levinson, N. S. (Eds.). (2016). *The turn to infrastructure in Internet governance*. Springer.

Myers, D. (1987). "Anonymity is part of the magic": Individual manipulation of computer-mediated communication contexts. *Qualitative Sociology*, *10*(3), 251-266.

Nafus, D. (2012). 'Patches don't have gender': What is not open in open source software. *New Media & Society*, *14*(4), 669-683.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*.

Nakamura, L. (2013). *Cybertypes: Race, ethnicity, and identity on the Internet*. Routledge.

Nakamura, L., & Lovink, G. (2005). Talking race and cyberspace: An interview with Lisa Nakamura. *Frontiers: A Journal of Women Studies*, *26*(1), 60-65.

Nellis, M., Beyens, K., & Kaminski, D. (Eds.). (2013). *Electronically monitored punishment: International and critical perspectives*. Routledge.

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and philosophy*, *17*(5), 559-596.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New media & society*, *6*(2), 195-217.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32-48.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. NYU Press.

Nye, J. S. (2004). Soft power. In *Power in the global information age* (pp. 76-88). Routledge.

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Broadway Books.

Orlikowski, W. J. (2005). Material works: Exploring the situated entanglement of technological performativity and human agency. *Scandinavian Journal of Information Systems*, *17*(1), 6.

Pastrana, S., Hutchings, A., Caines, A., & Buttery, P. (2018, September). Characterizing eve: Analysing cybercrime actors in a large underground forum. In *International Symposium on Research in Attacks, Intrusions, and Defenses* (pp. 207-227). Springer, Cham.

Pfitzmann, A., & Hansen, M. (2005). Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology.

Pickard, V. (2007) Neoliberal visions and revisions in global communications policy from NWICO to WSIS, Journal of Communication Inquiry, 31(2), 118-139

Pinch, T. (2010). The invisible technologies of Goffman's sociology from the merry-go-round to the internet. *Technology and culture*, *51*(2), 409-424.

Pink, S. (2016). Digital ethnography. *Innovative methods in media and communication research*, 161-165.

Plummer, K. (2000). A world in the making: Symbolic interactionism in the twentieth century. *A Companion to Social Theory. 2nd ed, Blackwell* 193-222.

Pothineni, D., Mishra, P., Rasheed, A., & Sundararajan, D. (2014, April). Incentive design to mould online behavior: a game mechanics perspective. In *Proceedings of the First International Workshop on Gamification for Information Retrieval* (pp. 27-32). ACM.

Pollock, N., & Williams, R. (2008). *Software and organisations: The biography of the enterprise-wide system or how SAP conquered the world*. Routledge.

Pollock, N., & Williams, R. (2010). E-infrastructures: How do we know and understand them? Strategic ethnography and the biography of artefacts. *Computer Supported Cooperative Work (CSCW)*, *19*(6), 521-556.

Postill, J. (2014). Freedom technologists and the new protest movements: A theory of protest formulas. *Convergence*, *20*(4), 402-418.

Powell, A. (2012). Democratizing production through open source knowledge: from open software to open hardware. *Media, Culture & Society*, *34*(6), 691-708.

Raab, C. D. (1997). Privacy, democracy, information. *The Governance of Cyberspace, London: Routledge*, 155-74.

Raab, C. D., Jones, R., & Székely, I. (2015). Surveillance and resilience in theory and practice. *Media and Communication*, *3*(2).

Rapp, L., Button, D. M., Fleury-Steiner, B., & Fleury-Steiner, R. (2010). The internet as a tool for black feminist activism: Lessons from an online antirape protest. *Feminist Criminology*, *5*(3), 244-262.

Rawlinson, K. (2015), Banning Tor unwise and infeasible, MPs told, *BBC News*, Retrieved from: https://www.bbc.co.uk/news/technology-31816410

The Register, (2017), Tor loses a node in Russia after activist's arrest in Moscow, https://www.theregister.co.uk/2017/04/13/tor_loses_a_node_in_russia_after_activists_arrest_in_moscow/

Reiman, J., & Leighton, P. (2015). *Rich Get Richer and the Poor Get Prison, The (Subscription): Ideology, Class, and Criminal Justice*. Routledge.

Reyns, B. W. (2010). A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers. *Crime Prevention and Community Safety*, *12*(2), 99-118.

Rider, K. (2018) The privacy paradox: how market privacy facilitates government surveillance, *Information, Communication & Society, 21*(10), 1369-1385.

Ritchie, J., Lewis, J., Nicholls, C. M., & Ormston, R. (Eds.). (2013). *Qualitative research practice: A guide for social science students and researchers*. sage.

Ritzer, G. (2015). Prosumer capitalism. *The Sociological Quarterly*, *56*(3), 413-445.

Ritzer, G., Dean, P., & Jurgenson, N. (2012). The coming of age of the prosumer. *American behavioral scientist*, *56*(4), 379-398.

Ritzer, G., & Jurgenson, N. (2010). Production, consumption, prosumption: The nature of capitalism in the age of the digital 'prosumer'. *Journal of consumer culture*, *10*(1), 13-36.

Rivest, R. L. (1998). The case against regulating encryption technology. *Scientific American*, *279*(4), 116-117.

Rock, P. (Ed.). (1994). *History of criminology*. Aldershot: Dartmouth.

Rogaway, P. (2015). The Moral Character of Cryptographic Work. *IACR Cryptology ePrint Archive*, *2015*, 1162.

Saco, D. (1999). Colonizing Cyberspace:'National Security'and the Internet. *Cultures of insecurity: States, communities, and the production of danger*, *14*, 261.

Salter, M. (2018). From geek masculinity to Gamergate: the technological rationality of online abuse. *Crime, Media, Culture*, *14*(2), 247-264.

Sampson, H. (2004). Navigating the waves: the usefulness of a pilot in qualitative research. *Qualitative research*, *4*(3), 383-402.

Saunders, K. W. (1991). Privacy and Social Contract: A Defense of Judicial Activism in Privacy Cases. *Ariz. L. Rev.*, *33*, 811.

Schafer, B. (2016). Surveillance for the masses: the political and legal landscape of the UK Investigatory Powers Bill. *Datenschutz und Datensicherheit-DuD*, *40*(9), 592-597.

Schlossman, D. (2017). *Actors and Activists: Performance, Politics, and Exchange Among Social Worlds*. Routledge.

Schneier, B. (2014). Metadata= surveillance. *IEEE Security & Privacy*, *12*(2), 84-84.

Schuilenburg, M. (2017). *The securitization of society: crime, risk, and social order* (Vol. 12). NYU Press.

Schulze, M. (2017). Clipper meets Apple vs. FBI: a comparison of the cryptography discourses from 1993 and 2016. *Media and Communication*, *5*(1), 54-62.

Scordato, M., & Monopoli, P. A. (2002). Free Speech Rationales After September 11th: The First Amendment in Post-World Trade Center America. *Stan. L. & Pol'y Rev.*, *13*, 185.

Scott, M. (1994), *Trouble and Her Friends*, Tor

Sherman, L. W. (2009). Evidence and liberty: The promise of experimental criminology. *Criminology & Criminal Justice*, *9*(1), 5-28.

Shibutani, T. (1955) "Reference Groups as Perspectives," American Journal of Sociology 60: 562–9.

Skibell, R. (2002). The myth of the computer hacker. *Information, Communication & Society*, *5*(3), 336-356.

Smith, M., Szongott, C., Henne, B., & Von Voigt, G. (2012). Big data privacy issues in public social media. In 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST) (pp. 1-6). IEEE.

Smythe, William, and Maureen Murray. 2000. Owning the story: Ethical considerations in narrative research. *Ethics and Behaviour* 10 (4): 311–36.

Snader, R. & Borisov, N. (2008). A tune-up for Tor: improving security and performance in the Tor network. In *NDSS* (8): 127

Söderberg, J. (2015). *Hacking capitalism: The free and open source software movement*. Routledge.

Solove, D. (2008). Understanding privacy. Cambridge, MA: Harvard University Press.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.

Sparks, R. (2002). Out of the Digger' The Warrior's Honour and the Guilty Observer. *Ethnography*, *3*(4), 556-581.

Stallman, R. (2002). *Free software, free society: Selected essays of Richard M. Stallman*. Lulu. com.

Star, S. L. (1988). The structure of ill-structured solutions: Boundary objects and heterogeneous distributed problem solving. In Readings in distributed artificial intelligence, ed. M. Huhns and L. Gasser. Menlo Park, CA: Kaufman.

Star, S.L. and Griesemer, J.R., 1989. "Institutional ecology, 'translations' and boundary objects: amateurs and professionals in Berkely's Museum of Vertebrate Zoology, 1907-39", *Social Studies of Science*, 19 (3): 387-420

Star, S. L. (1990). Power, technology and the phenomenology of conventions: on being allergic to onions. *The Sociological Review*, 38(1_suppl), 26-56.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information systems research*, *7*(1), 111-134.

Star, S. L. (1999). The ethnography of infrastructure. *American behavioral scientist*, *43*(3), 377-391.

Star, S. L., & Strauss, A. (1999). Layers of silence, arenas of voice: The ecology of visible and invisible work. Computer supported cooperative work (CSCW), 8(1-2), 9-30.

Star, S. L., Bowker, G. C., & Neumann, L. J. (1998). Transparency at different level of scale: convergence between information artefacts and social worlds. *Library and Information Science, Urbana-Champaign*.

Star, S.L. (2010). This is not a boundary object: Reflections on the origin of a concept. *Science, Technology, & Human Values*, *35*(5), 601-617.

Steijn, W. M., & Vedder, A. (2015). Privacy under construction: A developmental perspective on privacy perception. *Science, Technology, & Human Values*, *40*(4), 615-637.

Steinmetz, K. F. (2016). *Hacked: A radical approach to hacker culture and crime*. NYU Press.

Stenson, K. (2005). Sovereignty, biopolitics and the local government of crime in Britain. Theoretical criminology, 9(3), 265-287.

Sterling, B. (2002). The *Hacker Crackdown,* IndyPublish.com

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and justice in digital society: towards a 'Digital Criminology'?. International Journal for Crime, Justice and Social Democracy, 6(2), 17-33.

Strauss, A (1978) "A Social World Perspective," in Norman Denzin (ed.), Studies in Symbolic Interaction 1: 119–128, Greenwich, CT: JAI Press

Strauss, A., & Corbin, J. (1994). Grounded theory methodology. *Handbook of qualitative research*, *17*, 273-85.

Strauss, A., & Corbin, J. M. (1997). *Grounded theory in practice*. Sage.

Surette R (2015) Performance, crime and justice. Current Issues in Criminal Justice 27(2): 195-216.

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., & Van Geelen, T. (2019). Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online. *Policy & Internet*, *11*(1), 84-103.

Swire, P., & Ahmad, K. (2012). Encryption and Globalization. *Columbia Science and Technology Law Review*, *23*.

Syverson, P. (2009, April). Why I'm not an entropist. In *International Workshop on Security Protocols* (pp. 213-230). Springer, Berlin, Heidelberg.

Taylor, P. (2012). *Hackers: Crime and the digital sublime*. Routledge.

Taylor, I., Walton, P., & Young, J. (2013). *The new criminology: For a social theory of deviance*. Routledge.

Techdirt (2017), Here's What Happened When The Dutch Secret Service Tried To Recruit A Tor Admin, *Techdirt*, Retrieved from: https://www.techdirt.com/articles/20170131/08374336596/heres-what-happened-when-dutch-secret-service-tried-to-recruit-tor-admin.shtml

Teicher, M. (2015). Interviewing Subject Matter Experts. *International Cost Estimating and Analysis Association (ICEAA)*.

Tepper, M. (2013). Usenet communities and the cultural politics of information. In *Internet culture* (pp. 39-54). Routledge.

Tesar, M. (2015). Ethics and truth in archival research. *History of Education*, *44*(1), 101-114.

Thomas, G., & Wyatt, S. (1999). Shaping cyberspace—Interpreting and transforming the Internet. *Research Policy*, *28*(7), 681-698.

Thomson, D., Bzdel, L., Golden-Biddle, K., Reay, T., & Estabrooks, C. A. (2005, January). Central questions of anonymization: A case study of secondary use of qualitative data. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research* (Vol. 6, No. 1).

Thomson, T. (2016), *Rosewater*, Orbit

Tomczak, P. (2016). *The penal voluntary sector*. Routledge.

Tor Project (2019), History, https://www.torproject.org/about/history/ accessed 06/11/2019

Trottier, D., & Fuchs, C. (Eds.). (2014). *Social media, politics and the state: Protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube*. Routledge.

Turner, T. C., Smith, M. A., Fisher, D., & Welser, H. T. (2005). Picturing Usenet: Mapping computer-mediated collective action. *Journal of Computer-Mediated Communication*, *10*(4), JCMC1048.

University of Edinburgh (2019), Research Ethics and Integrity, https://www.ed.ac.uk/arts-humanities-soc-sci/research-ke/support-for-staff/res-ethics-policies/ethics

Unruh, D. R. (1980). The nature of social worlds. *Pacific Sociological Review*, *23*(3), 271-296.

Van Teijlingen, E., & Hundley, V. (2002). The importance of pilot studies. *Nursing Standard (through 2013)*, *16*(40), 33.

Van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: Botnets as hybrid criminal actor-networks. British journal of criminology, 55(3), 578-595.

Vedder, A. (2011). Privacy 3.0. In *Innovating Government* (pp. 17-28). TMC Asser Press.

Venturini, T. (2010). Diving in magma: how to explore controversies with actor-network theory. *Public understanding of science*, *19*(3), 258-273.

Vincent, J., & Haddon, L. (Eds.). (2017). *Smartphone cultures*. Routledge.

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication & Society*, *7*(1), 92-114.

Vold, G. B. (1951). Criminology at the Crossroads. *The Journal of Criminal Law, Criminology, and Police Science*, *42*(2), 155-162.

Von Bernstorff, J. (2003). Democratic global Internet regulation? Governance networks, international law and the shadow of hegemony. European Law Journal, 9(4), 511-526.

Wacquant, L. (2009). *Punishing the poor: The neoliberal government of social insecurity*. duke university Press.

Wacquant, L. (2012). Three steps to a historical anthropology of actually existing neoliberalism. *Social anthropology*, *20*(1), 66-79.

Wachter-Boettcher, S. (2017). *Technically wrong: sexist apps, biased algorithms, and other threats of toxic tech*. WW Norton & Company.

Wagner, B. (2013). Governing Internet Expression: How public and private regulation shape expression governance. *Journal of Information Technology & Politics*, *10*(4), 389-403.

Wall, D. S. (1998). Catching cybercriminals: policing the Internet. *International Review of Law, Computers & Technology*, *12*(2), 201-218.

Wall, D. (1999). Cybercrimes: New wine, no bottles?. In Invisible crimes (pp. 105-139). Palgrave Macmillan, London

Wall, D. (2007). Cybercrime: The transformation of crime in the information age (Vol. 4). Polity.

Wall, D. S. (2012). The devil drives a Lada: The social construction of hackers as cybercriminals. In *Constructing Crime* (pp. 4-18). Palgrave Macmillan, London.

Wall, D. S., & Williams, M. L. (2013). Policing cybercrime: networked and social media technologies and the challenges for policing.

Walton, P., & Young, J. (Eds.). (1998). *The new criminology revisited*. London: Macmillan.

Watson, K. D. (2012). The Tor network: a global inquiry into the legal status of anonymity networks. *Wash. U. Global Stud. L. Rev.*, *11*, 715.

Weeks, J. (1982, October). Foucault for historians. In *History Workshop* (pp. 106-119). Editorial Collective, History Workshop, Ruskin College.

Weis, A. H. (2010). Commercialization of the Internet. *Internet Research*, *20*(4), 420-435.

Weisburd, D. (1997). *Reorienting crime prevention research and policy: From the causes of criminality to the context of crime*. US Department of Justice, Office of Justice Programs, National Institute of Justice.

Weimann, G. (2016). Going dark: Terrorism on the dark web. *Studies in Conflict & Terrorism*, *39*(3), 195-206.

Whittle, A., & Spicer, A. (2008). Is actor network theory critique?. Organization studies, 29(4), 611-629.

Wilding, F., & Cyberfeminist International. (1998). Where is feminism in cyberfeminism*?*, *n.paradoxa. Vol* 2.

Wiles, Rose, Graham Crow, Sue Heath, and Vikki Charles. 2008. The management of confidentiality and anonymity in social research. *International Journal of Social Research Methodology* 11 (5): 417–28.

Williams, J. W., & Lippert, R. (2006). Governing on the margins: Exploring the contributions of governmentality studies to critical criminology in Canada. *Canadian journal of criminology and criminal justice*, *48*(5), 703-720.

Williams, M. L. (2015). Guardians upon high: an application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56(1), 21-48.

Williams, R., Stewart, J., & Slack, R. (2005). *Social learning in technological innovation: Experimenting with information and communication technologies*. Edward Elgar Publishing.

Williams, S. (2015). Digital defense: Black feminists resist violence with hashtag activism. *Feminist Media Studies*, *15*(2), 341-344.

Williams, S. J. (1986). Appraising Goffman. *British Journal of Sociology*, 348-369.

Williams, B. A., Brooks, C. F., & Shmargad, Y. (2018). How algorithms discriminate based on data they lack: Challenges, solutions, and policy implications. *Journal of Information Policy*, *8*, 78-115.

Winner, L. (1999). Do artefacts have politics? The Social Shaping of Technology. DA MacKenzie and J. Wajcman, eds.

Winter, P., & Lindskog, S. (2012). How china is blocking tor. *arXiv preprint arXiv:1204.0447*.

Wood, D. M., & Wright, S. (2015). Before and after Snowden. *Surveillance & Society*, *13*(2), 132-138.

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology*, *28*(3), 277-298.

Yar, M. (2012). Virtual utopias and dystopias: The cultural imaginary of the Internet. *Utopia: Social Theory and the Future*, 179-95.

Yar, M. (2014). *The cultural imaginary of the Internet: virtual utopias and dystopias*. Springer.

Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. European Journal of Criminology, 2(4), 407-427.

Yar, M. (2017). Toward a cultural criminology of the Internet. In Technocrime and criminological theory (pp. 132-148). Routledge.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society*. SAGE Publications Limited.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*, *23*(4), 516-539.

Youmans, W. L., & York, J. C. (2012). Social media and the activist toolkit: User agreements, corporate interests, and the information infrastructure of modern social movements. *Journal of Communication*, *62*(2), 315-329.

Young, J. (1988). Radical criminology in Britain: The emergence of a competing paradigm. *Brit. J. Criminology*, *28*, 159.

Young, J. (2009). Moral Panic, Its Origins in Resistance, Ressentiment and the Translation of Fantasy into Reality. *British Journal of Criminology*, 49(1), 4-16.

Young, J. (2011). Moral panics and the transgressive other. *Crime, media, culture*, 7(3), 245-258.

Zwitter, A. (2014). Big data ethics. *Big Data & Society*, *1*(2), 2053951714559253.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, Public Affairs.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89.

Zureik, E., & Salter, M. (Eds.). (2013). *Global surveillance and policing*. Routledge.

# appendix a
# list of participants

Core Tor developers:

- Participant A – Interview carried out in-person.
- Participant B – Interview carried out over online voice call
- Participant C – Interview carried out over Signal voice call.
- Participant D - Interview carried out in-person.
- Participant E – Interview carried out over email.
- Participant F – Interview carried out over Skype call.
- Participant G – Interview carried out in-person
- Participant H – Interview carried out in-person
- Participant I – Interview carried out over Skype call

Other core contributors to the Tor Project:

- Participant J – Interview carried out over Skype call
- Participant K –Interview carried out over Skype video chat.
- Participant L - Interview carried out over Skype video chat.

Academics and Open Source contributors:

- Participant M – an academic conducting research on Tor. Interview carried out over Skype call.
- Participant N - an Open Source contributor to Tor and a relay operator. Interview carried out over Skype call.

Relay operators:

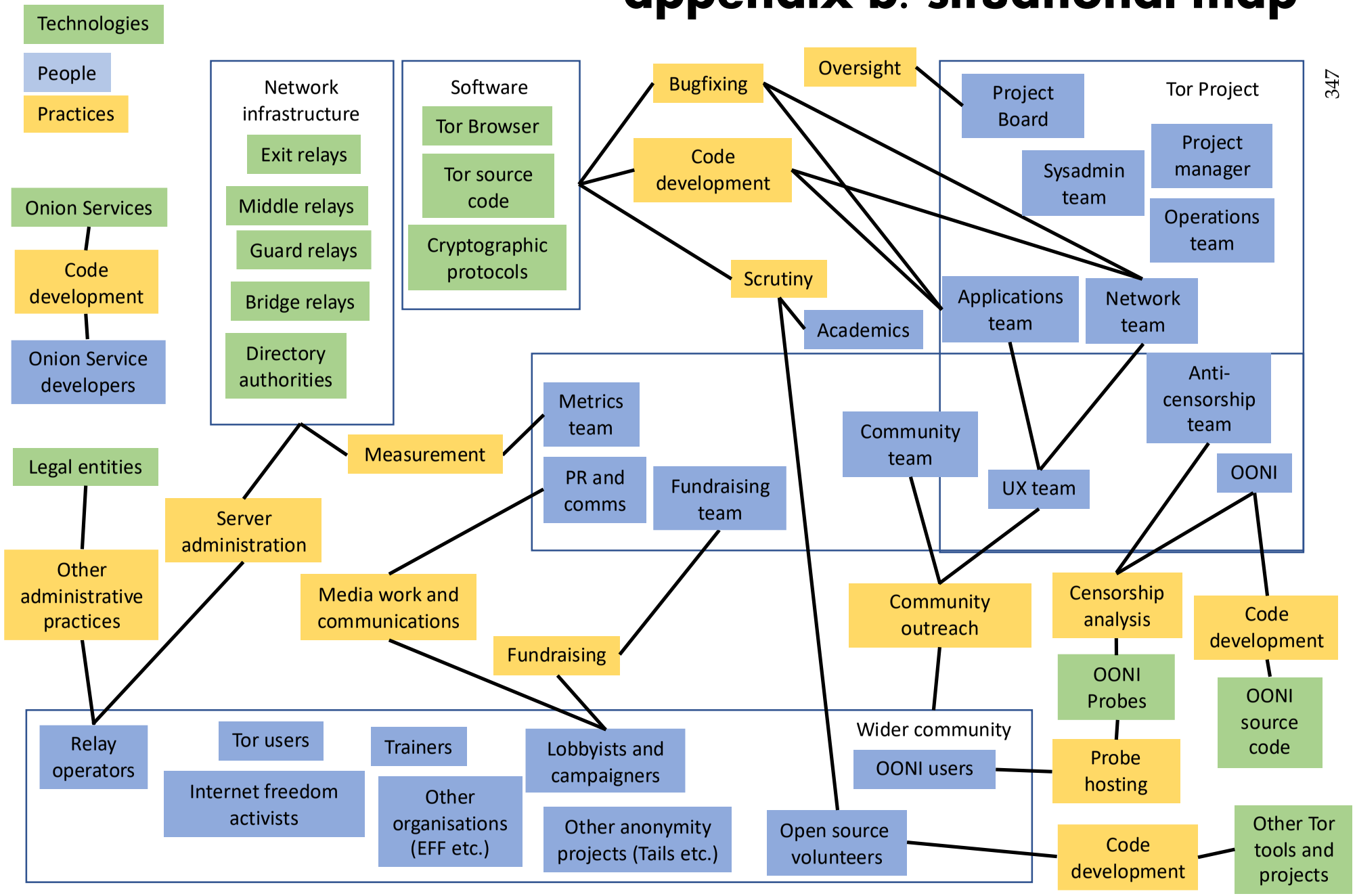
- Participant O – Interview carried out over encrypted XMPP chat.
- Participant P – Interview carried out over Skype text chat.

- Participant Q – Interview carried out over Skype call.
- Participant R – Interview carried out over Skype video chat.
- Participant S – Interview carried out via email.
- Participant T – Interview carried out via email.
- Participant U – also a sysadmin at an Internet Service Provider. Interview carried out in-person.
- Participant V – Interview carried out in-person.
- Participant W – Interview carried out in-person.

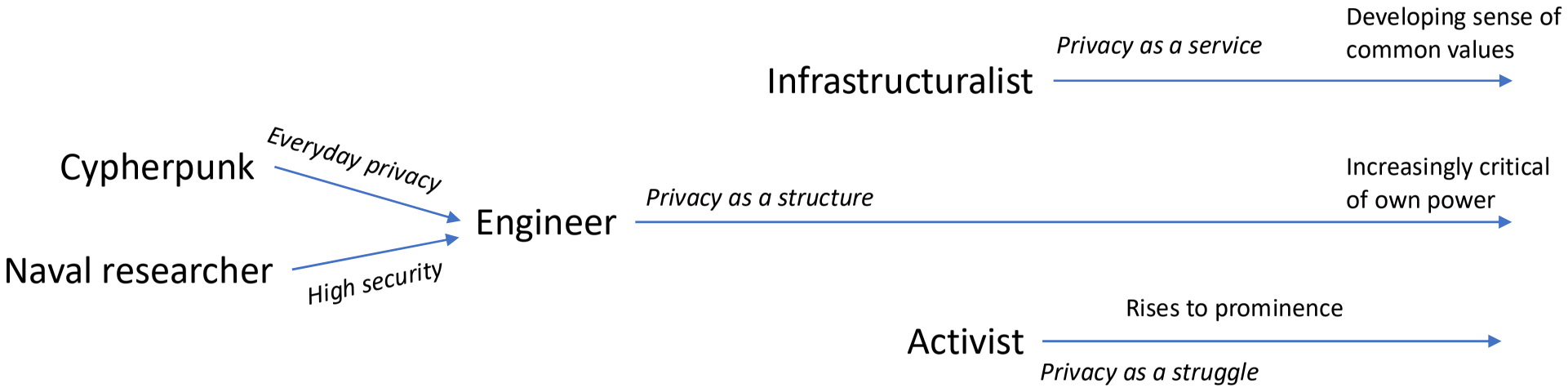
Hidden Service developers:

- Participant X – Interview carried out over Skype video chat.
- Participant Y – Interview carried out over Skype video chat.
- Participant Z – Interview carried out over Skype video chat.

# appendix b: situational map

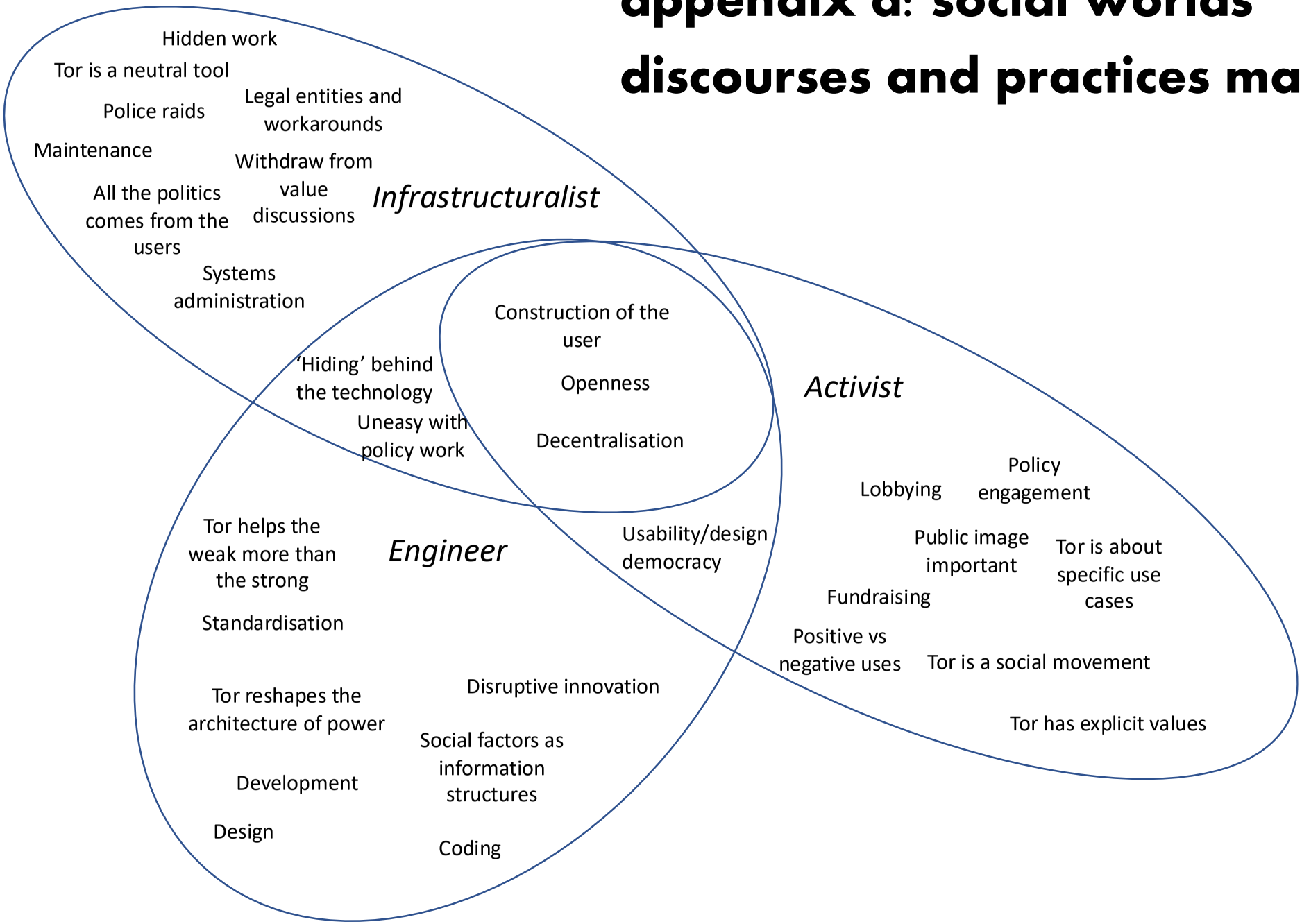


# appendix c: social worlds timeline

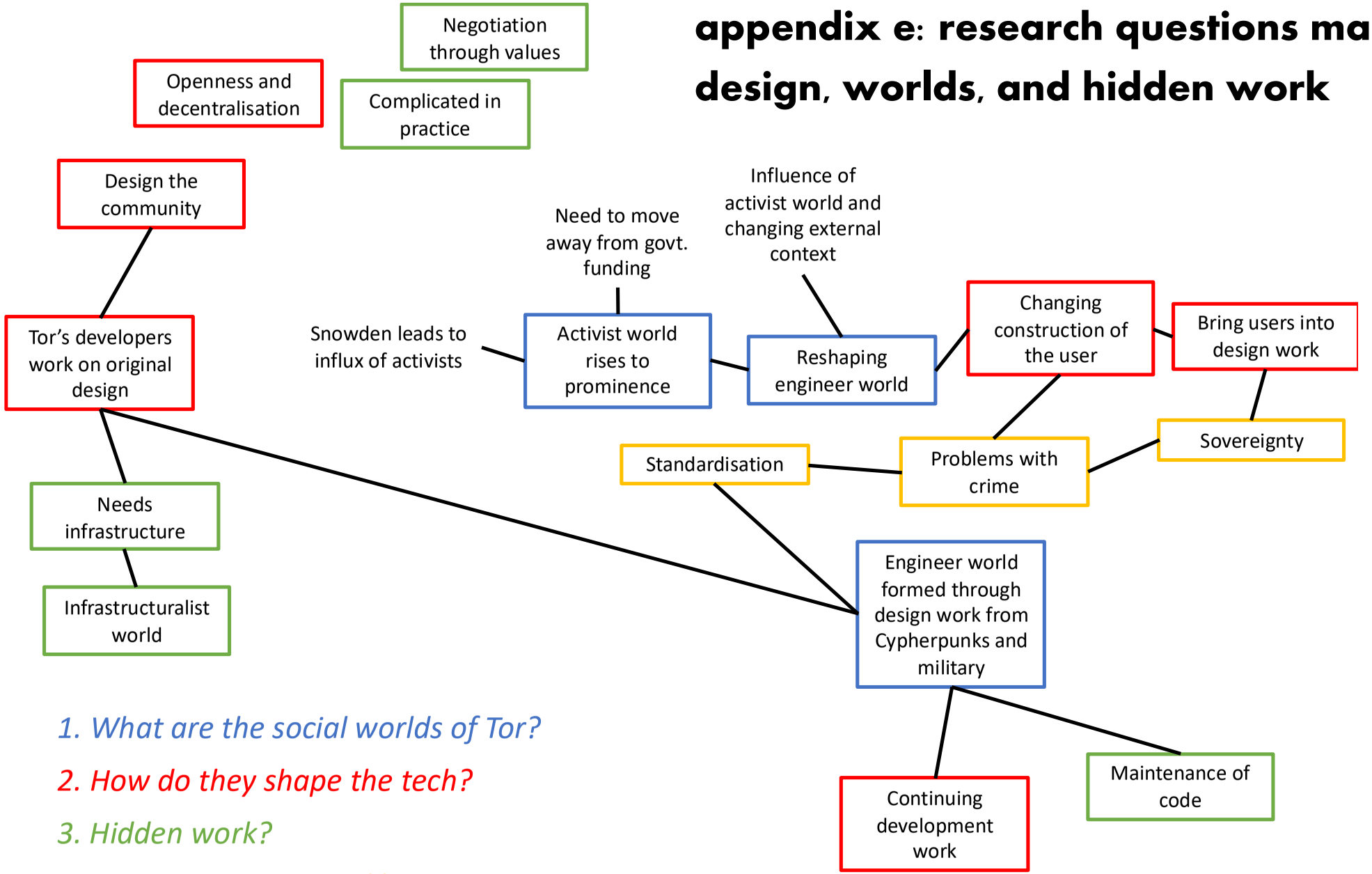



**Onion Routing** | **Tor early development** | **Tor released** | **Snowden revelations**

# appendix d: social worlds discourses and practices map



# appendix e: research questions map - design, worlds, and hidden work




*1. What are the social worlds of Tor?*

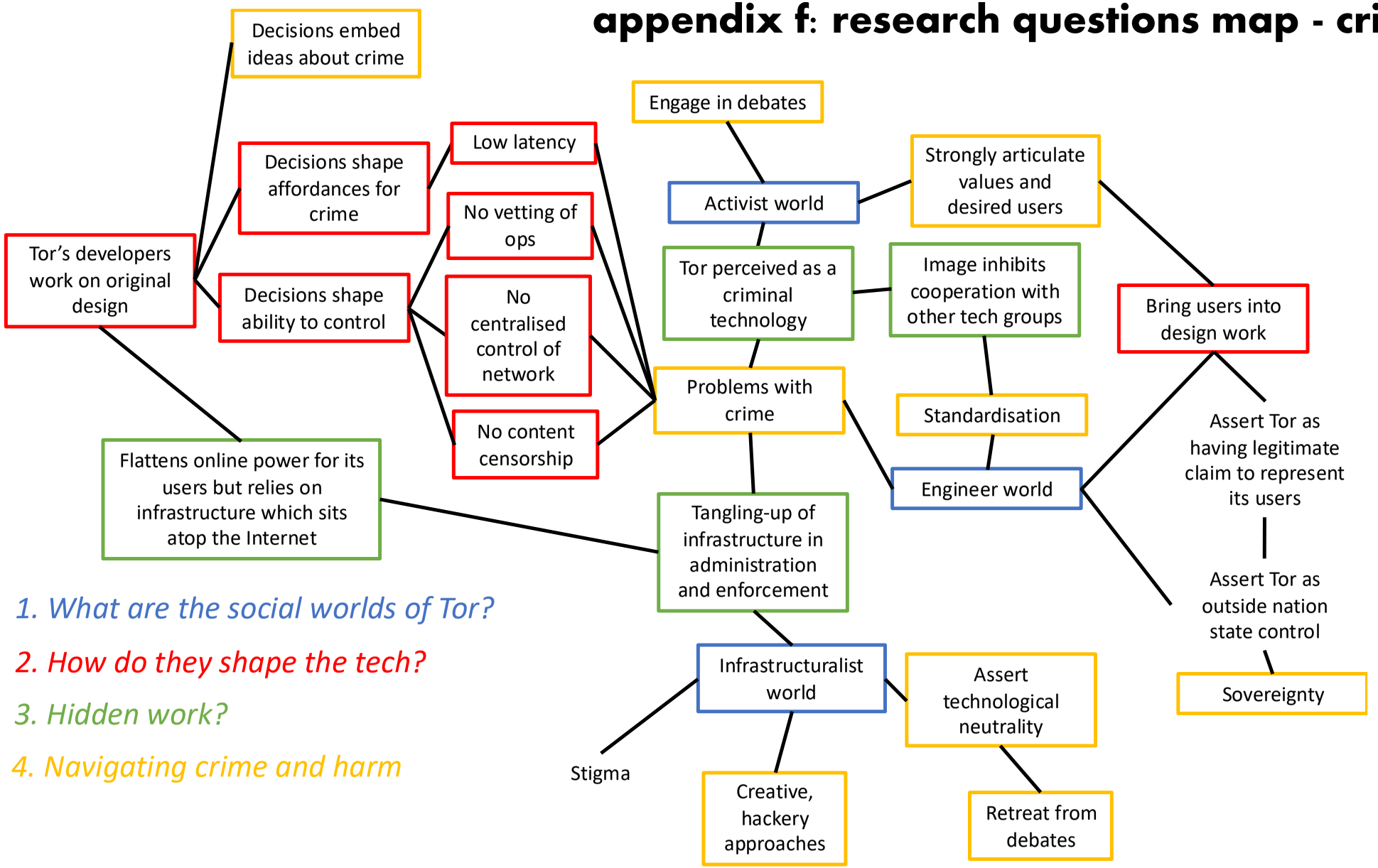
*2. How do they shape the tech?*

*3. Hidden work?*

*4. Navigating crime and harm*

# appendix f: research questions map - crime






*1. What are the social worlds of Tor?*

*2. How do they shape the tech?*

*3. Hidden work?*

*4. Navigating crime and harm*