INVESTIGATING THE DYNAMICS OF SURVEILLANCE AND RESISTANCE IN THE INFORMATION SOCIETY

WILLIAM GEORGE KERR CHIVERS

THIS THESIS IS SUBMITTED IN CANDIDATURE FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

JULY 2016

SCHOOL OF SOCIAL SCIENCES

CARDIFF UNIVERSITY

ACKNOWLEDGEMENTS

Carrying out this research has led me to accrue a significant number of debts. I am grateful for the opportunity to acknowledge these here and I hope to repay them over a period of many, many years. I am thankful first for the support and patience of my supervisors Martin Innes and Matthew Williams. Both have provided invaluable guidance and have been generous with praise and encouragement. *Sero sed serio* is the motto of the Kerr clan, my Scottish ancestors; 'late, but in earnest'. Matt, I think, may have had an inkling of what he was taking on when I opted to pursue a doctorate but I fear I may have left Martin somewhat exasperated at times with my particular brand of perpetual nonchalance.

I am also thankful for the constructive guidance and support of several members of staff at Cardiff University: Tom Horlick-Jones, Rob Smith, Tom Hall, Mike Levi, Gordon Hughes, Adam Edwards and Pete Burnap. Evenings spent in the company of the Centre for Crime, Law and Justice have been thoroughly enjoyable, even if some lay heavy on the head the following morning. I especially feel lucky to have worked my way through the PhD in the company of a wonderful group of postgraduates. We are frequently reminded as doctoral students of our shared trials and tribulations. I have concluded, therefore, that future advertisements for funded PhDs should follow the example of Ernest Shackleton's call for members of his Antarctic expedition:

> 'Men wanted for hazardous journey. Small wages, bitter cold, long months of complete darkness, constant danger. Safe return doubtful. Honour and recognition in case of success.'

Honour and recognition, my fellow PhD-ers, honour and recognition!

This research was funded by the Economic and Social Research Council (ESRC) and I am extremely grateful for their backing for both the MSc and the PhD. I owe an enormous debt of gratitude to those who took part in the research for sharing their expertise and insight with me and to Anke Domscheit-Berg and Christine Assange for their generous assistance in my attempts to make contact with Daniel and Julian. To everyone who has shaped what has been an unforgettable learning experience, I am extremely appreciative. The Surveillance Studies Summer School 2013 at Queen's University in Kingston, Canada was a turning point for me in confirming the

importance of studying surveillance and my desire to pursue an academic career based around this. My thanks go to all the delegates of #4S13 and to the staff who made it so enlightening: David Lyon, David Murakami Wood, Kirstie Ball, Valerie Steeves, Laura Huey and Dan Trottier.

I am most grateful to my family, Richard, Annie, Kate and Darrell. Advice, support or respite, they have provided these throughout. Dad, I owe my enthusiasm for writing to you; Mum, you are simply a star. I am truly lucky in my family, you guys are awesome. The perpetual student at last has a job and pays taxes! Last of all, where would I be without Liv? Studying for a PhD at the same time as each other is no mean feat but I don't think I could have done it without you. What an adventure! I owe you a holiday[1].

W. Chivers April 2015

Postscript:

Needless to say, I did not foresee spending a further twelve months revising the original thesis. It has been the single most difficult task I have ever had to complete, for many reasons. Yet, here it is. I'm thankful as ever that I've had a supportive bunch of folks around me – and a tolerant bunch too, for when I have been sulking.

W. Chivers July 2016

[1] You owe me much tea.

In loving memory of Rachel Anne Southern, Joyce Marguerite Chivers and Janet Freeman

ABSTRACT

This thesis investigates the relationships between surveillance, acts of resistance to surveillance and their respective roles in the contemporary social order. The context for this investigation is the contemporary 'information society'. This is characterised by globally networked information and communication technologies, and is represented most plainly by one medium in particular: the Internet. The Internet has historically been a contested domain; it represents, for some, the cornerstone of civil liberties yet at the same time it is highly regulated and susceptible to control. The significant social, cultural, economic and political impacts of the Internet include the proliferation of techniques of digital surveillance. However, while the Internet has facilitated the growth of these practices, it has also created new opportunities for resistance to surveillance. By attending to the social dynamics and mechanics of resistance, we can generate more nuanced and subtle understandings of the ways in which social control is being performed.

A framework of nodal governance steers this research. Consequently, this study locates these dynamics within three specific sites: online civil society, the regulatory process and the media. These cases demonstrate how a range of social actors, across a variety of settings, are implicated in the dynamics of digital surveillance and resistance. An innovative, multi-strategy approach to the fieldwork, including computational social science methods, captures these emergent dynamics as they are played out. The analysis of the data is guided by a theoretical preoccupation with control that serves to illustrate its plural and fluid character. Central to this are social and technological networks as forms of organisation and communication that facilitate surveillance and resistance. The thesis concludes that contemporary social control is an inherently *socio-technical* process, shaped primarily by dynamics of digital surveillance and resistance.

TABLE OF CONTENTS

CHAPTER FOUR
STUDYING DIGITAL SURVEILLANCE AND RESISTANCE: A MIXED-METHOD/MULTI-STRATEGY APPROACH

CHAPTER FIVE
THE ORGANISATION OF RESISTANCE: NETWORKS AND NODAL GOVERNANCE

CHAPTER SIX
REGULATION OF SURVEILLANCE AS A SITE OF RESISTANCE

CHAPTER SEVEN
NEWS AND NEW MEDIA: THE LEGACY OF THE CYPHERPUNKS

CHAPTER EIGHT
EMERGING THEMES FROM THE SITES OF SURVEILLANCE AND RESISTANCE

CHAPTER NINE
CONCLUSION

FIGURES

TABLES

CHAPTER ONE

INTRODUCTION

1.1 NO EXCUSE FOR INVISIBILITY

At an event in 2015, Alan Rusbridger remarked there is now 'no excuse for invisibility'. The former *Guardian* editor was talking about the extent to which the evolution of digital communications and media has produced a fundamental restructuring of our ability to engage and interact with people and places virtually anywhere in the world. That invisibility is 'inexcusable' was not a proclamation on any sort of right to remain hidden, more an observation that technological advances allow us – and indeed require – new means by which to understand and shape our world. We have developed the capacity to render what was previously invisible, visible, and consequently we have the capacity to harness that potential to impact positively on globally dispersed situations. Rusbridger cited the example of live crowdsourced crisis mapping in the aftermath of the earthquake in Haiti in 2010[2]. Satellite imagery was used to collaboratively construct and update vital maps of the transport infrastructure of Haiti. Monitoring social media and emergency SMS platforms permitted individual calls for assistance to be plotted that could then be used as actionable intelligence by response teams on the ground. Such an example shows it would be inexcusable to overlook our ability to make distant people and places visible in such a way that it changes the political profile of certain events.

The discussion that followed these observations later shifted to consider the current landscape of digital surveillance. At this point it struck me that the *Guardian* editor's earlier comment actually spoke to a much deeper set of issues that were roundly captured by this notion of visibility/invisibility. Here, concerns about the ability to maintain a degree of privacy were implicit. In the context of pervasive, global, digital surveillance, for many people the antithesis to Alan Rusbridger's observation rings equally true: there is no excuse for ubiquitous visibility. No excuse for

[2] http://voices.nationalgeographic.com/2012/07/02/crisis-mapping-haiti/

rendering entire populations – or at least their social lives and interactions in the virtual realm – subject to the surveillant gaze of either governments or private corporations.

The Internet is a socio-technical system highly susceptible to regulation, in a variety of forms (Lessig 1999). Such regulation means digital environments can be designed to automatically collect a huge variety of data about Internet users. At the same time, visibility has traditionally been a one-way street. The term 'surveillance' means 'to watch over'; it implies a power dynamic wherein one party effectively remains invisible. The construction of cyberspaces as sites where people can be monitored and managed is the product of a specific set of economic and security interests (Loader 1997). Events over the last 24 months have shown the truth in this, but they have also evidenced a significant shift in the politics of surveillance. For as much as control, the Internet affords the opportunity for resistance. The result is a constant dynamic of moves and counter-moves between surveillance on the one hand and resistance on the other.

In June 2013, the landscape of government intelligence and mass surveillance was changed irrevocably. Edward Snowden was an infrastructure analyst and expert in cyber-security and counter-intelligence for the United States' National Security Agency (NSA). Disillusioned both with the lack of reform of surveillance activities by US intelligence agencies and by the undermining of the transformative potential of the Internet by ubiquitous surveillance (Greenwald *et al.* 2013a), Snowden amassed thousands of confidential documents detailing the surveillance capacities and intentions of the NSA. In late 2012 and early 2013 he made contact with journalist Glenn Greenwald and filmmaker Laura Poitras, signalling his desire to leak this trove of information. In May 2013, he absconded from the NSA station in Hawaii and flew to Hong Kong. On the 6th June, while he was in Hong Kong, *The Guardian* published the first story related to Snowden's leaked information – an exposé of the collection of millions of phone call records of Verizon customers by the NSA (see Greenwald 2013a).

What followed over the course of many months was a persistent and detailed release of information concerning (primarily) the digital surveillance apparatus of the NSA as well as partner intelligence agencies in the UK, Canada, Australia, New

Zealand and Germany. Within only the first two months of publication, several important systems operated by the NSA and other agencies had been publicly identified. The PRISM program allowed for the collection of a vast array of online data including the contents of emails, VoIP[3] chats and transferred documents direct from the servers of several major US Internet firms: Google, Microsoft, Yahoo!, Apple and Facebook (see Greenwald and MacAskill 2013; Greenwald *et al.* 2013b). The XKeyscore system was a database containing all this information and more – including social media web history and communications metadata – and was searchable by NSA analysts without prior consent or authorisation by the courts. Confidential information provided by Snowden in the form of training materials for XKeyscore claimed the system was the 'widest-reaching' means of gathering Digital Network Intelligence, able to capture 'nearly everything a typical user does on the Internet' (see Greenwald 2013b). The Tempora program, meanwhile, was operated by the UK Government Communications Headquarters (GCHQ) and involved the indiscriminate harvesting of Internet data (both content and other metadata) direct from the submarine fibre-optic cables that carry the majority of Internet traffic. 'Mastering the Internet' and 'Global Telecoms Exploitation', the two components of Tempora, indicate the scale of the ambition of this program (see MacAskill *et al.* 2013).

Having been granted asylum in Moscow, Snowden continues to play an active role in contributing to on-going debates about the scale, intensity, necessity and proportionality of digital surveillance, the implication of multinational corporations in these practices and oversight and accountability (or lack thereof) of these powerful institutions of surveillance. His efforts – along with all other whistleblowers – allow us to flesh out our thinking about the concept of visibility and invisibility.

'There is no excuse for invisibility' says Alan Rusbridger. The intelligence agencies would argue otherwise and they have done; it is necessary that their activities remain invisible to be effective in combating terrorism and organised crime. Snowden's actions forced visibility onto these agencies and their partners. At the same time they show how, by exploiting the potential of digital communication, all

[3] Voice over Internet Protocol, e.g. Skype.

manner of social interactions and behaviours are made visible. Of course, there are more influences at play here to account for. We make ourselves increasingly visible by virtue of changes in social organisation and interaction (Lyon 2002); we volunteer, by varying degrees, large quantities of personal information on social media platforms and we collude in practices of consumer surveillance for the sake of convenience and reward (Andrejevic 2007). However, the key issue is *consent* to visibility. When the extent to which we are made visible is obfuscated, and when we have little say in how this is achieved, as Snowden showed, invisibility is certainly inexcusable. The on-going dynamic between surveillance and resistance is further seen in the pushback from the intelligence agencies attempting to justify their actions and in governmental attempts to legislate for greater surveillance powers. They argue there is no excuse for invisibility of citizens *if they have done nothing wrong*; the classic argument that if you have nothing to hide, you have nothing to fear (see Solove 2007a). It is ironic that in the aftermath of Snowden's revelations this flawed argument should backfire so spectacularly on the intelligence community.

This thesis investigates the relationship between surveillance, acts of resistance to surveillance and their respective roles in the contemporary social order. Framed by theories of nodal governance, the empirical data in this research are analysed to illuminate how and why innovations in surveillance capacity and capability, induce new modes of resistance. By attending to the social dynamics and mechanics of resistance, we can generate more nuanced and subtle understandings of the ways in which social control is being performed and understood.

1.2 SO WHAT'S THE (SOCIAL) PROBLEM?

The Snowden revelations ignited a clamorous debate about mass (digital) surveillance and various attendant issues including privacy, necessity, proportionality and regulation of both the intelligence agencies and Internet communication in general[4]. Surveillance, perhaps now more than ever, is framed as a social problem that demands a response. The increasing digitalisation of surveillance raises questions about the potential for *control* inherent in such systems

[4] The latter of which is a prominent theme in this thesis; see Chapters Two and Three.

as a result of the availability of increasingly granular details about our personal lives. Here it is not only surveillance conducted by institutions of the state that is problematic; increasingly it is the surveillance powers of private entities that are framed as a social problem. Snowden has helped to catalyse public sentiment around these related issues. However, such public conversation is not new. The revelations, while significant, are but the latest in a long trajectory of claims-making about the necessity and dangers of surveillance. Any sentiments concerning the dangers of surveillance are strongly counter-balanced by the fact that surveillance is inseparable from the 'problem' of crime and terrorism, the response to which is, inevitably, more surveillance. The terror attacks in Paris in 2015 and the on-going concern with paedophile rings in the UK, send powerful messages to the public that monitoring of online activity is vital to ensuring the safety and security of children, communities, and the country. Ever more sophisticated and wide-reaching control is therefore promoted by the state as vital for the security of citizens. However, we also see that surveillance and social control are constantly negotiated and resisted; efforts that subsequently generate new or adapted forms of control (Marx 2009; Innes and Levi 2012).

Public space surveillance exploded as a mechanism of crime prevention in the early 1990s. A catalyst of this was the murder of James Bulger in 1993. The identification of his killers from CCTV footage helped to support the Conservative government's crime prevention agenda (see Home Office 1994[5]). Estimates suggest that from 1990 to 2002 the number of CCTV cameras in England and Wales designed for crime prevention purposes increased from 100 to approximately 40,000, while over the three-year period 1996-1998 three quarters of the Home Office crime prevention budget was spent on CCTV (Armitage 2002). CCTV use – both public and private – continued to escalate and current approximations of the number of cameras in England and Wales range anywhere from two to four million. Nevertheless, CCTV is expensive and its effectiveness in preventing crime has frequently been called into question (e.g. Gill and Spriggs 2005). Some recent indications are that CCTV is falling out of favour with law enforcement (Instrom 2014[6]), however, technological

[5] 'CCTV: Looking Out For You'.

[6] A recent study commissioned by the Police and Crime Commissioner for Dyfed-Powys Police recommended, amongst other things, the removal of redundant cameras, a shift away from actively

developments in the form of unmanned aerial vehicles (UAVs/'drones') suggest that CCTV may in fact simply be evolving into a more mobile, tactical resource.

Technological advances have gone hand-in-hand with the evolution of surveillance. This thesis is predicated on that fact. CCTV, for instance, is now high definition and capable of facial recognition. However, while there has been a global expansion of technologically enabled surveillance, the scale and pace of change between countries has been different. Britain is often given the dubious honour of being called the world's leading 'surveillance society', which again is tied to the 'hallmark' of modern surveillance, CCTV[7]. Other countries, with a legacy of state intrusion into citizens' private lives, are much less passive when it comes to mass surveillance. Resistance, then, is an important topic to study as it sheds light on these comparative differences. Related to the question of technology is what it 'adds' to surveillance practices that predate such transformations (Dandeker 1994). The answer is that technological developments such as the Internet have allowed for the manipulation of the very environment in which control is exercised. Technological changes do not just make surveillance more accurate or more granular; they make surveillance the default position. The digital world is designed to surveill.

The trend of equating crime prevention with expansive surveillance has continued in the 21st century, albeit shifting towards digitalisation as a response to changes in social organisation and interaction online. In the wake of the terror attacks in 2001 in New York and in 2005 in London, the 'necessity' of extensive surveillance was given new life. Surveillance at border gateways was particularly intensified, air travel became an enormously regulated affair, biometric technologies such as the UK ePassport in 2006 were introduced and communications data – i.e. logs of email and telephone calls – were prioritised as an invaluable resource for the 'war on terror'. These trends continue today; in the wake of the 'Charlie Hebdo' incident, David Cameron outlined his desire to overcome barriers to accessing encrypted communications within the UK (see Watt *et al.* 2015). What people do online is increasingly captured within the discourse of crime prevention. A key facet of this

monitored CCTV in favour of passive (unmonitored, recorded) systems and the constant evaluation of existing CCTV to ascertain its continued economic value.

[7] BBC News (2009) noted that the London borough of Wandsworth had more CCTV cameras than Dublin, Johannesburg, Boston and Sydney combined.

discourse, an area that this thesis explores, is that governments 'cannot do it alone'; in recognition of their access to massive quantities of data, private sector companies are situated (through regulatory processes) as valuable auspices of security.

However, rapid expansion of the national and international surveillance apparatus has been met with resistance. The UK has an active community of civil liberties organisations that itself is part of a global network concerned with issues related to free speech, censorship and privacy. These groups have played a pivotal role in shaping the public conversation about the control implications of new surveillance practices. The No2ID campaign group, for instance, was instrumental in the repeal of the Identity Cards Act 2006. Later, in response to government plans in 2012 to extend the surveillance powers of law enforcement, a large number of individuals and groups alike voiced their discontent and were again successful in forcing the plans to be abandoned[8]. Independent oversight bodies and academic researchers have also been influential claims makers in respect of surveillance. In 2004, the UK Information Commissioner Richard Thomas warned that Britain was in danger of 'sleepwalking into a surveillance society' (see Booth 2004). These comments led to an ICO-sponsored report by the Surveillance Studies Network (see Wood *et al.* 2006) that was updated four years later (see Wood *et al.* 2010). These reports described current surveillance practices and, in 2006, projected developments until 2016. Many of these are already in evidence to an extent; the introduction and expansion of UAVs, body-worn cameras on police officers, RFID[9] sensors embedded in mundane household items, personalised advertising in public spaces and extensive biometric border security. Official concerns with the gradual expansion and pervasiveness of surveillance in the UK are still evident, with the Surveillance Commissioner Tony Porter recently reiterating Thomas' concern, albeit in the context of re-igniting the debate about CCTV (see Riley-Smith 2015).

It is not only state-sponsored surveillance that is resisted by the public and civil society; monitoring techniques have also proliferated in the private sector. Supermarket loyalty cards are a prime example of this. Our shopping habits are recorded and analysed and we are persuaded to remain loyal customers as a result

[8] See Chapter Six.
[9] Radio Frequency Identification.

of the individually tailored rewards we are offered. Recently, Samsung 'smart TVs' have been shown to be capable of recording conversations in their vicinity (i.e. in the home) and sending the data to third party marketing companies (see Harris 2015). Online, such practices are amplified. The dominance of multinational communications corporations and service providers such as Google, Facebook, Apple and Microsoft has produced myriad mechanisms by which Internet users are monitored, tracked, influenced, persuaded and regulated. Browsing histories, purchasing habits, personal details and preferences and geographical location are only some of the data valuable to commercial enterprises. The data stream generated by our online activities is big business – so much so that it has generated its own buzzword in recent years: 'big data'. Again, the very architecture of the Internet is shaped so as to facilitate processes of identification and surveillance (Lessig 1999[10]).

Once again, however, these patterns have elicited negative public reaction. In the US, for instance, CASPIAN[11] campaigns against loyalty card monitoring of consumers. But it is online forms of monitoring – and regulation of Internet life in general – that the public conversation has begun to problematise. For activists who advocate its founding principles, the Internet is the cornerstone of free speech and democracy in contemporary society. Consequently, attempts to subject the Internet to surveillance are often met with resistance[12]. These concerns have been amplified as a result of the confluence of political and economic interests in monitoring online behaviour (Fuchs 2008). Snowden's revelations highlighted how political and economic forms of surveillance are entwined making it increasingly difficult, yet also vital, for the public to make their voice heard.

The overarching impression is that the Internet is a site of struggle, where governments, corporations and individuals or groups of citizens, amongst others, grapple for the right to determine the shape of the playing field. The Internet is an enormously empowering technology but also a site of 'ambiguous danger' (Molotch

[10] Also, Chapter Two.
[11] Consumers Against Supermarket Privacy Invasion and Numbering
[12] Prominent examples in recent years include the Stop Online Piracy Act, Protection of Intellectual Property Act and Anti-Counterfeiting Trade Agreement in the United States – all of which were instances of legislation perceived as a threat to civil liberties and digital rights – and the on-going battle to preserve 'net neutrality' (Save the Internet 2015).

2012). It allows for democratisation of communication, innovation and political engagement. At the same time it is increasingly subjected to the will of political and economic interests that are eager to capitalise on the wealth of information available and the potential it offers for identifying, monitoring and managing populations. Digital surveillance and resistance are networked, diffuse and diverse practices involving a plurality of actors with overlapping mentalities. This thesis is immersed in this contested domain. The set of questions guiding it develop out of this complex dynamic of relationships and motivations.

1.3 RESEARCH CONTEXT, AIM AND QUESTIONS

Broadly speaking, this thesis examines contemporary social control. It achieves this by focusing on the relationship between digital surveillance and resistance, both constituent parts of social control, in an age of proliferating information networks. Social control is not something that simply 'happens'. It is the product of constant actions and reactions between groups in society. Surveillance and resistance are one important way in which we can see this dynamic occurring.

The preceding discussion highlights the relevance and continuous evolution of the relationship between surveillance and resistance. It also captures the contemporary context in which studies of surveillance are situated. Specifically, it signals a prominent undercurrent that has featured in many studies of surveillance, namely, the role of the state in the conduct of surveillance. Surveillance scholars have traditionally embraced Foucault's (1977) elaboration of 'panoptic' surveillance, a metaphor for the dispersal into wider society of a disciplinary mode of power. The concept has shaped much of the literature on surveillance, and continues to do so owing to the conceptualisation of power and governmentality that underpins it.

Despite its appeal, many in the field of surveillance studies question the utility of the panopticon as a model of contemporary surveillance (e.g. Haggerty 2006; Lyon 2003a, 2006; Dupont 2008). It makes several assumptions that are increasingly untenable in the contemporary information society. It describes a centralised or top-down process of surveillance where 'the few watch the many' and consequently has its roots in a state-centric view of control. While discipline is dispersed into society's institutions, this process is part of a wider system of governance guided by

the state. There is also little attention given to the role of individual agency and resistance in Foucault's original exposition. Above all, technological developments that have produced changes in social organisation force us to reconsider the relevance of the panopticon. The democratisation of surveillance – the increasing availability of surveillance tools and technology – challenges panoptic notions. Closely linked to this is resistance, 'where efforts are deployed by the subjects of surveillance to understand, reveal, mock, evade, and neutralize surveillance technologies through the collaborative power of socio-technical networks' (Dupont 2008: 258). The characteristics of the information society[13] also make it difficult to subscribe to the idea of centralised, top-down control. Instead, networks and dispersed control mechanisms are more suitable organising concepts.

Previous research has examined the relationship between surveillance and resistance at the micro level, where surveillance is creatively and deliberately evaded and challenged (Marx 2003; Dupont 2008). This thesis, however, is concerned with social processes on a broader scale, examining the interplay between digital surveillance and resistance across a number of social settings – within civil society, in the context of regulation and in the media. To capture a sense of these dynamics a nodal governance framework is employed in the research. Nodal governance is a theoretical construct for understanding the way in which 'a variety of actors operating within a social system interact along networks to govern the systems they inhabit' (Burris *et al.* 2005: 33). This perspective has gained currency in the study of security and crime control for highlighting the multitude of actors – increasingly those beyond the state – who are involved in delivering these social goods. Surveillance, as this opening gambit has illustrated, is a key mechanism in this apparatus of control. Nodal governance also draws attention to the processes of cooperation and competition (Fuchs 2008; Wood and Shearing 2007) that characterise the relationships between these actors. It is helpful, therefore, for identifying the entities wherein surveillance and resistance take place. It is a framework that will aid in capturing the dynamics of action, reaction and counter-reaction at play.

[13] See Chapter Two.

With this framework in place, the research is guided by the following overarching research questions:

1. How are digital surveillance and resistance related?
2. Why do individuals and groups who resist surveillance identify a need for doing so?
3. What are the implications of these patterns for our understanding of control in the information society?

These questions structure the analysis in the thesis, drawing out key elements of the relationship between digital surveillance and resistance and the implications of these for social control in the information society. The thesis explores these questions empirically and theoretically. Empirically, it examines three sites where the dynamics between digital surveillance and resistance are played out and can be observed: online civil society; regulation of surveillance, and; WikiLeaks and the news media. The nodal governance framework provides the rationale for selecting a variety of social domains and actors (nodes) that contribute in different ways to the landscape of digital surveillance and resistance. Each of these sites shows different ways in which surveillance and resistance intersect and are enacted by different nodes (research question one). They show, through empirical examples, why and how digital surveillance is resisted (research question two). Each case also contributes to a rolling narrative of the characteristics of social control in a digitally mediated world (research question three).

Theoretically, the thesis offers insight into how established theories of control can be developed and applied to contemporary information society. To do this, the cases that constitute the research are each analysed using theoretical frameworks relating to social control. A theory of nodal governance, as well as informing the structure of the research, is used to examine the online organisation of resistance in Chapter Five. In Chapter Six, regulation as a modality of control is analysed in the context of legislation that aimed to reform surveillance practice in the UK. Finally, in Chapter Seven, literature on moral panics and the construction of social problems is used to analyse the impact of WikiLeaks and Edward Snowden on the landscape of digital surveillance. These frameworks are combined in this thesis to capture the multi-layered phenomena of digital surveillance and resistance. At each step of the

analysis, the reader's focus is drawn in more detail to the intricacies of this relationship.

1.4 STRUCTURE OF THE THESIS

Chapter Two sets out the context in which this research is situated in the form of a brief social history of Internet communication. The chapter explores the relationship between the information society and surveillance. It argues that technological, economic and cultural developments have had a major impact on social order, the nature of surveillance and the character of resistance. It begins by drawing out key characteristics of the conceptualisation of contemporary society as 'informational' and 'networked'. Following this, the chapter describes the emergence of the Internet as a socio-technical medium of communication and outlines the technical systems that allow it to function. Understanding these systems makes it clear how they relate to expanding capacities for *both* surveillance and resistance. Attention is paid to the political and economic drivers of regulation of surveillance and Internet communication more broadly, and the chapter thereby begins to chart the nodal character of governance in the network society.

Continuing these themes, Chapter Three engages with theoretical contributions to the study of social control and surveillance. The chapter describes the evolution of theories of control, and assesses in greater detail the division between a Foucauldian, panoptic approach to surveillance (and resistance) and the networked, nodal conception on which this research is predicated. This leads into an explanation of the literature on surveillance, outlining the characteristics of 'digital', 'political', 'economic' and 'resistive' surveillance. The connections between theories of control and surveillance and their impact on the direction of the research are made clear.

Chapter Four presents the methodology. It describes the fieldwork and analysis, outlining the three research sites that act as gateways into developing an appreciation of the intricacies of social control in a digital, networked society. Whilst not an explicitly stated aim of the thesis, the chapter also raises questions about how to effectively research surveillance and resistance online. To that end, Internet-based research methods are advocated, including emerging and innovative

strategies of computational social science. Alongside these, the chapter justifies the use of more 'traditional' methods of inquiry and recounts some of the obstacles that arose in trying to access and recruit some high profile respondents. The chapter also reflects on the conduct of research into surveillance, including the subjectivity of the researcher in this field and being bound up in the processes and practices that the research outlines.

Chapters Five, Six and Seven deal in turn with each of the research sites. The first empirical contribution to the thesis, Chapter Five, is an examination of the *networked nature of the social organisation of resistance*. It suggests that to understand the dynamics of digital surveillance and resistance, we need to look at how the Internet allows for organisation and politicised communication (i.e. 'information politics') to take place. The chapter develops the nodal governance framework on the grounds that resistance is multi-polar; just as governance is nodal, so too are the counter-responses to surveillance and control. The chapter achieves this by examining the online structure and communication patterns of civil society groups – specifically those oriented around issues of privacy, surveillance and digital rights. Civil society is a governing node, however, within civil society are individual nodes jostling for position and acting out their own connections and interactions. Network analysis and other data show how these groups align with each other and interact with other nodes beyond civil society. These relationships are visualised, providing a level of empirical insight frequently missing from theoretical elaborations of nodal governance.

Chapter Six examines the legal frameworks that *regulate surveillance* and *generate effects of resistance*. It illustrates why digital surveillance is seen as problematic and thus relates to the second research question 'why do individuals and groups who resist surveillance identify a need for doing so?' as well as generating more insight into the relationship between surveillance and resistance (research question one). Drawing on documentary analysis of the consultation process that was part of the Draft Communications Data Bill (CDB) in 2012, this chapter widens the scope from civil society to a whole host of other stakeholders (i.e. nodes) who were engaged in debates about digital surveillance. At the same time, it narrows the concern with surveillance and resistance to a specific instance where the regulation of

surveillance was being reshaped. The findings here relay some of the main points of contention in the Bill. While these concerns are important in their own right, the CDB also signalled a broader opportunity for codification of resistance in law. In addition, the relationship between the government and private commercial organisations in shaping social control is subjected to analysis. Broadly, the chapter contributes to the continuing narrative by illustrating the role of regulation as a modality of control but also how and why it generates resistance.

The final substantive empirical component of the thesis, Chapter Seven, turns to examine the *symbolic and communicative aspects of surveillance and resistance.* The chapter is informed by a study of the news media and 'new media' platform WikiLeaks. This case is the most granular presented, bringing to light the actions of one specific node concerned with online resistance or 'resistive surveillance'. The example of WikiLeaks is used to demonstrate how resistance to surveillance capitalises on the opportunities of a new technological medium. At the same time, the saga of this organisation (seen through the lens of media reports) is one that displays clearly the counter-attempts by government to maintain social order by framing WikiLeaks as deviant and problematic. Consequently, as a basis for the chapter, the concept of moral panic is used to explore the construction of both surveillance and resistance as problematic. By following this recent history to its current point, appropriately, this chapter returns us to where the thesis begins – with Edward Snowden and the contemporary state of surveillance.

Chapters Eight and Nine conclude the thesis. The preceding chapters show conflicting tendencies towards centralisation and decentralisation in both digital surveillance and resistance, patterns of competition and cooperation and implications for the idea of visibility, where this chapter began. Chapter Eight explores these themes. Chapter Nine draws together the key findings from the three research sites and summarises what has been learned about the dynamic between digital surveillance and resistance, the reasons for resistance and the lessons for thinking about contemporary social control. It offers reflection on the limitations and future directions of the research before concluding with the broader theoretical, methodological and policy contributions of this thesis.

--. --- ...- . .-. -. -- . -. - ... ---- ..-. - .... -. -.. ..- ... - .-. .. .- .-.. .-- --- .-. .-.. -.. --..--

CHAPTER TWO

A (BRIEF) SOCIAL HISTORY OF THE INTERNET: THE INFORMATION SOCIETY AND SURVEILLANCE

2.1 INTRODUCTION

This chapter is the first of two that set the context for the research. Where settings for social research are often physically bounded, this study is situated in the digital environment of the Internet. The Internet is the cornerstone of the 'information society' – a concept explored in this chapter – and in laying out the digital context of the thesis, it is important that we understand the social and technological foundations of this system. The contribution of this chapter, therefore, is to expand upon some of the key messages outlined in the introduction and to achieve one primary aim: to illuminate the connection between the 'information society' and contemporary forms of digital surveillance and resistance.

The discussion that follows is set out in the following terms. First is a theory of the information society, drawing on commentaries that have outlined its chief characteristics. These incorporate the various and related social, technological, cultural and economic features of contemporary society, as they are constituted within and by digital networks. It is suggested that these features, particularly 'informationalism' (Castells 1996), are tied to contemporary forms of surveillance. Continuing with this fundamental point, the chapter also explores the concept of regulation as it applies to the Internet. The Internet is a highly regulated socio-technical system and the discussion here highlights how surveillance is both designed into and a natural product of interactions in cyberspace. However, what also becomes apparent is how such regulation permits new and effective forms of resistance to surveillance to emerge. This chapter consequently lays the foundations for a more detailed theoretical exposition of social control, surveillance and resistance in Chapter Three.

The history that this chapter presents is complex. However, it is necessary to understand the many influences upon the shape and character of the Internet and the information society. These are grouped into two broad themes – technological and social forms of ordering. Any such separation is somewhat artificial; however, as the thesis goes on to show, surveillance and resistance can be characterised as both technological and social processes.

2.2 THE INFORMATION SOCIETY

There is a widespread consensus that we are living in an 'information society' (Beniger 1986; Castells 1996; Williams 2006; Webster 2014). The continued scale and pace of information technology development has had profound implications across the whole of society. Central to these is the proliferation of networks; of economic, political and technological systems, of individuals and of diverse and dispersed communities and populations. The effect of these has been to produce what Manuel Castells (1996) calls the 'Network Society'. The social and technological changes both producing and produced by the rise of information networks amplify those social shifts typically associated with the transition from modernity to late/reflexive/liquid modernity (see Giddens 1990; Beck 1992; Beck *et al.* 1994, Bauman 2000). So too has the rise of information as a global commodity altered the social organisation of relationships between institutions and their interests. This introductory discussion draws out several features of the information/network society[14] that have particular relevance to this thesis.

It is insufficient to assert the existence of an information society or define its characteristics based solely on the prevalence of advanced computing and communication technologies (although these are of central importance). Rather, there are several dimensions to understanding what is meant by an information society. Webster (1995) outlines five ways in which we can understand the information society: economic, technological, spatial, cultural and occupational.

[14] While Castells uses the term 'network society' I have opted to refer to the contemporary situation as the 'information society'. I do not imply any difference with this alternative nomenclature; the decision is based on a more ready association with practices of surveillance.

The characteristics of the 'new economy' constitute a significant portion of Castells' (1996, 1997, 1998) analysis of the information age. For Castells, with his Marxist roots, this 'economic base' of society is a key determinant of social order. The new economy, emerging in the latter part of the twentieth century, he argues, is informational, global and networked. The basis of this economy, its raw material, is information, transmitted across pervasive and flexible electronic networks. Information is the source of productivity and power in this new global economy; the networked economy is characterised by increased efficiency in production and management made possible by global networked communications. 'Informationalism', the outcome of the interaction between a new information-technology paradigm and the economy, is described by Castells as the 'action of knowledge upon knowledge itself as the main source of productivity' (1996: 17).

The informational, global and networked economy (and indeed the information society as a whole) has at its heart the Internet. The changes Castells (1996) describes did not begin with the emergence of the Internet – the shift to an information-driven economy was identified in earlier work by the likes of Machlup (1962) and Porat (1977) – but they have been accelerated and compounded, as this chapter goes on to describe. Online commerce now constitutes a significant part of national economies. In 2014, Internet sales accounted for 11.2% of all retail spending and the average weekly spend for that year was £718.7 million (ONS 2015). One example of how the Internet has caused global shifts in the nature of commerce (related to digital surveillance) is online advertising. Revenue is generated on most websites through banner and click-through advertising. Our web browsers store information on websites we visit ('cookies') and this information is used to deliver targeted adverts based on our preferences and predicted spending habits[15].

As well as representing the pervasive technology by which flexible, global communication and trade is made possible, the Internet also emerges as an active domain in itself. The Internet is thus both a tool and manifestation of the information society. Already this signals why the Internet is such a vital and contested resource and space. The interests of the capitalist system are played out

[15] As of May 2011, all EU websites are required to display a notice of informed consent for the collection of cookies. In the UK this is enacted under the Privacy and Electronic Communications Regulations.

on and via the Internet, sometimes with those of nation states and sometimes against them. According to Fuchs (2013) 'what has emerged in the online sphere is corporate and state control.' The impact of these two forces in online regulation and policy is discussed later. Likewise, as discussed in Chapter Three, Marxist-influenced theoretical perspectives emphasise the economic imperatives and relationships that shape online social control. The Internet is subject to regulation, then, largely as a product of economic interests. The Internet can be regulated in various ways but one of the driving forces is to make identifying users commonplace (Lessig 1999) – again for the purposes of monetising Internet activity. As will become clear, attempts to regulate the Internet in these ways have significant impacts for the daily experiences of Web users; indeed this has contributed to the issues at the centre of this research.

There is a clear overlap and mutual influence therefore between economic and technological characteristics of the information age. The technological definition is the one primarily espoused by proponents of the information age and understandably so; without technological advances the networking and informationalisation of the economy, occupations and cultures would not have occurred. While the Internet is at the core of the technological definition, we should acknowledge the convergence of technologies that has led to the Internet becoming a ubiquitous feature of everyday life for large sections of the population. These are described in more detail below (section 2.3) but what are referred to here are increases in sophistication and processing capacity, coupled with decreasing size and cost, of computers, laptops, mobile telephones (smartphones) and tablets.

Whilst acknowledging the central importance of technology to the changes described so far, this thesis seeks to avoid technological determinism by illustrating the *inter-relationship* between social and technical factors in the context of surveillance, resistance and control. To this end, the technological underpinnings of the information society are particularly relevant to this thesis where they overlap with its spatial and cultural characteristics (Webster 1995). While there is much to be taken from Castells' (1996, 1997, 1998) expansive analysis of the information age, considerations of the spatial and cultural changes being brought by technological development are evident in much earlier work. Preceding, but in parallel with

Castells' global and networked effects of the information society, Marshall McLuhan (1964) popularised the term 'global village' to describe the effects of new communication media; previously distanced or isolated places became increasingly connected, decreasing the time it took for information to travel between people. Earlier still, in 1926, Nikola Tesla foresaw the emergence of worldwide (and indeed mobile) wireless connectivity:

> 'We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do his will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket' (Kennedy 1926).

McLuhan and Tesla's prescient insights suggest a 'shrinking' of the globe. This coincides with notions of a 'borderless' world, where nation state boundaries are transcended by virtual networks. This is an enduring issue for this thesis as it raises questions about the ability of governments to exert control in a virtual realm (i.e. the Internet) that exists largely independently of physical and geographical limitations[16].

In respect of culture, the information society exposes us to a vast array of cultural symbols and messages. The proliferation and convergence of media channels on the Internet naturally alters how we perceive and engage with the wider world. The advent of social media has intensified this process, bringing people together in social relationships – some now fleeting, others more permanent – and allowing for the sharing and construction of cultural norms. Related to this is the concept of online community. Of relevance for this thesis is the extent to which Internet users around the world possess shared ideals about the nature and opportunities of cyberspace. Perhaps the most prosaic formulation of these important ideas is John Perry Barlow's *Declaration of the Independence of Cyberspace*[17], the following extract from which illustrates the connection between spatial and cultural characteristics of the information age.

> 'You [governments] do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it

[16] Although, as we see later (Chapter Six), national jurisdictions do play a role in shaping the ability of government to surveill online communication.
[17] See Appendix I.

> were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions…You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions' (Barlow 1996).

The growth and colonisation of the Internet thereby ushered in vociferous debates concerning the value of information, access to it and the cultural importance of free speech that the Internet was, and still is, seen to represent. For the likes of Barlow (1996), cyberspace was distinct from 'real space' and the community that inhabited it responsible for forging a social domain free from restrictive government intervention and control. Activists and campaigners advocate for the Internet as capable of establishing and protecting a liberating social order. However, as this chapter later demonstrates, the Internet is highly susceptible to technological forms of regulation and control (see Lessig 1999; Galloway 2004). Related to this, some authors have observed that 'experiences online are not considered as 'virtual' or apart from 'real' life, and that this presumed dichotomy is a false one' (e.g. Markham 1998, Miller and Slater 2000 [cited in Williams 2006: 16]). This contention is followed throughout the thesis. Despite some unique characteristics of cyberspace, digital surveillance controls are intrinsically bound to their offline manifestations.

It is also important to note that the trends identified above are far from universal. A substantial 'digital divide' exists between those who can access networked communication technologies – and benefit from them – and those who cannot. This divide is played out globally between different countries and continents and also locally; most Internet users are young, middle-class males (Compaine 2001). The idea of an inclusive, global, online community is skewed. However, by paying attention to the 'flawed dichotomy' between online and offline social life we gain a sense that the struggles for regulation and control online have as much of an effect on the 'real world' as the virtual and, by extension, on both those who are empowered and disempowered by networked communication technology.

2.3 THE ARCHITECTURE OF THE INTERNET

The technological foundations of the Internet are important not only for an historical appreciation of this mode of communication but also in the context of

studying new modes of social control. The intention here is to outline a short socio-technical history of the Internet (not purely technical; as already noted, social and technical factors are inseparable in this context). The intentions that led to the creation of the Internet and the architecture that governs its operation are intrinsically linked with accompanying developments in digital surveillance.

2.3.1 DISTRIBUTED AND SECURE

The Internet, in its earliest incarnation, emerged nearly simultaneously on both sides of the Atlantic during the Cold War era. In the United States, a perceived scientific knowledge gap between the USA and USSR and fears over the threat of nuclear war with the Soviet Union lead Paul Baran of the Rand Corporation to conceive of a 'survivable' computer network. In 1964, acknowledging that an attack on a centralised communications hub could cripple the United States, Baran proposed a decentralised computer network that would be capable of withstanding nuclear attack. Under such a system, communications could be hindered but would still be able to route around the network effectively.

At roughly the same time, but unaware of Baran's work, Welsh computer scientist Donald Watts Davies invented a system of sending data via a distributed network (such as telephone lines) by breaking it up into smaller pieces and reassembling it as it arrived with the recipient. Coining the terms 'packet' and 'packet-switching' to describe this system, Davies was motivated by an academic interest in collaborative and simultaneous working on remote computers. Packet-switching remains the system by which the inter-networking of computers operates today[18].

The coincidence of the work of these two pioneers occurred when Davies' packet-switching technology was put into place by the U.S. Department of Defense in the form of ARPANet (Advanced Research Projects Agency Network) in 1969. This small group of networked computers allowed academics based at different universities across the United States to share resources. This first incarnation of the Internet as

[18] The alternative system, 'circuit-switching', operated via a physical connection made by wire between one caller and one recipient such as in traditional telephone exchanges. The disadvantage compared to packet-switching is that only one connection can use the wire at once; in other words, packet-switching allows multiple users to send data at once – a vital requirement for high speed Internet communication.

a secure, distributed communications network was born of both academic and military interests. It is important to note that both of these influences remain today – albeit combined with powerful economic motives.

In 1989 Tim Berners-Lee contributed perhaps the single most important development since Baran and Davies 20 years previously. Berners-Lee, working at the European Organisation for Nuclear Research (CERN), was motivated in a similar fashion to Davies; he conceived of a means by which scientists around the world could share resources and findings without having to be in the same location and be able to create links between these documents. His invention, the World Wide Web, is what most of us would recognise, and refer to, as the Internet today. It is important, however, to understand the distinction between these two. The World Wide Web is only one functional layer of the Internet; specifically, a computer protocol dictating a particular form of content known as Hypertext Mark-up Language (HTML)[19]. Webpages are written in this language and allow for the standardised presentation of text and image files over the Internet. The documents that constitute webpages can also be hyperlinked to one another, which is the basis of the Web. The Web, as a distinct form of media, was more user-friendly and accessible than the forums and Usenet discussion groups that had previously dominated communication and interaction via the ARPANet/Internet. Consequently, the birth of the Web signified the start of mass-uptake in public use of the Internet that both drove, and was driven by, commercial interests.

2.3.2 PROTOCOL AND CONTROL

These technical developments are in actuality the design and implementation of standards of computer protocols. Protocols are guides for behaviour. As the term gained currency in the computer sciences, it came to mean a set of agreed upon standards for computer communication. In respect of networked communications, for computers to be able transmit data, rules have to exist about the format of the content, how it will be parsed and sent, what to do if data get lost in transit, how the data will be sent between different networks and how the data travel over physical

[19] For example, a second constituent part of modern Internet communications is email, which operates using a different protocol known as Simple Mail Transfer Protocol (SMTP).

infrastructure (copper and fibre-optic cables for example). The Web and its languages are all protocols of differing hierarchical stature[20]. The reason it is helpful to understand this is because the architecture of the Internet (both its codes and cables) is a highly constraining form of regulation. Regulation is about affecting *process* (Innes 2014) – how something must be done – and thus the functionality of the entire Internet depends on it being regulated. The suite of protocols known as TCP/IP are responsible for governing access to the Internet and the Web[21]. These technological artefacts, that 'radically distribute control into autonomous locales' (Galloway 2004: 142) underpin the libertarian ethos of Internet activism. The Domain Name System (DNS), on the other hand, allows for hierarchical control of access to webpages. It is through this mechanism that websites can be removed from the Internet. Internet communication is therefore characterised by duality between highly liberating and restrictive forms of regulation (Lessig 1999). This is not only a metaphor for how the Internet allows both surveillance and resistance; this is the technological basis of everything that can occur online.

Galloway's (2004) exploration of protocol develops this principle that control and attempts to subvert it are the product of the same system. Protocol is a form of distributed management, within which *everything is possible within a predefined set of standards*. In the context of this research it means that digital surveillance and resistance are part of one socio-technical system that allows both to occur. Protocol is the way in which what seems like a chaotic, uncontrollable directionless system (the Internet) is managed and subjected to order and logic. Protocols should not be equated with 'rules', per se, more with the 'best course of action'. For the majority of Web users, there is little option but to follow this guidance; it is the least difficult route to engagement with the Web and with others there present. However, the commercialism that drives Internet activity would be better served with *proprietary* standards for communication. Access to the Web would be predicated on rules and ownership of the means of communicating with the network. As Lessig (1999: 7) says 'if the code of cyberspace is owned…it can be controlled; if it is not owned, control is much more difficult.' This speaks to a bigger debate for the thesis

[20] See Hall (2000) and Kozierok (2005)
[21] See Appendix A for a more detailed discussion of the architecture of the Internet.

concerning who has the power to shape regulation (and consequently surveillance[22]) of the Internet.

Galloway's (2004) analysis supports Deleuze's (1992) assertion that contemporary society has transitioned beyond Foucault's disciplinary model to a control model[23]. Where the former can be characterised in *decentralised* terms – the dispersal of discipline into multiple locales in society – the latter can be understood by the *distributed* network form. As Deleuze (1992: 6) argues:

> 'types of machines are easily matched with each type of society – not that machines are determining, but because they express those social forms capable of generating them and using them…the recent disciplinary societies equipped themselves with machines involving energy, with the passive danger of entropy and the active danger of sabotage; the societies of control operate with machines of a third type, computers, whose passive danger is jamming and whose active one is piracy and the introduction of viruses.'

That contemporary society is reliant upon the power of computing, communication technology and information processing is a foregone conclusion. However, we should properly acknowledge Deleuze's foresight, writing prior to the popular uptake of the Web. The parallels with Castells (1996) are also evident; ours is a society that has developed and adapted to the capabilities of computer technologies. 'Active' dangers include hacking[24] – a politicised form of resistance and a particularly creative appropriation of the potential of Internet technology[25]. The passive danger of 'jamming' (i.e. that systems can fail) can be understood in terms of efficiency. For a society dependent upon pervasive computing and an informational economy, efficiency and reliability are vital and it is here where protocols come into their own.

Protocol alerts us to the forms of control embedded in technologies that are used for – and are proscriptive of – social organisation. This research is not a study of protocol but the message to take from this is important. Rules and forms of control are embedded within operating systems, much as the physical laws of the world shape our daily lives. However, in both cases these laws shape how we communicate, how we organise, how surveillance occurs and how it can be resisted.

---

[22] See Chapter Three.
[23] See Chapter Three.
[24] See section 2.5.
[25] This theme informs the analysis of WikiLeaks in Chapter Seven.

The pervasiveness of protocol as a form of management has led, according to Galloway (2004: 243), to the Internet being 'the most highly controlled mass media hitherto known.' This is provocative. It does not fit with the common social and political perception of the Internet as 'free' or 'unregulable'. Lessig (1999: 25) argues that 'there is no single way the Net has to be'. There are multiple forms it could take and each would allow for different degrees and types of control. Lessig's (1999) contributions to these debates are revisited below. Galloway's (2004) 'protocol' and Lessig's (1999) 'code' both signal the technical means by which online environments can be shaped and controlled. Increasingly, the influences upon this come from political and economic spheres – whose relationship is at times tenuous – which forces us to question where the 'centre' of a possible centralised model of control would lie[26]. However, control online is not dictated *solely* by the technical architecture. The concern of this thesis is with the *socio-technical* character of control. How control operates online is thus undecided. It is constantly being reconfigured as attempts are made to allow for greater control by governments and by corporations and as people and groups push back and strive for less control of this kind – or alternatively, control that protects values such as privacy and free speech.

2.3.3 EXPANSION

Beyond the technological and computational developments concerned with inter-networking, several related advancements have increased the worldwide availability, usage and capability of the Internet and the World Wide Web. Consequently, the opportunities for digital surveillance are enhanced. A few important and on-going developments can be identified: the improved physical infrastructure of the Net[27], the spread of Internet-enabled mobile devices (such as smartphones and tablets), and the expansion of wireless connectivity (Wi-Fi) (ONS 2013: 11). In the simplest terms, these developments mean that there is a greater variety of social activity that can be done online and can consequently be surveilled.

[26] Typically, conceptions of control have advocated a centralised model. This thesis later identifies some of the ways in which centralising *and decentralising* tendencies are evident in online control (see Chapters Five to Seven).

[27] There are over 260 submarine fibre-optic cables that constitute the primary physical architecture of the Internet. An interactive map of these cables is available at http://www.submarinecablemap.com/

Video-calls, online gaming and streaming of audio-visual content are three prominent examples.

Figures from the Office for National Statistics (ONS) bear out these points. In 2013, 21 million (83%) UK households had Internet access – an increase of 3% from the previous year (2013: 14). In 2006, 31% of households connected to the Internet used a dial-up connection on a standard telephone line; in 2013, this figure dropped to less than 1%. The majority of households are now connected via a broadband connection and of these, an increasing proportion year on year utilises fibre-optic or cable connections (ONS 2013: 16). Smartphones and, more recently, tablet devices have meant that people can increasingly access the Internet 'on the go'; 53% of adults accessed the Internet via a mobile phone in 2013, compared to 24% in 2010 (ONS 2013: 12).

This expansion of the communications infrastructure is relevant for this thesis in a few ways. The economics of the expansion of the physical infrastructure are regulatory forces in the same way as the infrastructure itself. They are both permissive and restraining in that they allow for a vast variety of online activity but also dictate who can do and access what online. They reinforce the fact that some of the chief influences on online control are economic but also that government regulation of these companies' activities will have a significant impact on this. We also see in these developments the increasing invasion of physical space by virtual. In respect of surveillance, as indicated above, ubiquitous mobile computing leads to the generation of more granular data about individuals, including their physical and digital behaviour.

2.4 REGULATION AND THE INTERNET

So far the concept of regulation has featured in technological terms. The discussion now turns to the social and economic aspects of regulation, to illuminate the influences on the growth of digital surveillance and subsequently why resistance may occur. Regulation is the control and management of risk through the use of law (Innes 2003) and attends to process rather than outcome (Innes 2014). In other words, like code and protocol, legislative (i.e. 'social' and 'economic') regulation dictates the way things must be done. This begins to develop the theme of nodal

governance underpinning the fieldwork of the thesis by introducing key nodes involved in practices of both digital surveillance and resistance – specifically governments and private entities.

It is difficult to argue against the advent of the World Wide Web as representing the most significant shift in respect of regulation concerned with the Internet; the Internet as a commodity grew from this point and has continued to do so since. The discussion points towards some of the technological developments associated with these economic motives. What follows here is an outline of some of the chief influences over the regulation of Internet communication. These are divided broadly into two main categories driving Internet regulation: commercial interests that position the Internet as central to the global information economy and public/state interests that respond to the challenges posed by the global Internet, particularly in relation to crime and national security.

2.4.1 CONTROLLING THE SWITCH

Commercial interests online fall into two broad categories. Primarily, this concerns those involved in the online business sector. However, we cannot forget the telecommunications industry itself that has ownership of the physical infrastructure of the Internet. As demand for Internet access and greater bandwidth increases, these companies have had an increasingly significant role to play. Owning the physical infrastructure obviously has ramifications for control over the Internet; the major telecoms companies have the power to prevent or at least slow down Internet traffic as it passes through their networks. Equally they can be instructed by court order to remove access to websites that have caused some transgression[28]. Their privileged position also means they have been a target for 'back door' access by intelligence agencies, as the Snowden revelations showed.

One example illustrates the power held by such companies. A current issue related to these companies, considered by many activists, campaigners and technologists as undermining the founding principles of the Internet is 'net neutrality'[29]. This

[28] This may or may not be effective, as the case of WikiLeaks (Chapter Seven) illustrates.
[29] For detailed background on this issue see 'Save the Internet' (http://www.savetheinternet.com/net-neutrality).

describes the free end-to-end movement of information across the Internet without restriction or privilege. Major US telecoms companies have lobbied for greater control over how they deliver services to customers. However, permitting telecoms companies to create a 'fast lane' system for Internet traffic, allowing them to charge additional fees for access to online services and giving them the capability to block access to competitors' networks and websites goes against the core ideals of the Internet. Vint Cerf, speaking on behalf of Google (2005) has noted:

> '…do great damage to the Internet as we know it. Enshrining a rule that broadly permits network operators to discriminate in favor of certain kinds of services and to potentially interfere with others would place broadband operators in control of online activity.'

The question this raises concerns the concept of control we are dealing with. Most references to 'centralised control' in the literature point to state control but in this context, commercial entities are equally as significant. It may be more appropriate to think of multiple, decentred points of control that seek to regulate different activities, according to different motivations of the public and private sectors – hence the framework of nodal governance employed here. Centralisation in this context is also, perhaps, inappropriate as it implies a single locus of control. This runs counter to what we have already established about the distributed structure of the Internet and, more broadly, about the role of flexible, global networks in the information economy. Related issues of censorship and intellectual property legislation highlight the potentially choking effect the major telecoms companies can have over the Internet. Economic advantage and provision of security are two primary motivations for regulation and surveillance online. Consequently, the drive for Internet regulation also comes from other commercial online service providers.

2.4.2 THE GROWTH OF WEB COMMERCE

It was not until the mid to late-1990s that commerce online began to grow. The emergence of the first popular graphical web browser *Mosaic* in 1994 was a necessary precursor to this, as were subsequent improvements in user interfaces with the Web such as *Netscape Navigator* and *Internet Explorer*. From the initial capability for individuals and businesses to communicate via the Internet to the World Wide Web as a global marketplace, the Internet has come to be the

manifestation of Castells' (1996) information-technology paradigm; it is a convergence of flexible, pervasive technologies operating via network logic to exchange and trade information.

The shift to online service delivery did not happen overnight. Even major multinationals such as Amazon and eBay (established in 1994 and 1995 respectively) were slow to take off. However slow this may have been, by the turn of the millennium the 'dot-com bubble' was at its peak; businesses had latched onto the idea of e-commerce, while Internet entrepreneurs were reaping the benefits of new technology and media markets. By 2001 the bubble had burst; the information economy could not keep up the pace. During the growth period of Internet commerce, however, the seeds were also sown for the future form of online entertainment and interaction. Pseudo.com – the brainchild of entrepreneur Josh Harris – was an interactive media/chat platform delivering audio and, later, video streaming entertainment services and was the first of its kind. The company was bankrupt in 2001 but the projects that Harris went on to develop were similarly 'visionary' – to a large extent predicting the growth of future Internet entertainment services. *We Live in Public*, a real-time Big Brother-style interactive broadcast of Harris' daily life, resonates particularly with this research. The public fascination with voyeurism helps to perpetuate the 'normality' of surveillance.

Today, Web commerce is dominant. Many high street retailers have an online presence, while purely Web-based corporations such as Amazon and eBay global commercial giants. Information and communication technologies are therefore disruptive in the sense that new business models continually replace more established ones. 'Big data', for example, is the big business of the moment. Growing from long-established practices in marketing and advertising, supplementing these with new data storage and processing power, businesses are now able to harvest and analyse astronomical amounts of consumer data. Cross-pollination of these datasets can yield accurate predictions about consumer behaviour and deliver targeted services to boost revenue. In an *Observer* article, Naughton (2013) describes how US retailer Target used data analytics to predict the due date of pregnant women based on purchasing histories. It is not far-fetched to see these systems drawing on the capabilities of biometric identification technology

to build a truly individual and real-time picture of consumers. In addition, retailers are not the only businesses to draw on the predictive potential of big data. Internet and social media giants such as Google and Facebook possess significant data repositories that are sold to advertisers, generating their primary source of income – particularly in the growing mobile Internet market. These practices exemplify some of the defining traits of the contemporary 'surveillance society'.

The relevance of this for the thesis lies in the predominantly commercially driven environment of the World Wide Web. The corporate interests at the heart of the Web shape the user experience and have dictated forms of interaction between users and corporations and between users themselves. One of the main drivers of Internet regulation, therefore, is protection for both commerce and for consumers. Safety of financial transactions is necessarily vital, but balanced against this is a desire to avoid stringent policies that could restrict online commerce (see Lessig 1999: 41 and Lyon 2003a). Resistance (to regulation and surveillance) does not come solely from citizens but just as emphatically from the private sector[30].

Other surveillance themes are evident here. 'Dataveillance' (Clarke 1988) grew out of pre-WWW informationalism and has evolved into the big data practices of the private sector. Lessig (1999) also takes up the theme of monitoring people online. One possible future for the Internet that he outlines is an 'architecture of identification'. Knowing and being able to verify who an Internet user is opens the door to much greater control; 'an ID-enabled world facilitates regulation' Lessig says (1999: 54), bringing to mind earlier work by Simon Cole (2001). In *Suspect Identities*, Cole charts the history of fingerprinting as a reliable and acceptable method of verifying identity. Regulating the Net to make users more 'visible' is, in this way, the latest step in the history Cole describes. Control across national and trans-national jurisdictions is also made easier in this way and both corporate entities and states have an interest in this. Identifying users and tracking them using cookies leads to more accurate and targeted advertising and subsequent economic gain. Verification is tied to security of online transactions and thus is favoured by commercial enterprises; encryption and certification of this kind already exists to an extent and is what has allowed Internet commerce to flourish. Yet what Lessig proposes goes

[30] See Chapter Six.

further. He envisions a cyberspace where ID authentication constitutes the *basis* of cyberspace. The link between digital surveillance and regulation is how Lessig sees this occurring: persuasion and incentives. By making online life easier for people who possess a digital ID, coercive regulation by the state that enforces the use of digital IDs is not required. *Convenience* is the key. Equally, as a society we accept much of the everyday, mundane surveillance we encounter because it is more convenient to do so (Lyon 2001; Andrejevic 2007).

The social and technical factors that make regulation and surveillance of online behaviour possible are inseparable. Writing in an American context, Lessig (1999: 53) calls this relationship 'East coast versus West coast code'. Law and regulation is an East coast (i.e. state) activity; code writing (increasingly a commercial domain) is a West coast one. The former progressively exerts power over the latter (through regulation), enabling the Internet architecture to be changed in favour of government interests. As Lessig describes,

> 'we must distinguish between two claims. One is that *given the architecture of the Net as it is*, it is difficult for government to regulate behaviour on the Net. The other is that, given the architecture of the Net, it is difficult for the government to *regulate the architecture of the Net*. The first claim, I believe, is true. The second is not' (1999: 43, *emphasis* in original).

Thus the relationship between political and the economic actors is a vital part of understanding regulation and control online. In Chapter Six, amidst a web of negotiation and bargaining they emerge as prominent actors – part adversaries, part allies. The broader tone of the thesis illustrates the difficulty in regulating and surveilling the Internet; there is (increasingly) resistance.

2.4.3 A GAME OF CAT AND MOUSE (PART 1: KEEPING PACE)

The discussion now expands on different ways in which regulation and surveillance overlap online. In the UK, the Electronic Commerce (EC Directive) Regulations 2002 are the primary instance of the protection afforded to consumers online and the obligations of service providers. The rapid development of technology and social interaction on the Web, however, has led some to question the applicability of these regulations. In dealing with a *global* network of communications, there are problems raised when it comes to the transmission of personal data across national

boundaries and the processing and storing of this data overseas. Here we see one of the primary challenges for regulation in the information society that is a direct result of the growth of a global, networked society.

Naughton (2013) identifies the current regulatory dilemma as that which surrounds the big data revolution, describing the usual legislative efforts to keep pace with technological change as akin to 'watching somebody try to drive a car by looking only in the rear-view mirror. The results are amusing and predictable but not really interesting.' At the time of writing, the European Commission is debating draft regulations concerning the processing of personal data of EU citizens. The General Data Protection Regulation (GDPR), proposed in 2012 outlines the need for more robust regulation in this area:

> 'Rapid technological developments have brought new challenges for the protection of personal data. The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life.' (European Commission 2012: 1).

The proposed regulation makes provisions for an overarching set of data protection rules for all EU member states. Unlike the current situation, where the EC Directive is incorporated into national legislation in varying ways (such as the UK Electronic Commerce Regulations), the GDPR is a unifying regulation with which all member states would have to comply. This raises a number of issues. First, EU member states are likely to differ in their approaches to data protection, in part as a result of prevailing attitudes towards privacy[31] and differing appetites between nation states for risk and regulation (Vogel 2012)[32]. This is already playing out in practice with the Information Commissioner for the UK stating recently the proposed regulation was 'too dirigiste' and that Britain 'was not interested in regulation that is a to-do list' (Oltermann 2013)[33].

Second, the GDPR places obligations on companies *outside* of the EU if they process the data of EU citizens. This is crucial; in the information society, such regulation is

[31] See Chapter Five.
[32] See Chapter Six. This observation also resonates with the observation in the previous chapter the global spread of surveillance has not been uniform.
[33] Following the UK European Referendum in June 2016 this may, of course, no longer be problematic.

bound to impact on the global economy. Data transmission between the EU and the US is currently governed by the 'Safe Harbor' regulation from 2000, which allows data to be transferred between the two states irrespective of different security standards. This, too, has been the subject of debate at the European Commission, particularly in the wake of Snowden's revelations regarding US and UK intelligence agency practices (see below). The GDPR proposes a fine of 2% of global turnover for breaching the regulations. For major corporations like Google and Facebook, this is more than a trifling figure. Tensions in this regard between national and supra-national governments and corporations are never far from the surface. Each of the actors here are in some way dependent upon the others in economic terms but will also have their own motives in regard to data protection and online commerce.

These themes are visible in the findings of this thesis. Differences between countries in their approaches to privacy and resisting surveillance are seen in Chapter Five. The issue of 'jurisdictionality' in respect of surveillance and regulation, is reintroduced in Chapter Six. And in Chapter Seven it is shown how WikiLeaks took advantage of different legal protections in different jurisdictions.

2.4.4 A GAME OF CAT AND MOUSE (PART 2: KEEPING TABS)

The focus shifts a little at this point to examine those forms of regulation that apply to digital/communications surveillance powers (specifically in the UK). Counter-terrorism is foremost among the justifications given by governments for the need for increased controls in cyberspace. The issue of cybercrime in general, however, has been the source of much academic and policy debate. With new technologies come new avenues for crime, whether these are 'traditional' crimes re-engineered for the virtual domain or entirely new crimes that are produced as a result of the new opportunities available (Wall 1998).

The debate around the GDPR has been complicated recently following the leaking of confidential information from the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ) by whistleblower Edward Snowden[34]. Besides providing unparalleled insight into the digital surveillance capabilities of the intelligence agencies, these revelations have also shed light on the

[34] See Chapter Seven.

uneasy relationship between the nation state and corporations. Big (communications) data is not only of commercial value; there is a legacy of intelligence agency interest, particularly in the US context, in the wealth of information available as Internet communication has developed.

Prominent among this history is ECHELON, a joint signals intelligence (SigInt) initiative between the UK, US, Australia, Canada and New Zealand – a partnership referred to as 'Five Eyes' in the latest leaked documents. ECHELON grew out of Cold War-era foreign intelligence and denotes the capabilities for the interception of communications data. Concerns grew during the late 1990s that ECHELON was being used beyond its original remit – including having been used for industrial espionage in the US – resulting in a European Parliament report (2001). Similar fears over public surveillance emerged in 2003 when the media reported on the US 'Total Information Awareness' program, which was subsequently (and astutely) renamed *Terrorism* Information Awareness. This initiative was naturally part of the significant counter-terrorism efforts post-9/11, which continue to be a primary motivation for government agencies to advocate the benefits of communications surveillance.

The recent revelations continue in this vein. Communications data have been described as both invaluable to law enforcement in order to combat terrorism and organised crime and correspondingly inaccessible (particularly in the UK context) owing to insufficient powers granted to police and intelligence agencies to obtain and retain such data. The current legislation in the UK governing surveillance powers of law enforcement and other public authorities and their access to personal data is the Regulation of Investigatory Powers Act 2000 (RIPA). Wide-ranging, RIPA covers a breadth of surveillance powers: the intercept of communications (e.g. wire-tapping) via a warrant, the collection of communications data[35] and (covert) human surveillance and intelligence. RIPA also outlines processes for dealing with encrypted electronic data and the oversight mechanisms provided by various commissioners and the Investigatory Powers Tribunal (IPT). RIPA repealed the

[35] Typically described as the 'who, when and where' of communications; for more detailed discussion see Chapter Six (6.4).

previous (and outdated) legislation in this area, the Interception of Communications Act 1985[36].

The primary purpose of RIPA and other legislation in the UK regarding collection and retention of communication data is for crime prevention. In practice, law enforcement can only access communication and content data on a case-by-case basis and after they have justified the *necessity* and *proportionality*[37] of the request as it pertains to a specific investigation. Communications data are typically used to ascertain 'the activities, contacts and whereabouts of a person who is under investigation' (for more detail see Home Office 2012). Accessing the *content* of communications is more strictly governed and, specifically, local authorities are not permitted under RIPA to use covert techniques to obtain these or any other data. To this end, several public authorities are allowed access to data including the security and intelligence services, police and HM Customs and Excise. Subsequent legislation has been motivated by this crime prevention agenda and while regulation is directed at Communications Service Providers (CSPs) with regards to data retention obligations, the underlying aim remains the same. The Anti-Terrorism, Crime and Security Act 2001 was a key instance of this, allowing for a code of practice[38] to be issued to CSPs delineating retention of communications data.

There is a significant degree of shared ground between RIPA and other Acts of Parliament and European Directives that are concerned with personal data. These have been the subject of increased scrutiny in recent years as digital communications have proliferated and both industry and government have sought to respond to opportunities this presents. The Data Protection Act 1998 – the implementation in UK law of the European Data Protection Directive 95/46/EC – is the primary legislation that covers individuals' rights regarding data held on them by organisations. It outlines eight principles that data handlers must abide by, including length of retention. Despite this, digital rights campaigners the Open Rights Group note that it 'is widely felt to be both weak and defective compared to the original Directive' (ORG 2014). As above, the GDPR has faltered, with opposition

[36] This Act, created as a response to the case of Malone (1984), prevented the unlawful interception of postal or telephonic communications, i.e. without knowledge/consent of the subject.
[37] Two key terms in the discourse of resistance – see Chapter Six.
[38] The Retention of Communications Data (Code of Practice) Order 2003

coming from the UK among others. Home Secretary Theresa May noted that '[t]he UK's priority is to ensure the right of access to, and to erase, personal data does not prejudice or hinder criminal investigations or proceedings' (Hansard 2014: WS112). Concerns have also been voiced over the detriment to the UK economy of proposed restrictions on transfer of personal data outside of the EU.

More recent is the EU Data Retention Directive, which came into force in 2006[39]. It compelled CSPs to capture various communication data relating to their customers and retain it for between six and 24 months. This was declared invalid on the 8th April 2014 by the European Court of Justice. In their ruling the Court stated that

> 'by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.' (Court of Justice of the European Union 2014)

While this ruling will provide a major hurdle for future legislative attempts at data retention in the UK, the appetite for such regulation has been shown clearly over the past decade. At the time of writing the most recent example of this was the Draft Communications Data Bill (CDB) 2012[40], the latest in a long history of attempted reforms of surveillance regulation. In 2006, the Labour government proposed the Intercept Modernisation Programme (IMP). While the IMP was never formalised, being dropped after an unpublished (and unfavourable) public consultation in 2009, its basis was allegedly the retention of greater amounts of communication data and the storage of these in a centralised government database[41] (see for example Prince 2008). Despite their opposition at the time to these plans the Coalition government revived the IMP in 2010 as the Communications Capabilities Development Programme (CCDP). While departing from the idea of a centralised database, these plans remained committed to the goal of managing the risk posed by technological developments; maintaining the focus on crime prevention and terrorism, the CCDP appeared in the 2011 revision to the government's counter-terrorism strategy (CONTEST):

[39] Implemented into UK law by Statutory Instrument (Data Retention (EC Directive) Regulations 2009).
[40] Since 2012, two further changes have been implemented/planned in the form of the Data Retention and Investigatory Powers Act (2014) and the Investigatory Powers Bill (2015).
[41] See Chapter Six (section 6.3) for a discussion of the relevance of centralisation of information.

> '…the Government will therefore introduce a programme to preserve the ability of the security, intelligence and law enforcement agencies to obtain communications data and also to intercept communications within the appropriate legal framework.' (HM Government 2011: 52)

Data collection, processing and retention thus have a prominent place in the crime prevention agenda of the UK government and (reformed) regulation here is constantly pursued. At the same time this is clearly a contentious area and one that is proving to be a volatile environment for governments to legislate in, not least because of competing interests in personal data. The public consultation on the CDB is the case study that is the basis of Chapter Six. These documents provide a unique insight into the development of digital surveillance capabilities as well as how such surveillance is resisted.

Snowden's revelations have also shed light on the role of the private sector in the activities of the intelligence community. As should be clear by now, the data held by corporations is a gold mine not only in economic terms but also, allegedly, for crime prevention purposes. Internet corporations do not acquiesce easily with government requests to hand over the personal data of customers. However, Greenwald *et al.* (2013b) described the complicity of a number of corporations, specifically Microsoft, with the data collection efforts of the NSA. Data that were encrypted, such as video chats using Skype, were made accessible to the NSA without the knowledge of users. It later emerged (Ball *et al.* 2013b) that the NSA was also actively pursuing means to gain access to encrypted information held by the likes of Google through sophisticated attempts to break encryption protocols[42] and by covertly influencing software design to make future access easier (creating 'back doors' into software, as mentioned above).

The reasons why regulation of Internet communication is pursued reveal a complex, dynamic interplay of corporate and state interests. These simultaneously competitive and cooperative interests have considerable impact for end-users and, clearly, raise important questions about personal data in the context of digital surveillance. Security of personal data emerges as a pressing question, as do the purposes for which personal data are collected either in the private sector or by intelligence agencies. The role and necessity of regulation of surveillance powers is

[42] One specific form of encryption targeted was 'Secure Sockets Layer' which is commonly used to protect online purchases.

brought into question by these revelations. The powers requested under the CDB were, in hindsight, remarkably similar to those already being practiced. Existing legislation such as the Regulation of Investigatory Powers Act 2000 (RIPA) is also questionable for its ability to curtail the use of such powers. The discourse around digital surveillance in the UK has not yet reached a critical mass but it is in the ascendance, helped along by such 'condensing symbols'[43] as the NSA Files. This is a significant point of departure for this research.

2.4.5 POLICY FUTURES?

In summing up this overview of the regulatory environment on the Internet, it is worth considering the future and what it may hold for Internet users, corporations and governments. Brown *et al.* (2010) conducted a series of expert focus groups designed to reveal opinions as to potential futures for the Internet. The outcome, resembling Webster's (1995) typology, was four possible scenarios that combine technological, economic and social trends. Each scenario depicts a future where the influence of a particular political agenda, corporate motive or social trend is prioritised. The four scenarios were shaped in accordance with four contemporary trends observed as part of the research process: the continued rise of the Internet economy in general; the increased significance of environmental concerns for people's social life; the amalgamation of consumer environments into social media platforms and; the role of the Internet as a democratising tool and an arena for dissent (Brown *et al.* 2010: 49-50). There is insufficient space here to deal with every aspect of these scenarios but some relevant features can be drawn out.

1. *Smooth Trip:* emphasises the development of the information economy. Saturated mobile and Internet markets drive innovation. Ubiquitous mobile Internet access. The Internet community becomes more united against commercial and governmental control of cyberspace; however, there is a global identity scheme akin to passports that ensure the convenience of an Internet-based social and professional life (bearing some resemblance to Lessig's (1999) architecture of identification).

[43] See Chapter Seven.

2. *Going Green:* major climatic shifts result in global environmental action. The Internet is the cornerstone of a new green global economy and simultaneously acts as a unifying arena for an increasingly network-aware citizenry.
3. *Commercial Big Brother:* the Internet is primarily a commercially-operated domain for advertising, consumption and entertainment; governmental engagement online is minimal. Users are passive, privacy all but disappears and user-generated content, innovation and education fade away in a commercial environment dominated by big Internet players.
4. *Power to the People:* greater user-interconnectedness leads to innovative and collaborative community and application building online. Users have greater control over Internet environments and in turn, governments and corporations are reactive rather than proactive. Inclusive technologies and politics produce locally-driven, informal social networks that effectively resist coercive regulation.

These scenarios are enlightening for this research. In each, there are elements that speak to a study of surveillance, resistance and control. Any one of the four scenarios *feels* possible and equally, some aspects appeal more than others. The continued growth of social networks is entirely plausible, as is their potential to foster community initiatives. The commercial value of personal data has already been highlighted here and thus it is also reasonable to foresee an Internet future that expands upon this. Brown *et al.* observe that the Internet will become vital for EU citizens in five to ten years' time (2010: 21), partly as a result of increased online delivery of government services. Such trends are already apparent in the UK, with the centralising of several services in one virtual gateway, GOV.uk[44]. Corporate and government-driven regulation has the potential to produce wide-scale change in user experience of the Internet. In this regard 'Commercial Big Brother' seems to be a 'worst case scenario', particularly from the point of view of a growing culture of surveillance, diminished personal privacy and restriction of free exchange of ideas online.

[44] See Chapter Six.

2.5 CULTURE AND THE INTERNET

The discussion so far has alighted briefly on some of the social and cultural aspects of the Internet and information society: the new diversity of Web interfaces, the increasing worldwide usage of the Internet and mobile Internet ubiquity. The commentary now turns to two distinct areas of interest: the legacy of hacker culture and 'Web 2.0'. Here, as in the preceding commentary, we can see the seeds of trends that could easily contribute to any of the four 'policy futures'.

2.5.1 THE LEGACY OF HACKER CULTURE

Hacking is a form of 'cyber trespass' (Wall 2001). For Wall, hacking can involve the planting of viruses, the misrepresentation of data such as webpages, breaking encryption and security measures in order to obtain classified information ('cyber spies') and targeted cyber-attacks on institutions using methods such as Distributed Denial of Service (DDoS) to render a system inoperable or cause economic damage ('cyber terrorists'). Yet hacking is also associated with the libertarian roots of the Internet. The 'true' hackers (Levy 1984) of the 1960s and 1970s were responsible for opening up much of the early computer hardware and for contributing to the gaming culture of the 1980s. Added to this, Taylor (2001) tell us about 'Microserfs' – former hackers who have since joined major computer firms[45] – and 'hacktivists' who are motivated by political goals. The significance of the history of hacking for this thesis is that it is tied to some of the core ideals that continue to motivate resistance to repressive forms of online control. It is also a highly effective and creative form of resistance, and the legacy of this is seen in the actions of WikiLeaks.

WikiLeaks' Editor-in-Chief Julian Assange was convicted in 1995 of hacking into the computer system of telecoms company Nortel[46]. Anonymous and their splinter group LulzSec are subversive groups of hackers/hacktivists who target institutions, businesses and government agencies – and now political movements as well – perceived to be undermining Web freedoms with restrictive regulation, privacy-

[45] Many IT companies, such as Microsoft and Google, also offer financial rewards to hackers and computer scientists if they can find vulnerabilities in new software, with the intention of improving the security of their products and services for consumers.

[46] His pseudonym 'Mendax' translates as 'noble truth'. Assange has been described as an 'ethical hacker' given his code of conduct of not causing any undue harm to computer systems that are hacked.

invading surveillance or censorship. Very few convictions have been brought against members of Anonymous, largely as a result of the difficulty in identifying those responsible for their actions[47]. The resilience of hacker groups such as Anonymous and LulzSec (and indeed WikiLeaks, although as a media platform they would not be classified as hackers/hacktivists) is due to the distributed nature of their networks afforded by the Internet. This echoes the earlier discussion of protocol (Galloway 2004); by its very nature, the Internet offers a unique and powerful site for both resistance as well as for control. Hackers operate within the realms of possibility of the Internet. In other words, they exemplify a form of resistance that is made possible by the very system that gives rise to the forms of surveillance, censorship and corporate control that are the targets of hackers' actions.

This provides a foundation on which to answer the research question of why people resist surveillance? As some of the actions of Anonymous and LulzSec demonstrate, anti-commercialism is at the heart of hacker culture. The ethos of hacker culture has always been, as Levy (1984: ix) identifies, based around the ideals that 'all information should be free' and 'access to computers…should be unlimited and total.' Similarly, British hacker Dr-K stated 'corporations and governments cannot be trusted to use computer technology for the benefit of ordinary people' (2000: 9).

In the context of digital surveillance, hackers motivated to subvert the workings of proprietary technology are arguably not contributing to a wider discourse about the prevalence of online surveillance and collection of personal data. However, this research views the issues as inter-related. Hacking for whatever purposes demonstrate the potential of Internet technology to foster resistance and dissent. Moreover, restrictive regulation around the Internet can be understood as part of a broader surveillance and control *culture* that grows out of the possibilities of a pervasive, globally networked society. This is predicated on the desire to know, to categorise and to single out for different treatment (see Gandy 1993; Lyon 2003b). For commerce, this is for profit. For government, it is for risk management. This discussion of hacking and hackers is therefore not an isolated one. It intersects with

[47] One 'Anon' was recently sentenced to 10 years custody in the US for his role in obtaining and making public millions of emails relating to intelligence contractor Stratfor, in the publication of which WikiLeaks also played a role (see Pilkington 2013b). The Stratfor case in itself has some relevance to this research, as the activities of Stratfor were bound up in the global surveillance-industrial complex.

a number of themes unified by the potential of the Internet to act as a site for resistance and dissent.

Not everyone who campaigns against restrictive Internet regulation is a hacker. However, they share common ideals and each group exists to the benefit of the other. The shared ethos stems from a desire for the free exchange of ideas and knowledge and for limiting the oversight of individuals online by commercial actors and governments. Digital surveillance in its many forms is incorporated under this umbrella in that it represents unwanted, or at least dangerous, incursions into private and social lives. To protect against this, a number of practical solutions have emerged that permit users to interact differently with the Internet (anonymously for the most part) and to protect themselves online from a demonstrably prevalent culture of political and economic surveillance. These tools are open-source and community driven. As such, they represent an important example of a mechanism of resistance and also, in the environment they produce, a safe arena for dissent.

Two of the best examples of these tools which are experiencing greater uptake are *The Onion Router* (Tor) and *GNU Pretty Good Privacy* (GnuPG). The Tor Project is run primarily by the Electronics Frontier Foundation and among other things, offers an Internet browser that allows users to remain anonymous online (i.e. no identifying IP address). GnuPG on the other hand is a piece of software for encrypting and key-signing communications. This allows users to send encrypted emails so that any interceptor will be unable to read the content and also to electronically 'sign' emails so that the recipient can verify the sender.

These mechanisms for 'surveillance self-defense'[48] are effective and becoming more widespread as the extent of digital surveillance becomes more widely known. However, there are two limitations to the technology. First, a degree of technical competence is required to operate Tor and GnuPG (as only two exmaples) effectively. Second, open-source encryption software (specifically Tor) has been targeted by the NSA in its attempts to break forms of online encryption. Nevertheless, these tools and others like them are a relevant example of the

[48] https://ssd.eff.org/

growing culture of privacy awareness amongst Internet users – and perhaps also an ingredient for the 'Power to the People' future Internet scenario.

Here an interesting analytical question arises, which Galloway (2004: 160) helps to formulate. Is resistance to digital surveillance to be understood in *individual* or *collective* terms? There is much to be said, as this chapter has shown, about the power of networks in contemporary society and thus the potential of collective, collaborative resistance. This is the primary contention of Chapter Five. However, Galloway draws out an alternative perspective. Hackers' resistive behaviour is equated with the more general rise of Internet awareness among the general public. For Galloway hackers are decidedly individual. Parodying traditional Marxist calls for unity, Brand (1987, in Galloway 2004: 160) writes: 'Workers of the world, fan out.' Further to this, the Critical Art Ensemble (CAE, 2009: 22) assert that '[t]he use of power through number – from labour unions to activist organisations – is bankrupt, because such a strategy requires consensus within the resistive party and the existence of a centralized, present enemy.' In the face of distributed/decentralised power, resistance needs to operate on the same basis. This is what the CAE go on to refer to as a 'nomadic' form of resistance (see also Deleuze and Guattari 1987); if you like, a type of guerrilla warfare.

The distinction between individual and collective resistance is blurred. We should not assume that collective, networked action is the best or, indeed, only way to challenge the enactment of control. Neither must resistance be approached as a contest between a powerful and powerless group. Resistance to surveillance does not only come from campaigners for privacy, for instance, but from private sector entities with substantial capacities to surveill Internet users. In other words, the configurations of resistance are many and will vary according to context. In the context of the information society, the target of resistance is often where technologies are developed or regulated that are perceived to threaten the interests of one or more groups. All of these ideas are evidenced throughout the thesis as various forms of networked and individual resistance are explored.

2.5.2 WEB 2.0

The combination of technological and economic antecedents circa-2000 produced significant shifts in the way in which every day Internet users experienced the Web but also importantly, *shaped* the Web. More and more social activity has moved online and found new ways to be expressed and engaged with. Consumption, dating, counselling, gaming and finding news have all established an online presence. From the early 2000s, however, the most successful Web enterprises were those that re-positioned the user as producer, or rather 'prosumer' (Toffler 1980).

The term 'Web 2.0' was coined in 2004. Its definition is contested but broadly speaking it is intended to refer to a step-change in the way in which users engage with the Web. In comparison to 'Web 1.0' – webpages created and edited by administrators – Web 2.0 emphasises the shift to *user-generated content* (UGC). Alongside UGC, Anderson (2007) notes five other key trends associated with Web 2.0: harness the power of the crowd; data on an epic scale; architecture of participation; network effects and; openness. When aggregated, these factors add up to increased online participation and collaboration between individuals and groups. As Anderson (2007) phrases it, Web 2.0 'lowers the barrier to entry'. There is overlap here with Castells' (1996) notion of informationalism – knowledge being brought to bear upon knowledge. Despite the emergence of 'prosumption', new markets have grown out of the value that user participation brings. The 'big data' industry and associated consumer analytics are prime examples of this. In topological terms, too, drawing on Webster's (1995) schema of the information society, Web 2.0 draws our attention to the 'coming together' of people online to collaboratively work and create documents, projects and communities.

Web 2.0 is not necessarily an accepted phenomenon. The idea of connecting people rather than simply computers as unique to Web 2.0 is rejected by Tim Berners-Lee, who, when questioned whether Web 2.0 is about connecting people and facilitating collaboration responded:

> 'Totally not. Web 1.0 was all about connecting people. It was an interactive space, and I think Web 2.0 is, of course, a piece of jargon, nobody even knows what it means. If Web 2.0 for you is blogs and wikis, then that is people to

> people. But that was what the Web was supposed to be all along…the idea of the Web as interaction between people is really what the Web is. That was what it was designed to be – as a collaborative space where people can interact' (Berners-Lee 2006).

With that said, there has been an undeniable increase in Web services that foster participation, collaboration and interactivity. The most prominent example of this is social media. There is insufficient space here to elaborate the many linkages between social media, the changing face of the Web and surveillance discourses (for example Trottier 2012). Social media cannot be ignored, however, and hence there are a few key points to note.

The reach of social media is vast. The largest social media website, measured by active users, is Facebook, who claimed to have over 1 billion users in October 2012 (Facebook 2013). In July 2013, 100 million people use Facebook on mobile per month. By comparison, Twitter advertises over 230 million active monthly users, sending 500 million tweets per day and 76% of whom are active on mobile (Twitter 2013). Both of these sites are listed by Alexa Internet (2013) in the global top ten most visited websites[49]. Also in the top ten are three other social networking sites (YouTube, LinkedIn and China's QQ) and in addition Google, at number one, offers social networking services via Google+ launched in 2011. If nothing else, these figures serve to enforce earlier observations regarding the expanding information economy.

Social media demonstrate all of the characteristics of UGC proposed by Anderson (2007). They are by their nature descriptive of UGC. Problem-solving on social media points to its crowdsourcing potential. Mammoth quantities of data are produced by such a volume of users, which are readily amenable to not only social science analysis but are collected, processed and sold in the information economy. The 'architecture of participation' describes the inviting usability and personal benefits of social media and the network effects – the suggestion that services get better the more users engage with them – are, in essence, the foundation of these companies' business models. Last, openness in social media can be understood by the development of myriad secondary applications and programs that 'tag-on' to social media or make use of publicly available application programming interfaces

[49] Based on monthly traffic rank, calculate from the combined average daily visitors and page views.

(APIs) to harness the potential of social media data. The very concept of 'sharing' information in these public forums is synonymous with openness. However, Lessig (2006, in Anderson 2007: 25) offers a word of caution here: with social media such as YouTube (and the same largely applies to Facebook amongst others) 'never does the system give users an easy way to actually get the content someone else has uploaded.' This begs the question of to what extent 'Web 2.0' (at least in the corporate service provision sense) is truly collaborative and participatory. Are these qualities reserved, instead, for non-corporate, community-based initiatives that hark back to the more liberal, utopian, open-source roots of Web 1.0 technologists?

The coincidence of Web 2.0 with technological developments already mentioned – such as data storage capacity – and economic motivations to do so has meant that our personal digital data are increasingly more permanent. This has led to debates about the 'right to be forgotten'. As is most often the case, once data are provided by us to, say, Facebook, those data are free to be collected, analysed and sold by the company. Should we choose to close our account with Facebook, what happens to the data? That history of social interaction is not forgotten, even if data are deleted from your account before leaving.

Recent social networking applications for mobile phones play on this desire for 'ephemeral' data. *Snapchat* is an application that allows users to take a photograph and send it to a contact, where it displays on screen for between 1-10 seconds and then disappears. There is no record left on the recipient's phone[50] but they can 'screenshot' the photo. This system is likely to appeal to a desire for impermanence in social media – even more so if the recent trend of teenagers spending less time on Facebook in favour of mobile messenger apps continues (Olson 2013). This may not be problematic for most users but it does, at least theoretically, raise the possibility of embarrassing images being recovered at a later date. On a more formal level, the 'right to be forgotten' appears in the proposed GDPR outlined above.

[50] It has been demonstrated that with the right forensic data tools *Snapchat* photographs can be recovered from the recipient's phone (InfoSecurity 2013).

Web 2.0 has also featured prominently in the surveillance studies literature, most notably for discussions of the surveillance/sousveillance/synoptic[51] potential of social networking websites. Trottier (2012) has argued that a characteristic of Facebook interactions is the tendency/ability for users to expose others without their knowledge – for instance by 'checking in'[52] to locations with friends or tagging them in photos and comments.

These observations of Web 2.0 are important for this thesis in a number of ways. Social media represent an important addition to the landscape of digital surveillance and control. For one, we again see the relevance of Lessig's (1999) architectures of identification. Certain information on Facebook cannot be accessed (e.g. the profiles of people you are not friends with) because of who you are verified to be. Simultaneously, one's identity is monitored intensely on Facebook in order to gather information that can be sold to advertisers. This chapter has already emphasised the role of commercial regulations online. These are central to the operation of social media but there has also been increased regulatory attention from government. Chapter Six illustrates the attempts made by the UK government in 2012, in part, to capture social media data about individuals. The picture is not entirely negative however; regulation also dictates social media companies' responsibilities to service users.

Berners-Lee (2010) was among the first to describe Facebook and its ilk as 'walled gardens'; virtual environments within which corporate owners have control over all media, content and access. His claim that 'the Web could be broken into fragmented islands' is reminiscent of the decentralised conception of control. Social media are digital surveillance 'hotspots' and are consequently significant nodes in the nexus of control and governance. Yet at the same time they offer the resources for public debate and online civic engagement, as Chapter Five illustrates. Once again is dualism – of the surveillance and resistance dynamic playing out in the same digital spaces – a prominent theme. The apparent shift in the nature of social

[51] See Chapter Three.

[52] Checking-in via Facebook uses either GPS data or user-generated information to display where a user is currently situated, for example, a restaurant, the cinema or their home. This is displayed on the user's Facebook Wall as 'Wil Chivers was at Cardiff University School of Social Sciences with *Friends X, Y, Z*.'

organisation online represented by Web 2.0 is the basis for this – fostering the collaborative, networked interaction of individuals.

Projecting into the future of the Web is a difficult task, given a lack of agreement on where we are at present. However, the vision of Berners-Lee is of a 'Semantic Web' that understands the context of data. The effect would be to produce a Web that is more intuitive and relevant for users. Again, this relies on processes that overlap significantly with surveillance. In the context of this research, the Semantic Web contributes to the trend towards an 'Internet of Things'. This is the idea that more of our physical world is becoming connected via the Internet thanks to technology such as Radio Frequency Identification (RFID) tags, micro-sensors that store and transmit information about the item to which they are attached: clothing, foodstuffs, electronics. It is a prime example of making more of the world surveillable, showing more people *doing* surveillance and extends Lyon's (2001) classic definition of surveillance to the inanimate world. As Murakami Wood (2008: 93, citing Arraya 1995: 233) has also observed, 'a society of pervasive computing is a pervasive surveillance society because it must "give instantaneous access to any 'thing', including tools, books, and people, transforming them into *surveillable things*"'. Such a note is an appropriate point to draw this discussion of the connection between the information society and surveillance to a close.

2.6 IMPLICATIONS FOR THE THESIS

This chapter has illuminated the various connections between the contemporary information society, digital surveillance and resistance. These inter-related issues are the foundation of the thesis. The research, outlined in the previous chapter, is concerned with exploring the nature of control in the information society, using the relationship between digital surveillance and resistance as an analytical lens. Gaining even a small appreciation of the numerous and complex ways in which the information society has given rise to the potential for new forms of surveillance and resistance is a useful first step in this endeavour.

In particular, the chapter has sought to present two related issues that help to ground the research. The first is the combination of *social* and *technical* factors that constitute the information society and its relationship to forms of surveillance and

resistance. The Internet is in one part a technological system that creates the possibility for certain kinds of behaviours and processes – including surveillance and resistance (Lessig 1999; Galloway 2004). Equally, the Internet is a social system wherein new patterns of order and organisation have emerged. A product of both political and economic motivations, these emphasise informationalism and digital surveillance. Resistance occurs where other social and cultural values are promoted; some dating back to the roots of the Internet, others a product of continuously evolving forms of online social organisation. The thesis demonstrates that the socio-technical workings of the information society (and the Internet specifically) allow us to think about a 'socio-technical' form of social control.

The second issue is regulation. This thesis is not a study of regulation. However, the relationship between digital surveillance and resistance is influenced greatly by the forms of regulation that this chapter has delineated: of the Internet architecture that facilitates both surveillance and resistance; of the ways in which people can connect and communicate online; of how personal data can be transmitted around the world, and; of how communications providers conduct digital surveillance on behalf of governments and law enforcement. These echo the combination of social and technological components of control.

This scene setting of a global, networked and information-based society implicates and introduces a breadth of social actors, whose relationships to one another constitute the landscape of digital surveillance and resistance. This foreshadows the concept of nodal governance developed in Chapter Three and that guided the choice of research sites in the fieldwork. This implies multiple centres of control, each with their own motivations for pursuing surveillance or resisting surveillance. Those involved both compete and cooperate with one another (Wood and Shearing 2007; Fuchs 2008), which connects to the earlier discussion of the simultaneously individualised and collective nature of resistance. Resistance to digital surveillance, then, is more complex than opposing dominant power. There are cultural, technological and political influences on how and why resistance (to surveillance) occurs. The story of surveillance and resistance is an old one but it finds new energy in the contemporary information society.

-.-- --- ..- .-- . .- .-. -.-- --. .. .- -. - ... --- ..-. ..-. .-.. . ...- -. -.. ... - . . .-.. --..--

CHAPTER THREE

THEORETICAL FOUNDATIONS: SURVEILLANCE, CONTROL AND GOVERNANCE

3.1 INTRODUCTION

This chapter explores the major theoretical constructs and debates that guide this research: social control and surveillance. While in many ways theories of surveillance are a subset of the broader concept of social control, the relatively young discipline of surveillance studies has much to contribute. Given that the aim of this thesis is to examine the relationship between surveillance and resistance and what it can tell us about contemporary forms of control, there are several themes from the surveillance literature that can be drawn out, particularly where they intersect with dominant theoretical approaches to social control. The aim of this chapter, then, is to lay out current and historical thinking about social control (underpinned by notions of power) and to illustrate how studies of surveillance fit within these discussions and contribute to the framing of the research.

These tasks also entail developing an appreciation of the theory of nodal governance. This theory guides the analysis in Chapter Five but, as described in Chapter One, it also structured the fieldwork. It is important, therefore, to understand how nodal governance fits with theories of control and with the approach that was adopted during the research. Reflecting the previous chapter, this chapter argues for a conception of control alert to its networked, flexible character in the contemporary information society. This is an approach that, in some ways, challenges the orthodoxy of a Foucauldian reading of contemporary surveillance and also necessitates examining a broad range of social actors and domains implicated in practices of digital surveillance and resistance.

3.2 IDEAS OF SOCIAL CONTROL

Social control is a concept employed widely across the social sciences. Although each disciplinary treatment brings with it intrinsic assumptions about the nature of the subject under scrutiny, there have been key influences from the major theoretical traditions of the social sciences that have shaped how social control has come to be understood. The earliest engagements with ideas of social control – which pre-date the coining of the term as such – can be seen in the foundations of modern social science. Marx, Weber and Durkheim all grappled with questions of social order, conformity, conflict and deviance, all of which are important constituents of the study of social control. The influence of these early thinkers can still be seen in the formulations of control described here.

This discussion traces the major contours in thinking about social control. The various approaches that are outlined touch, in different ways, upon issues that relate to surveillance. These connections are returned to later where the discussion focuses more explicitly on key issues in the surveillance literature.

3.2.1 CAPITALISM, INFORMATION AND CONTROL

Radical perspectives on social control emphasise the inherent conflict in society caused by the capitalist system (e.g. Bonger 1969) or other relations of domination and subordination (Dahrendorf 1959). It is with the state that the power to exercise social control lies, in order to maintain the social order necessary for the functioning of the economy. While state control today may not be as overt as described in the earlier works of Marx, there is still considerable attention given to the forms of control enacted by powerful capitalist institutions that are designed to maintain the status quo of the modern economy. Turk (1982) describes how the form of control enacted by these institutions has become more subtle – a 'soft' form of control. A contemporary parallel here is with Lessig (1999) whose 'bovine metaphor' suggests that control is best achieved online by means of small 'nudging' practices rather than coercive enforcement.

The previous chapter described the informationalising of today's economy and the shifting relationship between state and private sector that is crucial for this research.

Online, private sector corporations exert significant influence in shaping social engagement with technology. Meanwhile, the government works on two fronts: ensuring a stable, competitive economy and protecting the public against deviance in a new virtual environment. The lessons of the radical perspective on control, therefore, are still pertinent. A prominent example is Fuchs (2008) who provides an in-depth analysis of the role played by governments and the private sector in shaping the socio-technical Internet environment. He argues that the global, networked information economy is characterised chiefly by structural inequalities; 'segmented spaces in which central hubs (transnational corporations, certain political actors, regions, countries, Western lifestyles, and worldviews) centralize the production, control, and flows of economic, political and cultural capital' (2008: 119). Competition, then, defines the contemporary information society.

An important consideration therefore is the perceived legitimacy for the capitalist system and support for the dominant discourse on the need to control online deviance. Media provide government with an avenue for achieving this. The construction of deviance and deviants in the press and ultimately the generation of 'moral panics' can legitimise the need for (increased) social control of certain populations (Cohen 1972; Hall *et al.* 1978)[53]. Government frequently portrays greater surveillance powers in the press as necessary for combating terrorism. However, their ability to control this discourse has been challenged by the emergence of a new media ecosystem that capitalises on the subversive possibilities provided by Internet communication (see Associated Press 2013). Fuchs (2008: 119-20) again picks up on this tension; the information economy 'is an antagonistic space that by producing new networks of domination also produces networks of liberation that undermine the centralisation of wealth and power that has thus far been achieved by networking.' Competition is thereby challenged by logics of cooperation.

Traditional conceptions place the locus of control with the state, although more recent analyses such as that of Fuchs (2008) do acknowledge the shift to other (commercial) institutions. However, a limitation is the modernist, binary conception of power that is its basis: power is 'something that is possessed by the dominant and

[53] Chapter Seven is oriented around these themes.

wielded against the subordinate; the subordinate may, in turn, resist and attempt to seize power' (Raby 2005: 152). A number of assumptions follow from this. Chiefly, power is a one-sided resource. You have it, or you do not. While there are strengths to the radical approach to social control, this formulation of power limits its explanatory capacity in the context of contemporary social control. Work discussed below (Sharp *et al.* 2000) is a helpful remedy to this, as are post-structuralist conceptions of control.

3.2.2 POST-STRUCTURALISM, DISCIPLINE AND CONTROL

The post-structural approach, by contrast, sees power as distributed strategically across the various institutions of society. The state retains an important position in the apparatus of control but this perspective recognises the dispersal of control functions beyond the sole remit of the state. This clearly differs from the modernist basis of radical theories, which, as Hollander and Einwohner (2004: 550) note, 'ignores the fact that there are multiple systems of hierarchy, and that individuals can be simultaneously powerful and powerless within different systems.' Raby (2005: 162) adds to this, asserting that 'power is enacted by all, and people occupy multiple subjectivities, or locations in relations of power.' Power, then, is not possessed or wielded solely by one group. Instead, it is a *relation* that flows throughout the institutions and citizenry of a society. The contention of this research is that this distribution of power is amplified as an effect of the global, networked information society.

The main proponent of this conception of power and control is Michel Foucault. Foucault's contention, primarily drawn from *Discipline and Punish* (1977) but found elsewhere in his works (Foucault 1991), was that modern society was characterised by the dispersal into wider society – beyond closed penal institutions – of a particular logic of control: discipline. This broad social project was what Foucault called governmentality or 'the art of government', but it was not limited to the state and politics. Rather, this described the organisation of rationalities and techniques for controlling human behaviour and producing a 'self-controlling' populace that met the needs and requirements of the (then) dominant factory system. Such 'normalising' strategies were influenced by the growth of natural and behavioural

sciences, which generated new understanding about the interaction, organisation and psychology of the human subject. *Knowledge*, therefore, assisted in the categorisation and classification of behaviour – in particular deviancy – that was central to the operation of this governing mentality. Discipline was thus a 'technology of the mind', a form of control that Foucault (1977) described as 'soul training'. He argued this marked a significant departure from earlier societies characterised by sovereign monarchical authority and its accompanying strategy of practising control with spectacular, bodily and lethal acts of punishment. Discipline was thus a subtler, more pervasive form of control.

Nevertheless, Foucault's concept of disciplinary power was in many ways a product of its age. Deleuze (1992) updated the concept, arguing that as a disciplinary society was borne of the factory system of labour, the evolving information society characterised by the machinery of computers, networked organisation and data flows required a new model of understanding power. A 'control society' by comparison, then, operated on a much more granular level. Individuals were (or indeed, are) no longer the unit of knowledge. Instead they are 'dividuals' constituted by numerous data streams that are a product of large amounts of information that is volunteered or collected about people and aggregated to provide a picture of broader social patterns. The parallel with the trends of the information society outlined in the previous chapter is clear, as is the connection to ideas of digital surveillance discussed later.

The lessons of discipline and control are important and both have their merits. Foucault's (1977) dispersal metaphor and basis of power in knowledge of human subjects are just as instructive as Deleuze's (1992) necessary update of this work to fit with global, networked and distributed patterns of social organisation. Foucault's work has of course had a major influence in the field of surveillance studies. This legacy should be acknowledged, not because it provides a universal model for understanding contemporary control or surveillance practices, but because it allows us to question current logics of control. There is also a degree of continuation into present forms of control. However, there are also many limitations. The accuracy of Foucault's historical analysis, for example, is questioned by Garland (1985, 2001), whose later work is arguably more sophisticated and rigorous. Equally, to return to

the primary critique outlined in Chapter One, the top-down model of surveillance that Foucault's panoptic metaphor suggests is inappropriate in the contemporary networked information society. This point is at the heart of this research.

3.2.3 'POST-SOCIAL' CONTROL AND NODAL GOVERNANCE

The post-structural perspective typified by Foucault and the patterns he identified were developed in the work of Stan Cohen (1985). Cohen noted a number of different trends that broke with those previously observed. Specifically, the state was divested of their monopoly over deviants and deviancy. However, the progressive intentions behind this 'destructuring impulse' were undermined; the result, ironically, was to extend the 'nets' of social control more widely, intensely and invisibly across society. Consequently, delegating control of deviancy *to* the community was subsumed by the control *of* communities. A broader spectrum of individuals and groups were caught up in a more pervasive and subtle control nexus. Rather than replacing the state-based control regime, the new formations augmented existing strategies with the result that the system became increasingly punitive. As this trend continued, the boundary between public and private domains was blurred; security and control were commodified and an array of private interests infiltrated their delivery (Shearing and Stenning 1981, 1983, 1985). Cohen's reformulation of the character of modern social control bears some resemblance to the patterns identified by Foucault – primarily the dispersed character of control – but in other respects it paved the way for novel thinking about social control that recognised the plurality of actors beyond the state with a stake in the system and the manifold aims that guided the questions of whom and how to regulate through control mechanisms.

The same conception of power underpins this approach. The central idea that control is pluralistic is extended by Johnston and Shearing (2003; see also Shearing and Wood 2003; Wood and Shearing 2007). Based on the earlier intellectual foundations of Shearing and Stenning's work (above), these authors sought to develop an alternative language of social control. One that moved beyond concerns with the 'social' (hence 'post-social' control) as both a *target* and *location* for control and advocated in its place distinct and varied locales or sites of governance – *nodes*.

'Nodal governance' therefore implies the presence of networks of governing entities with different aims and ideas about the governance of security. Increasingly, these 'mentalities' (Burris *et al.* 2005) are centred on managerialism, risk and prevention (Feeley and Simon 1994). This is due partly to the presence of private auspices of control alongside state agencies, as intimated above. This 'blurring of governing mentalities' (Wood and Shearing 2007: 29) – the recognition that other ways of thinking about the problem of security may be more effective – mirrors the patterns identified earlier by Cohen. On the same note the nodal governance perspective

> 'is not one that assumes a decline in state authority and power. Indeed, one could argue that state power is now even more diffuse and pervasive through the ways in which it governs through the knowledge, capacity and resources of others. The conceptual shift we advocate is simply one that recognizes the diversity of entities…that function as auspices or providers of security…' (Wood and Shearing 2007: 33-34).

Burris *et al.* (2005: 37-38) suggest that alongside specific ways of thinking about the matters they seek to govern (mentalities) nodes have specific methods ('technologies') for exerting their influence, the 'resources' to support their operation and have an 'institutional' form that allows the 'directed mobilization' of these three characteristics[54]. Importantly, nodes *exist*; they are not simply theoretical points in a network. The implication for this thesis is that their character and the relations between them can be explored empirically.

Wood and Shearing (2007: 27-28) observe that whether nodes come together to form networks is, likewise, an issue to be explored empirically. In language that resonates with Fuchs (2008), it is not a given that networking or cooperation exists between the multiplicity of actors involved in the system. Indeed, there can be competition between nodes – how, where and whom should be governed. This framing of governance (or control, whichever language we choose to use) as something that is negotiated and constructed as well as both coordinated and uncoordinated is one that guides the analysis in this research. The theme of competition and cooperation introduced in Chapter Two is an enduring one in this thesis and Chapters Five and Six pay particular attention to this antagonism.

[54] There is some conceptual overlap here with the literature on social movements that suggests groups and organisations can have more or less influence depending on their ability to mobilise resources. While this thesis does not delve into these debates, the parallel should be noted in the context of the analysis in Chapter Five.

Nodes are both governing and governed entities. They seek to enact their own forms of governance/control while at the same time being subject to forms of influence and mobilisation by other nodes. For instance a key dynamic that is seen at play in this research is that because private sector CSPs have extensive digital surveillance capabilities, the state attempts to regulate their conduct to harness these resources for crime prevention purposes. *Resistance*, the thesis argues, is therefore a part of the system of nodal governance insofar as nodes compete against one another for ownership of their various forms of social, cultural and economic capital (Bourdieu 1986; Dupont 2003, 2006) – their mentalities, technologies and resources[55]. However, what seem to be missing from the literature on nodal governance are the broader forms of resistance to the technologies of governance. In applied terms, this means resistance to the practices of surveillance that public or private nodes seek to implement. There is a global network of organisations that seek to resist surveillance practices[56]. These entities are as much governing nodes as the state and private auspices in that through their interactions with these entities they contribute to shaping the character of contemporary control. What we see, then, and what the empirical aspects of this thesis illustrate is that some nodes are engaged predominantly in resistance activity (civil society actors and media platforms), some are engaged more with surveillance as a form of control (the state) and others occupy both positions, being agents of surveillance for their own or others' purposes at the same time as resisting the efforts of the state to co-opt their resources and technologies (CSPs).

The conceptual shift that connects the theory of nodal governance to the broader 'post-social' approach to control is one that illuminates the plurality of actors involved in shaping control and how their varying mentalities and technologies influence the character of control. Governance, then, is about management of social systems. Nodal governance 'is an elaboration of contemporary network theory that explains how a variety of actors operating within social systems interact…to govern the systems they inhabit' (Burris *et al.* 2005: 33). The potential inherent in such networks has been amplified in the information society: 'information technology has allowed networks to retain adaptability and at the same time to achieve superior

[55] See Chapter Five and, later, Chapter Eight.
[56] See Chapter Five.

levels of coordination and management' (Burris *et al.* 2005: 37). Equally, the *need* to govern via networks is amplified in the context of global communication and the new risks presented by the contemporary information society. As with Deleuze's reworking of Foucault's disciplinary society, the theory of nodal governance is designed to fit alongside and explain contemporary patterns of global, networked social organisation. The unit of analysis in accordance with this approach are the various nodes that constitute such networks. The framework for this thesis is based on precisely this idea. The fieldwork examines different nodes involved in the dynamic relationship between digital surveillance and resistance: civil society groups, the state, communications service providers and media platforms. In turn this allows for a discussion of the character of contemporary social control.

3.3 SURVEILLANCE AND SOCIETY

The second half of this chapter provides a critical overview of the treatment of surveillance in the literature, including how it fits alongside accounts of social control and how resistance to surveillance has been explored to date. Throughout this discussion, a typology (of sorts) is developed for understanding different forms and features of digital surveillance: panoptic, political, economic, lateral and resistive are all ways of thinking about surveillance that will be useful for the analysis later in this thesis.

3.3.1 DIGITAL SURVEILLANCE DEFINED

Surveillance is a mode of social control. It features in this thesis as a vital part of this apparatus, particularly as a result of the proliferation of tools and techniques of surveillance made possible by the growth of the Internet. The most frequently cited definition of surveillance is:

> 'any collection and processing of personal data, whether identifiable or not, for the purposes of managing and influencing those whose data have been garnered' (Lyon 2001: 2).

The parallels in this definition with concepts of control and power will be returned to. Lyon's definition for the time being allows us to grasp the breadth of activity that might be associated with contemporary digital surveillance. Other authors have

sought to provide a degree of clarity as to precisely what sorts of practices 'count' as surveillance. Marx (2002: 12) defines 'new surveillance' as 'the use of technical means to extract or create personal data' that can be drawn from individuals or contexts. This draws attention to the continuing evolution of tools of surveillance beyond our own senses and self-reporting of information. Moreover, extraction of data from contexts as well as individuals, signals the trend towards techniques for pattern recognition and analysis. Marx also aims to distinguish 'new' surveillance by its move away from purely visual forms of surveillance, such as CCTV, which have long held the primary position in society as the most readily identifiable form (both physically and metaphorically) of surveillance. As the synopsis in Chapter One described, surveillance as a crime prevention mechanism in the UK developed primarily around CCTV strategies. Marx's observations are helpful for this research insofar as they point towards the on-going technological advancement of surveillance in the information society and its capacity to render people and contexts visible in increasingly sophisticated ways.

Fuchs (2008) also adds to this definitional debate, distinguishing between 'monitoring' and surveillance (see also Giddens 1985) as well as the various motives that exist in the information society for conducting surveillance. Andrejevic (2005) has questioned the impact for understanding surveillance in light of the increasing number of ways in which people can communicate and connect with one another online (Web 2.0 services such as social media are a prime example here). The thrust of his observation is that such connectivity facilitates peer-to-peer or *lateral* forms of surveillance. In this sense, information technologies empower people to become surveillance agents – able to (covertly) observe the actions of romantic interests, family and friends – at the same time as they subject themselves to surveillance by others. Fuchs (2008) hesitates to identify this trend as surveillance, preferring instead to designate this as monitoring. The difference between monitoring and surveillance comes down to motivation. Monitoring is the 'general notion of providing and gathering information with the help of electronic systems', whereas surveillance is 'the gathering of information on individuals or groups in order to control their behaviour' (Fuchs 2008: 268). Controlling behaviour is done for political or economic purposes; therefore surveillance is either a product of state efforts to control deviancy or private sector pursuit of profit through electronic

commerce. Surveillance, for Fuchs (see also Ogura 2006), is about influencing or managing human conduct[57] and therefore we see a good deal of similarity with Lyon's (2001) earlier definition.

A number of observations follow from this. It may not be necessary to distinguish between monitoring and surveillance. The reason for this is that surveillance implies a power dynamic; it signifies the capability to watch, observe or gather information about someone or something else. The etymology of 'surveillance' (to 'watch over') is a simple point that underpins many of the theoretical expositions of surveillance. While digital surveillance still incorporates these power dynamics, it does not follow that this must be a hierarchical relationship. Andrejevic's 'lateral surveillance' is preferred here to 'monitoring' because the former still points to the power dynamics at play[58]. Lateral surveillance does not involve the violence of the law or the market (Fuchs 2008: 267). However, there is an element of influencing other people through the carefully managed interpersonal interactions we engage in within online spaces, whether this is volunteering audience-specific information about ourselves (making ourselves 'surveillable') or monitoring the activities of others to guide our interactions with them.

Nevertheless, Fuchs is correct that it is important to be aware of the different motivations for surveillance. The primary drivers behind digital forms of surveillance are indeed political and economic. This fits with the discussion of the formative influences on the information society in Chapter Two. A chief characteristic or effect of surveillance – one that predates the contemporary information society but has been enhanced significantly by its continued expansion – is 'social sorting' (Lyon 2003b). This is the social and economic categorisation of people and groups that aids the goal of surveillance to influence and manage populations. In the commercial realm, 'the panoptic sort' (Gandy 1993) refers to singling out certain consumers for differential treatment or targeted advertising based on analysis of personal data. Gandy's earlier elaboration of this concept has found new currency with digital surveillance technologies. These practices are at the heart not only of

[57] Referring to Haggerty's (2006) observations regarding the potential for surveillance of non-human entities (bacteria, space, flora and fauna for example), Fuchs also classes these as monitoring.
[58] 'Interpersonal' or 'participatory' (Albrechtslund 2008) surveillance could also aptly describe the process and highlights the lack of political or economic motive.

online and electronic commerce (economic surveillance) but also increasingly in the efforts to identify risky or dangerous categories of people (political surveillance). We are often unaware of the existence of these various economic and political categories and of the fact that we may be allocated to them. Regardless, we are funnelled into these categories through surveillance of personal data that we supply (often willingly) online. As Lyon notes,

> 'in everyday life our life-chances are continually checked or enabled and our choices are channelled using various means of surveillance. The so-called digital divide is not merely a matter of access to information. Information itself can be the means of creating divisions' (2003b: 2).

The terms 'categorical suspicion' (Marx 1988) and 'categorical seduction' (Lyon 2007) neatly capture the dynamics of political and economic surveillance in these cases. While the ends are different, the same philosophy underpins both; that people can be ordered, classified, profiled and managed in various ways. However, as a result of burgeoning data available about individuals and populations, the distinction between political and economic surveillance has become blurred. This is the same message Cohen (1985) stated with regards to post-social control.

A note on which to conclude this initial (and admittedly brief) foray into surveillance studies returns to an idea from Chapter One: the concept of 'visibility'. Visibility is a helpful tool for this research. It is also one that translates well across the changing landscape of surveillance studies. Foucault (1977) pointed towards the 'state of permanent visibility' imbued into prisoners in Bentham's Panopticon. The expansion of this disciplinary mode of power rendered wider sections of the population visible in other senses. As Marx (2002) suggested, surveillance has evolved from purely visual/sensory observation to more granular and context-based forms, based on the extraction and creation of information. This is a process amplified as ICTs have developed and infiltrated most aspects of our daily lives. Our shopping habits make us visible to commercial entities. The concurrent trend of volunteering large amounts of personal information in online spaces shows people making *themselves* visible, both to public and private bodies but also to friends, acquaintances and strangers. There can be elements of empowerment or performativity (Koskela 2004) in divulging information creatively or for different audiences but the overall effect is to contribute to a greater state of personal, social, political and economic visibility.

Visibility is revisited below, for as well as digital forms of surveillance we can also understand *resistance* to surveillance in terms of visibility.

3.3.2 A DIGITAL PANOPTICON?

Having laid out some of the prominent conceptualisations of contemporary digital surveillance, the next task is to examine the fit between these and the approaches to social control discussed earlier. To return to Lyon's (2001) definition of surveillance, we can immediately see parallels with the disciplinary perspective of Foucault; surveillance is about managing and influencing individuals and groups. However, there is a distinctly contemporary feel to Lyon's definition that perhaps extends beyond what Foucault suggested. 'Processing of personal data' speaks more of information flows characteristic of the information society. Moreover, if data do not need to be identifiable, there is a level of abstraction in surveillance; it suggests that a level of control can be achieved without having to connect knowledge to specific subjects. Detailed knowledge about individuals' habits and preferences garnered from surveillance of their online activity does not need to be attributed to a known individual. Instead, our actions online create digital 'doppelgangers' that are taken to be an accurate representation of us. To reiterate, the designation of *digital* surveillance throughout this thesis is intended to refer to those surveillance practices that have evolved and expanded in tandem with those of the information society described in Chapter Two.

Historically at least, surveillance has been understood as a top-down or one-way process. Foucault's (1977) study once again provides the classic example; a good deal of research and theorising about modern surveillance has been influenced by Foucault's panoptic metaphor, adapted from Bentham's (1791) classic design of a circular prison with a central watchtower[59]. The enduring tenet of Foucault's discussion is that the panopticon would induce in a subject 'a state of conscious and permanent visibility that assures the automatic functioning of power' (Foucault 1977: 201). As above, this technique was central to Foucault's conception of governmentality. To what extent the panopticon remains a helpful model for understanding the breadth of modern surveillance is, however, contested (see

[59] See McLaughlin and Muncie (2013: 16-22).

Deleuze 1992; Poster 1996; Bogard 2006; Latour 1998; Haggerty 2006). As Lyon (2003a: 4) suggests 'it is not clear that [models like the panopticon] are entirely helpful ways of understanding surveillance today.' Yet at the same time, Lyon (2006) also acknowledges that 'the panopticon refuses to go away.' It is an enduring theoretical model for understanding surveillance. At first glance, it is clear why this might be so in the information society. Robins and Webster for instance claim that information technologies are a logical extension of the panopticon because they 'monitor the activities, tastes and preferences of those who are networked…Power expresses itself as surveillance and Panopticism, now on the scale of society as a whole' (1999: 118, 122). Other authors, including Lyon (1994) and Poster (1990, 1996), have attempted to contemporise the lessons of the panopticon, proposing new frameworks such as the 'electronic panopticon' or 'superpanopticon' respectively. However the evolution of the information society is such that totalising models of the type to which Lyon (2003a) refers are indeed undesirable for capturing the complex dynamics of contemporary surveillance and, by extension, social control. To reiterate the position from Chapter One, the theoretical basis of this research is that Foucault's model for understanding surveillance requires rethinking in the information society. In its place a distributed, networked, nodal conception of surveillance (and resistance) is proposed.

There are, then, patterns of contemporary digital surveillance that challenge the utility of the panopticon as an analytical frame. Norris (2003) for example argues that while widespread CCTV use does bear many similarities to the panopticon, its increasing digitalisation serves to exclude individuals and groups, rather than include (normalise) them. Likewise the 'social sorting' (Lyon 2003b) capacities of contemporary surveillance necessitate more attention; the gearing of surveillance towards prediction, prevention and risk management through the use of interconnected, searchable databases represents a very different manifestation of surveillance.

Related to this is Haggerty and Ericson's (2000) 'surveillant assemblage'. This concept is immensely useful for the thesis as it ties together the patterns identified above in respect of nodal governance with the contemporary organisation of surveillance. It depicts contemporary surveillance as 'rhizomatic' – organised in an

expansive, horizontal, networked fashion, spread across the breadth of social institutions. For example CCTV, as described by Norris and Armstrong (1999), can be seen as an assemblage comprised of computers, people, telecommunications and cameras (Haggerty and Ericson 2000: 614). It goes further than the panopticon in one sense in that it extends the analysis of surveillance beyond a government 'project', incorporating a plurality of actors such as private entities into relationships of surveillance. It consequently extends it in another sense insofar as this necessitates a shift in thinking about surveillance in top-down terms, which coincides with patterns identified so far in the chapter. In the same way that the theory of nodal governance points towards the simultaneous competition and cooperation that can exist between governing entities, Haggerty and Ericson (2000) show how the surveillant assemblage comprises relationships that can either be ad hoc or more permanent. In addition, the rhizome[60] metaphor indicates the 'under the surface' quality of surveillance and, to an extent, unpredictability about how surveillance practices will emerge.

Other parallels with the theory of nodal governance emerge if we consider shifts in the governing *mentalities* of surveillance. Governing nodes can be equated with actors in the surveillant assemblage; each has a specific way of thinking about surveillance and the technologies and resources for doing it. The chapter has shown that contemporary surveillance is designed to meet many ends. As a result, new subjects are constituted, new classifications and categories found. Big data analytics, for instance, provide the means to extract new forms of data and knowledge at the level of whole populations (Housley *et al.* 2014). There is, therefore, a stretching beyond the boundaries of control that is designed to normalise deviants; powerful economic motives dictate the character of much digital surveillance. In these contexts, the applicability of Foucault's governing rationality of discipline is questionable. We could also think about the overt and covert nature of surveillance. For Foucault, surveillance was somewhere in the middle. Observation had to be seen as a possibility by subjects – so not completely covert – yet not so blatant as to be coercive; this would negate the aim of changing the subject's relation to him or herself. Today, there is little doubt: we are constantly

[60] A rhizome is an organic structure; a root system that links otherwise seemingly dispersed and disconnected plants.

being surveilled. Although we may be unaware to precisely what extent, particularly online, we accept it. As mentioned in Chapter Two, this is often for the sake of convenience, access to services or for reward and benefits.

Panopticism signals directionality in surveillance. For all it says about the dispersal into society of a particular logic of control, the panoptic metaphor is tied to a top-down conceptualisation of power: the few watch the many. Critiques – or perhaps more appropriately adaptations – of the Foucauldian reading of surveillance are not, however, limited only to highlighting the more fluid, nebulous character of surveillance and control in contemporary society. Mathiesen's (1997) exposition of the 'synopticon' was an attempt to rethink and invert panoptic principles in an age of new and expanding media. Using entertainment and news media as primary examples, Mathiesen argues that where the panopticon enabled the few to watch the many, the synopticon enables the many to watch the few. By this Mathiesen referred to the ways in which the public can observe the lives and actions of the powerful through a multiplying number of media channels. However, the synopticon, despite inverting the panoptic gaze, was not liberating but instead intensified the repressive aspects of surveillance. Mathiesen noted, pessimistically, that 'taken as a whole things are much worse than Foucault imagined' (1997: 231). Coleman (2013) reinforces this point. A persistent stream of media messages about how we should admire the ways of the powerful few is, he suggests, a way to keep us in thrall to control.

Although Mathiesen's argument is a necessary addition to thinking about surveillance in contemporary society – particularly given the importance this research places on new forms of media and communication – the inversion of the surveillance relationship is overly simplistic. While it is accurate that new media allow the public to observe the lives of the elite (politicians, celebrities and their ilk) the ability of the few to watch the many remains a potent counter-balance to this. Further critiques of Mathiesen's (1997) work also suggest he underplays the role of the Internet. Doyle (2011) for instance suggests that contemporary online media have expanded further and far more rapidly than Mathiesen's analysis can account for. An example of this is social media. The forms of 'lateral surveillance' (Andrejevic 2005) identified above arguably usher in a state where the 'many watch

the many'. New media, then, continue to produce new dynamics of surveillance. So too do they produce new dynamics of resistance: the synopticon is one concept used to inform the analysis presented in Chapter Seven of the potential of new media platforms to invert surveillance relationships.

There are conflicting tendencies in digital surveillance. There is hierarchy in surveillance (such as political and economic surveillance) but there is also horizontality; recall from Chapter Two the evidence of this in both technological and social terms. This antagonism is at the centre of the issues explored in this research. Not only is power dispersed throughout society into multiple centres, it is also dispersed rhizomatically across a breadth of actors who both enact and resist or subvert control practices. Herein lies another criticism often directed at Foucault's analysis, namely that he leaves no room for considering resistance against disciplinary power. Doyle (2011) makes the same criticism of Mathiesen's synopticon; media channels can challenge the status quo, not only reinforce it. Nevertheless, the post-structuralist influence on social control endures by alerting us to the dispersal of power throughout society. This decentred, multiple, fragmented character of control is what is taken forward in this research. Acknowledging such networked and diffuse power and control also means recognising that resistance to one or other practice of social control or surveillance may not be sufficient to dismantle the whole apparatus. With that in mind, the final theme of this discussion turns to accounts of surveillance and resistance.

3.3.3 SURVEILLANCE AND RESISTANCE

Resistance is a comparatively under-researched and under-theorised issue in the field of surveillance studies (Fernandez and Huey 2009). There are several studies that are important milestones in our thinking about the relationship between surveillance and resistance (see for example Gilliom 2001; Bennett 2008; Marx 2003; Mann *et al.* 2003), and empirical research into resistance has gathered pace (see Bell 2009; Introna and Gibbons 2009; Martin *et al.* 2009; Marx 2009; Sanchez 2009; Wells and Wills 2009) but overall there is still work to be done in developing a critical understanding of how, why, where and by whom surveillance is resisted. Examining some of the trends in the existing literature on resistance helps to signify the

connections with the theoretical stance adopted in this research. This thesis is, of course, also designed to continue developing an empirical and theoretical understanding of resistance and surveillance.

Marx (2003) outlines eleven[61] 'behavioural techniques of neutralization' by which surveillance technologies can be resisted. Broadly, these 'moves' involve deliberate detection, identification and evasion of surveillance technologies or practices, confrontation and (physical) retaliation against surveillance systems, confounding of the information displayed or given to surveillance systems, and inverting the surveillance gaze. The examples Marx provides are primarily of 'real world' surveillance practices, although there is some mention of electronic forms of economic surveillance – for instance refusing to comply with supermarket loyalty schemes. For that reason, the work of Dupont (2008) is also enlightening. Acknowledging Marx's earlier work, Dupont turns his attention to online examples of resistance to surveillance. In particular, cryptography and anonymous Internet browsing are discussed as digital versions of 'blocking' and 'masking' (Marx 2003). His useful update also serves as a critique of the way in which surveillance scholars have approached the issues of the panopticon and resistance to surveillance, in that they fail to fully account for the democratisation of surveillance technologies and the creative ways in which people can appropriate both surveillance tools and online technologies more broadly to counteract digital surveillance practices. However, the contributions of Marx (2003) and Dupont (2008) both tend toward individualised strategies of resistance. This thesis seeks to incorporate these empirical and theoretical contributions with an approach that recognises the plural, networked and diffuse nature of surveillance and resistance.

A problem already noted with the Foucauldian reading of contemporary surveillance is that it offers little space for resistance. It is a totalising system of control that denies agency to those who are surveilled. This limitation, Doyle (2011) argues, was replicated in Mathiesen's account of the synopticon. The ecosystem of new and online media platforms is much more complex than Mathiesen suggested (Doyle 2011) and this raises questions about how these media can both propagate

[61] Marx called these: discovery, avoidance, piggybacking, switching, distorting, blocking, masking, breaking, refusal, cooperative and counter-surveillance moves.

surveillance as well as amplify the potential for resistance online. Relatedly, the plurality of contemporary surveillance opens it up to new forms of resistance. It is logical that where there are multiple surveillance agents pursuing their own objectives, there will also be opportunities for surveillance to be resisted where these objectives clash. This is the case in Chapter Six where political and economic forms of surveillance are seen to be at odds with one another.

This situation also alerts us to the fact that in the context of digital surveillance, some of the most effective resistance can come from those who are simultaneously the most powerful surveillance agents. Martin *et al.* (2009) argue that the landscape of surveillance and resistance goes beyond the typical 'subject-agent' relationship and is instead 'multi-actor', signifying the complex web of governing nodes and mentalities discussed previously. This research employs a similar multi-actor framework for examining surveillance and resistance and this sits alongside the theory of nodal governance. In tandem, these point to the necessity of exploring surveillance and resistance across a variety of social settings. Reinforcing the point made earlier, both these perspectives challenge a binary conception of power where it is possessed by some and wielded against others. Sharp *et al.* (2000), by contrast, discuss 'dominant' and 'resisting' forms of power. In the information society, communication technologies empower both those who seek to control and those who resist.

Moves against surveillance can also be met with counter-moves designed to nullify resistance. Marx (2009) picked up on this dynamic in a later addition to his work on techniques of neutralisation. The relationship between surveillance and resistance, he suggests, is cyclical.

> 'Neutralization is a dynamic adversarial social dance involving strategic moves and counter-moves…Those in the surveillance business respond to neutralization efforts with their own innovations which are then responded to in a re-occurring pattern. Whether for agents or subjects, innovations may offer only temporary solutions' (Marx 2009: 299).

The same patterns of action and reaction are evident in the development and deployment of counter-terrorism initiatives (Innes and Levi 2012). This pattern is amplified given that digital and online forms of resistance can be seen as more flexible and mobile. In Chapter Seven, online media platforms like WikiLeaks are

discussed as an example of how the Internet has fostered a particularly resilient and adaptable form of resistance that counter-moves can only for a short time debilitate.

Another prominent way in which resistance to surveillance has been conceptualised is as 'sousveillance' (Mann *et al.* 2003). From the French 'sous' (meaning 'under') and opposed to 'sur' ('over') the term denotes offering panoptic technologies to individuals to allow them to invert the surveillance gaze of organisations. Practical examples of sousveillance include people wearing body cameras to record the activities of those in authority (such as police officers). Sousveillance signifies the relocation of the power to watch and observe with those typically subject to such practices. There is a degree of conceptual overlap between sousveillance and Mathiesen's (1997) synopticon insofar as both propose a situation in which 'the many watch the few'. However, there is a difference in focus. The former is concerned with technologically augmented strategies for openly challenging the hegemony of information flow from people to private companies or state agencies. The latter implicates news and entertainment media in the control apparatus through the communication of information designed to promote the goals of political or economic surveillance. While this would suggest the synopticon is not associated with resistance, Doyle's (2011) critique demonstrates how contemporary online media *do* allow for resistance as well as surveillance. Alternative news media outlets have proliferated online, carving out spaces for challenging dominant discourses (about crime control and surveillance for instance). An effect of this has been to encourage cultural shifts in trust in major social institutions (Doyle 2011).

Rather than trying to keep these two concepts separate we might usefully employ the broader term of '*resistive surveillance*'. This captures the dynamics of resistance in the information society neatly and avoids any confusion in trying to delineate what is synoptic surveillance and what is sousveillance. Resistive surveillance points to those contexts in which digital technologies are used to surveill the actions of those in authority – or 'watch the watchers' to paraphrase the old adage[62]. In other words to render these entities more *visible*. This is also in keeping with the idea discussed earlier that 'surveillance' implies a power dimension. In this case, 'resistive surveillance' would counteract 'political' or 'economic' surveillance. Each

[62] '*Quis custodiet ipsos custodies?*' is a Latin phrase meaning 'who will guard the guards?'

side of this coin would be described as exercising resisting or dominating power respectively (Sharp *et al.* 2000). Less overt strategies of resistive surveillance are seen in the actions of advocacy groups – the 'privacy advocates' (Bennett 2008) who aim to protect civil liberties and minimise intrusive surveillance. These groups also try to shine a light on those practices (including regulations, as seen in Chapter Six) that extend surveillance capacities or threaten privacy but they tend to do so through lobbying, campaigning and raising awareness rather than creative and adaptive appropriation of digital technologies. This global network of organisations is subject to analysis in Chapter Five.

Resistance to surveillance is multi-faceted. As well as more pervasive and diffuse surveillance, ICTs have allowed for new and resilient forms of resistance. The relationship between digital surveillance and resistance is dynamic, a process of moves and counter-moves. Resistance enlists a broad range of actors, some of whom may also engage in forms of surveillance that are resisted elsewhere. This is significant for the second research question of the thesis concerning motivations to resist. As we will see, resistance to surveillance is not only about the traditional counter-balance of privacy. Last, resistance can incorporate, perhaps through adaptation or innovation, the same tools and technologies that are used to surveill. A pertinent feature of resistance to digital surveillance, therefore, is that it re-appropriates the idea of visibility. Which brings us back to the first point (and one that underpins the thesis as a whole); the information society amplifies and intensifies both those practices that seek to enact and subvert control.

3.4 LESSONS FOR THE RESEARCH

The purpose of this chapter was to outline the contours in the literature on social control and surveillance. The themes that have been drawn out are those that are relevant for the research and that illustrate the parallels between the various strands of theories of control, surveillance and resistance. The one-directional modernist conception of power that is the basis of radical theories, while helpful for considering the powerful economic motives underlying many of the recent trends in social control, is inappropriate for the current context. More convincing (and certainly more relevant to the information society) is a pluralistic conception that

sees power as distributed across society. Moreover, power is not a negative phenomenon – a possession of a dominant group in society – it is a resource that flows between different groups and can thus take the form of 'dominating' or 'resisting' power (Sharp *et al.* 2000). Following Cohen's (1985) reimagining of Foucault's analysis, we see that control has drifted away from the state (albeit dispersed into various institutions) and into numerous other locales or governing nodes. Private organisations are prominent among these but added to this are other actors such as NGOs or media groups who increasingly play an active role in the negotiation of control. Deleuze's (1992) brief exposition of the 'control society' similarly argues for moving beyond Foucault's disciplinary society and is much more helpful for framing the dynamics and logics of contemporary control. Specifically, it places the computer at the centre of these shifts and acknowledges the impact technological advances of this kind have on individual members of society. This is likewise in keeping with Haggerty and Ericson's (2000) elaboration of the 'surveillant assemblage'[63], which prioritises networks, flows and flexibility in the constitution of the social control apparatus. Other contributions from the field of surveillance studies reflect this tension between the legacy of Foucault's panoptic metaphor and more diffuse forms of contemporary surveillance.

.. -.-. --- -- . ..-. .-. --- -- -.-. -.-- -... . .-. ... .--. .- -.-. . --..--

[63] This is, perhaps, to be expected as the concept of assemblages was borrowed from earlier work by Deleuze and Guattari (1987).

CHAPTER FOUR

STUDYING DIGITAL SURVEILLANCE AND RESISTANCE: A MIXED-METHOD/MULTI-STRATEGY APPROACH

4.1 INTRODUCTION

Researching surveillance raises many questions for social research. Surveillance is concerned with the gathering and processing of information about people. It is a practice of observing, extracting, categorising, influencing and managing. Let us forget the ends; above all, surveillance is ultimately about *knowing*. There is a unique relationship, and similarity, therefore, between surveillance and social research. Coupled with an investigation of *resistance* to surveillance, this raises some poignant issues for social researchers that are explored towards the end of this chapter. Aspects of the methods used here allow us to question the position of the researcher as a surveillance agent and alerts us to the ethical and political dimensions of the research tools that are used.

This chapter describes the research process, outlining the multi-strategy and multi-method design and implementation of each stage of the fieldwork. While some degree of description is necessary, the broader aim is to situate this within the context of studying (digital) surveillance, resistance and social control. The focus on these phenomena in an *online* context at times necessitated, and was accompanied by an enthusiasm for Internet-based research methods. Consequently, contained within this chapter are commentaries on the exploratory and online aspects of the methodology that was employed as well as reflections on the usefulness of these and the obstacles that they presented. The research is also placed in the context of the current growth of digital and computational social science research methods. The design of this research was not fixed from the outset. Quite the opposite; it was at times opportunistic and responsive and was constructed above all in order to

support the theoretical motivations of the thesis and to be reflective of the dynamic and myriad configurations of surveillance and resistance. Consequently, there was diverse methodology that this chapter aims to clarify and justify.

4.2 THE APPROACH TO THE FIELDWORK

Fieldwork for this thesis was constructed in three parts, designed to explore each of the three settings identified in Chapter Two as constituting the landscape of digital surveillance and resistance: civil society, regulation and media. The research design for the fieldwork, therefore, took the form of three distinct yet related case studies. Each of the cases utilised different methods and different data. As outlined in Chapter One, the first case examined the online social organisation of resistance, using network analysis techniques (section 4.3). The second was concerned with the legal frameworks that seek to regulate surveillance and that generate effects of resistance, using content analysis of these documents (section 4.4). The final case explored media presentation of surveillance and resistance focusing on coverage of WikiLeaks and Edward Snowden, using a combination of quantitative content analysis and qualitative interviewing (section 4.5).

The choice of method was guided by the question of what data could shed light on the contribution of each sphere to the current landscape of surveillance and resistance and, more broadly, the nature of contemporary social control. Each of the three sites contributed to a rolling narrative that informed a response to each of the research questions. At the same time, Chapters Six and Seven (regulation and the media respectively) are based on data that engages more with research question two. To reiterate these research questions: how are digital surveillance and resistance related?; why do individuals and groups who resist surveillance identify a need for doing so?, and; what are the implications of these patterns for our understanding of control in the information society?

While each of the cases had the potential to form the basis of a much more in-depth study, the guiding rationale for the eclectic yet innovative research design was to unpack the variety of influences that shape the relationship between digital surveillance and resistance:

> 'Empirical cases, studied in depth…lead us to important social processes and the details of social organization that produce them' (Becker 2014: 5).

Case studies commonly face the criticism of being unable to speak to social processes and practices beyond the case in question (see Hammersley 2004). However, Becker's (2014) guidance on case studies is continually enlightening in that regard. He advocates that case studies should raise more questions than they answer:

> '…my work doesn't produce timeless generalizations about relations between variables. It results instead in the identification of new elements of a situation, new things that can vary in ways that will affect the outcome I'm interested in…I can use these new elements of organisation to direct my next inquiry' (2014: 3).

It would have been possible here, for example, to conduct a highly detailed analysis of one instance of the 'regulation of surveillance' or of the social and technological impact of WikiLeaks[64]. Yet this would have failed to account for the concurrent and shifting social processes unfolding alongside and playing an equal role in shaping the landscape of online control. Crucially, Becker tells us that 'everything present in or connected to a situation [we] want to understand should be taken account of and made use of' (2014: 3).

The overall approach to the fieldwork can be described, therefore, as both 'multi-strategy' (Layder 1993; Bryman 2004) and 'multi-method' (Bryman 2004a). Although some authors use these terms interchangeably (see Cresswell 2008) in this context the former indicates the combination of quantitative and qualitative strategies that were employed, while the latter describes the variety of (primarily) qualitative methods used throughout the research. Naturally, this raises questions of the epistemological orientation of the study. The principles of quantitative and qualitative strategies are not incompatible. This research subscribed to a 'technical version' (Bryman 2004: 454) of the divide between the two strategies; that they are capable of being fused in pursuit of a research agenda and that this benefits the research process. In Hammersley's (1996) terms, the justification for this is one of 'complementarity' as opposed to triangulation. The use of different strategies was not intended to corroborate or validate other findings from the research. Rather, it

[64] Chapters Six and Seven respectively.

was designed to comprehensively reflect and illustrate the diverse, complex and overlapping nature of modern digital surveillance.

At the same time, the quantitative aspects to the study (primarily those in Chapter Five) require some definition. The methods used contribute to and contemporise the debate about the compatibility of quantitative and qualitative strategies. The quantitative elements of the study fall under the category of computational social science research methods. This nascent field of social research aims to respond to the burgeoning of data available online ('Big Data') as a result of social changes in communication and interaction. It seeks to harness the potential of these changes to enhance social research (Ackland and Gibson 2013; Burnap *et al.* 2013, Dutton 2013; Edwards *et al.* 2013; Procter *et al.* 2013; Sloan *et al.* 2013) and respond to what Savage and Burrows (2007) have called the 'coming crisis of empirical sociology'. Traditional research methods such as surveys and interviews have already successfully migrated to virtual environments. Rogers (2009) however, is among those who suggest that we are currently witnessing the emergence of *digital* methods as opposed to *virtual*. The former are grounded in the realm of the Internet; they are, like the next generation of Internet users, *natively digital.* Hyperlink or tag analysis, exploiting search engines, data mining from social media all represent a new approach to studying society as it is expressed on the Internet. New forms of social interaction have laid the foundations for new forms of social research. Of course, this is not limited to social media as it is understood in terms of Facebook and Twitter (although these are at the heart of it); it is rather that social media use is indicative of a broader social change in the way in which we interact with each other and how the Internet is used. Edwards *et al.* (2013), for instance, point us to the change from the informational web (Web 1.0) to the socially generated web (Web 2.0); interaction online generates new forms of data and is thus to be investigated in new ways.

Computational methods that allow for the investigation of emergent forms of social organisation and interaction in online spaces are thus comparable with 'traditional' quantitative methods that aim to capture macro social processes, albeit in a static

fashion[65]. Computational social science research tools allow for the collection of data that simultaneously describes large-scale social organisation as it occurs online but also micro processes of interpersonal interaction. There is an inherent fusing, therefore, of qualitative and quantitative principles in this approach. Moreover, although these tools were used in only one of the research 'sites' (see Chapter Five) they reinforce the overlap between social research and the surveillance that is the subject of this thesis. As Lyon notes, we should seek to understand the '*capacities* of Big Data and their social-political *consequences*' (2014: 2, *emphasis* in original).

While each of the three research sites/cases were examined using different methods, these were supplemented with a short series of semi-structured qualitative interviews that spanned the three sites. These interviews targeted a variety of individuals who were identified for their expertise in the area of digital communication, activism, privacy and policy. They also represented the diversity of issues that interact to construct the modern environment of digital surveillance and resistance. Bespoke interview guides were created for each participant (or pair of participants in two cases[66]) that were designed to tap into their areas of expertise – Internet activism, digital rights, policy or specific technologies for instance. These 'conversations with a purpose' (Burgess 1984: 102) were consequently flexible and fluid and permitted probing based on insights gained from other data collection being carried out simultaneously. The interview guides also aimed to tap into general themes regarding perceptions of online surveillance and regulation. Each interview was designed to last approximately 45 minutes, an intentional decision, as contacting and recruiting potential participants in some cases required attempts to make the research appeal to very busy individuals (politicians and lawyers being two examples). The flexibility of the interview guides meant that on occasion the interviews lasted much longer than planned – to neither the concern of participant or researcher.

The selection of participants was not designed to be representative; rather, they were identified as holding specific knowledge or experience that would be useful for

[65] See Chapter Four (section 4.3) for a more detailed discussion of the benefits and contributions of computational social science research methods.
[66] Two academic researchers at the Oxford Internet Institute were interviewed together, as were two employees at the Government Digital Service.

the research. Nine interviews[67] were conducted in total and the data generated informed initial analysis across each of the three fieldwork sites.

- Eric King – Head of Research, Privacy International
- Pete Bradwell – Policy Director, Open Rights Group
- Dr Joss Wright – Oxford Internet Institute
- Dr Anne-Marie Oostveen – Oxford Internet Institute
- Trefor Davies – Chief Technology Officer, Timico
- Smári McCarthy – information activist
- Daniel Domscheit-Berg – OpenLeaks founder, former WikiLeaks spokesman
- 'Bert' – Government Digital Service
- 'Ernie' – Government Digital Service

Contact with these participants was established via email. In some cases this was a direct email to a potential participant identified as holding specific expertise. In other cases participants were recommended after making contact with a gatekeeper at an organisation. Initially, these interviews were designed as an adjunct to the other aspects of the fieldwork. However, it quickly became apparent that the contributions of the interviewees offered valuable insight into the research and provided several entry-points that directed analysis of the other data. Issues relating to these interviews are discussed later, particularly as regards access in the case of Daniel and WikiLeaks. There were some refusals to participate and other cases where contact with potential participants dried up before interviews could be scheduled[68]. As above, in both cases of failed recruitment, this was due to respondents' time commitments. Before the chapter moves on to examine the specificities of each research site, there are some necessary observations to make regarding the role of the Internet in this research.

[67] Seven of the nine interviewees agreed to their names being used in the research. In addition, all participants in the interviews consented either verbally (on record) or in writing to the conditions of the research set out in the 'Information for Research Participants' (see Appendix B)

[68] Three instances included the Director of a UK-based anti-surveillance campaign group, an MP from Iceland involved in the 'Modern Media Initiative' and a solicitor representing a coalition of advocacy groups at the European Court.

4.2.1 THE INTERNET: OBJECT AND MEDIUM

Having always held an interest in online research methods, it was an easy decision to engage them in pursuit of this research agenda. Previous research experience had demonstrated their use in facilitating traditional forms of research (such as conducting qualitative interviews by Skype or email) as well as allowing for innovative means of exploring social phenomena. At the same time, with the Internet as the object of study, online research methods were considered at times a necessity. In much the same way as ethnography developed as a method for studying social life in its natural context, an investigation of digital surveillance and resistance *had* to be situated – at least in part – online.

It becomes clear at this stage that the Internet occupies a dual position in this thesis as both an *object* and *medium* for research, which connects to the relationship already identified between surveillance studies and social science research. So too is this a product of the wider story of the thesis – technological development creating new relations and causing societal-level changes. Naturally, this impacts on social research; as Fischer *et al.* have noted, 'opportunities for social scientists will be driven both by changes in societies and advances in our research methods' (2008: 519). This highlights the fundamental link between theory and method. While the Internet opens up new possibilities for exploring social phenomena, it also necessitates theorisation of the new forms of social organisation and interaction that occur as a result.

The question of the nature of virtual spaces compared to 'real world' spaces has informed methodological debates as well as theoretical ones. This distinction is also keenly felt in the context of surveillance studies and other areas concerned with communication media (for example Meyrowitz 1985). New technologies blur the boundary between digital and physical spaces. Acknowledging this, the research followed in footsteps of social researchers who have framed digital and physical spaces as overlapping and inseparable (see Lyman and Wakeford 1999; Ruhleder 2000). Whereas some authors advocate a view of the two as separate environments for research (Hine 2000; Lysloff 2003) others, such as Garcia *et al.* (2009) argue that:

> '…there is one social world which contains both traditional and technologically advanced modes of communication and sites of social activity…"Virtual reality" is not a reality separate from other aspects of human action and experience, but rather a part of it. Therefore, ethnographers should define the field or setting of their research on the basis of their research topic, rather than arbitrarily or prematurely excluding one arena or the other.' (Garcia *et al.* 2009: 54)

This research was not ethnographic but the argument remains applicable. Surveillance is a phenomenon that is increasingly framed in digital terms but it cannot be divorced from its real world implications or facets – such as protest events or regulatory processes that shape it. The methods adopted in this study aimed to capture this character of surveillance by examining both online and offline processes so as to more rigorously theorise social control as it transverses the digital and the physical.

Online research methods, much like traditional methods, fall into two categories. 'Internet-mediated research' (Hewson *et al.* 2003) – also referred to as primary Internet research (Hewson and Laurent 2008) – involves the collection of novel or original data. Secondary Internet research on the other hand is defined as 'techniques and procedures for locating and accessing bibliographic materials online' (Hewson and Laurent 2008: 58), which thereby encompasses the collection of news reports, official documents and other forms of secondary data (see sections 4.4 and 4.5). The fieldwork for this research involved both primary and secondary methods. The former can be subdivided into two further categories, which can be called *Internet-facilitated* and *Internet-targeted* research.

The Internet-facilitated component of the fieldwork involved the use of Skype to carry out the qualitative interviews. As a research tool, Skype has the same methodological and practical benefits of telephone interviewing, such as allowing for synchronous communication[69] and saving on time and cost of travel (see O'Connor *et al.* 2008; Holt 2010). However, whereas telephone interviews lack the ability to pick up on contextual indicators present in face-to-face interviewing (see Evans *et al.* 2008), Skype's video functionality overcomes this. Of course, this is only applicable when both parties have webcams; of the nine interviews conducted during the fieldwork, five were carried out via Skype and of these three were video-enabled.

[69] As compared, for instance, to email interviews which are asynchronous.

The argument that Skype represents the best alternative to face-to-face interviews (Hanna 2012) is accurate, although only when accompanied by video. In some cases (even without video) it is actually preferable as recruiting participants from overseas (such as Daniel and Smári in this research) is a more feasible possibility (see Sedgwick and Spiers 2009). Skype is by no means flawless and some of the pitfalls identified by King and Horrocks (2010: 84-5) were experienced during the research; bandwidth limitations resulted in poor sound quality and one interview cut out part way through (a connection was later re-established). An important lesson was also learned early on. In a bid to preserve the face-to-face benefits of the interview, an attempt was made to record both audio *and* video with QuickTime. It was only afterwards that the poor sound quality during the interview was attributed to the increased processing capacity this placed on the computer. Consequently, transcription was difficult and at times impossible.

Internet-targeted research refers to the computational methods that were employed. These differ from Internet-facilitated methods as both the object and medium of research is based online. In this case, the objects were communities and networks constituted online in both hyperlink and social media environments. These are outlined in more detail in the following section and the data they generated form the basis of Chapter Five. However, for now, Fielding and Lee observe that:

> 'Emergent technologies enable new modes of research, new approaches to analysis, and new relationships between social research and society. Moreover, the emergence of a pervasive computational environment offers a new subject for social science inquiry, raising issues relating to the social shaping of technologies and the role that technology has in shaping society and social relations' (2008: 491).

The inference here is that understanding the mutual relationship between technology and society requires new forms of social research. However, care needs to be taken in applying these methods as with any novel form of research. 'The newness of a method can lead to unthinking application and a distancing of users from the craft aspects of a particular methodological approach' (Lee *et al.* 2008: 6). In the same vein, Hine (2005) has discussed how the hype surrounding novel, online methodological developments can lead to their indiscriminate use. This returns to my earlier point; care was taken throughout to ensure that the methods employed

were appropriate for the subject/case in question. Rather than novelty for novelty's sake, using computational methods was an exploration of the potential of new forms of research to shed light on the relationship between technology and society as much as it was an investigation of that relationship.

A final point regarding this research returns to the link with surveillance studies. Throughout the research, as a result of increased exposure and curiosity, I developed an interest in the 'tools of the trade' of both surveillance *and* resistance. Specifically, privacy-preserving software such as the Tor system that permits anonymous Web browsing and allows access to the 'Dark Web'. Such software is used by privacy advocacy organisations and activists around the world in order to maintain secure and confidential communications. These tools raise fascinating and as yet largely unexplored possibilities for social research (for some early examples see Chen *et al.* 2008; Chen 2012 and Gehl 2014) and surveillance studies. The Dark Web can provide access to very hard to reach populations but at the same time, it poses numerous ethical issues. Chief amongst these is the fact that users of the Dark Web are unlikely to want to be found online, let alone talk with researchers. Safety would also be a concern, given that the Dark Web masks a lot of criminal activity including the drug trade and illegal pornography. Nevertheless, given what has already been said about the Internet as an object and a medium and the need to continually adapt and expand our theoretical and methodological resources in line with technological development, the potential should not be overlooked. This research agenda is reconsidered in the conclusion to this thesis.

4.3 CHARTING THE TERRAIN: MAPS AND METRICS

The remainder of this chapter deals in turn with the three research sites: online civil society, regulation and media respectively. The first of these was concerned with the social organisation of resistance: identifying the key actors and their inter-relationships online, describing the characteristics of their network and how these changed over time. A theory of nodal governance was used to analyse these patterns from the data that were gathered, as will be seen here. Some attention was also paid to the extent to which physical geography was reflected in these virtual spaces and the implications of this for understanding resistance to digital

surveillance. The following discussion outlines and evaluates a toolkit for investigating online interactions between those who resist surveillance. Social network analysis (SNA) concepts also help describe how these interactions were interpreted. First of all, however, we can consider the benefits of visualisation of data that computational methods bring with them.

For mapping out the online community of groups that resist surveillance, Dodge and Kitchin's insights from the *Atlas of Cyberspace* provided a good deal of inspiration:

> 'Cartography provides a means by which to classify, represent and communicate information about areas that are too large and too complex to be seen directly. Well-designed maps are relatively easy to interpret, and they constitute concentrated databases of information about the location, shape and size of key features of a landscape and the connections between them…In essence, maps and spatializations exploit the mind's ability to more readily see complex relationships in images, providing a clear understanding of a phenomenon, reducing search time, and revealing relationships that may otherwise not have been noticed' (2008: 2).

These comments also speak to the utility of computational methods as a whole; extracting value and meaning from quantities of new transactional data that would hitherto have been impossible to collect and store, let alone analyse. Mapping techniques and visualisation of data, then, are vital aspects of computational methods. So too do they emphasise the blend of quantitative and qualitative principles present in this approach. Data visualisations are not only graphic outputs of research – like charts and plots – they are representations, in this case, of forms of organisation and interaction. Consequently, they are amenable to interpretation; they are data in their own right as opposed to being merely a product of data.

Recent commentaries on the growth of computational social science (for example Edwards *et al.* 2013; Housley *et al.* 2014) situate it within the 'conventional' pursuits of social science research. They also help to illustrate the value of these methods for this stage of the research. For Housley *et al.*, 'big and broad social data' open the possibility of 'studying social processes as they unfold at the level of populations' (2014: 4). The implication here concerns change (in social relations or structures) over time and the ability to capture this on a broad scale using emergent computational methods (what Edwards *et al.* (2013) refer to as locomotive and extensive research). Given the rapidity of technological (and hence social) change, being able to capture 'real-time' data is crucial for social scientists.

The presentation of visualised online networks was also crucial for developing an empirical application of the theory of nodal governance. In simple terms, the language of nodes and networks complement one another readily. Demonstrating and explaining the existence of communities and sub-communities, whether they are transient or permanent, is a core component of theories of nodal governance. The methodological approach used in this case study was thus well suited to the task in hand. The arguments in Chapter Five illuminate these points in more detail.

4.3.1 ISSUE CRAWLER

The starting point for this stage of the research was deciding how to examine the existence of an online community and subsequently identify appropriate tools for the mapping task. Adapting earlier work by Introna and Gibbons (2009), the decision was taken in the first instance to use web crawling software – automated programs ('bots') that find, index and download web pages – to examine the network of organisations that oppose various forms of surveillance (whom Bennett (2008) refers to as 'privacy advocates'). The main aim was to retrieve data on how organisations' websites linked to one another via hyperlinks. The rationale being that mapping out the network according to their linking practices could illustrate the availability and potential flow of counter-surveillance information across this network. Bennett's (2008) concept of 'information politics' as a modality for resisting surveillance – speaking truth to power, getting information to the people and places where it can have the greatest impact – suggests that a cohesive hyperlink network could improve the ability of advocacy organisations to resist surveillance by more effective transmission of information about surveillance to web users (i.e. the public).

For this research, web crawling software *Issue Crawler*[70] was used. Once supplied with an initial list of websites ('starting points') to crawl, *Issue Crawler* searches these websites for links to other pages. If two or more links are found to the same site from different webpages, this then becomes a new node in the network and is subsequently crawled. This process continues until the network is exhausted. The

[70] https://www.issuecrawler.net/

top 100 most linked-to websites are then used to visualise the network, using *Issue Crawler's* own software.

Starting points were determined by drawing on and refining earlier findings (Introna and Gibbons 2009). A list was first compiled of the ten most prominent actors in the network from 2008[71] and supplemented this with organisations known about from personal experience. A crawl was launched using these websites and the most prominent actors were noted. This process was repeated. Given the breadth of organisations that were returned from these initial crawls – including 55 prominent advocacy and technical organisations – ten starting points were distilled from those initially identified[72]. This process allowed a degree of confidence that the networks gathered were comprehensive.

Practically, *Issue Crawler* offers several benefits. It is automatic, so requires little attention and crawls can be scheduled to repeat for a pre-determined length of time and at regular intervals (e.g. hourly, daily, weekly). There is also flexibility in how the crawls are carried out and instruction on calibration. Crawl depth (the number of pages 'down' into a website the crawler will search) and iterations (the number of times a site is crawled in one search) are two such examples. The settings chosen were the best suited to mapping the network for the purposes of illustrating the potential for information politics, such as crawling by *page* rather than *site* (the latter of which would only search homepages and thus would be likely to miss content containing links to other organisations). Most importantly, crawls were scheduled *weekly* for a period of three months in line with principles discussed above of observing change over time. Given that an aim was to observe any impact on the network of surveillance-related news or events, weekly intervals seemed the most appropriate length of time to capture this. More regular crawls were avoided for ethical reasons (see Thelwall and Stuart 2006); although unlikely in a case of individual use such as this, there is a possibility of web crawlers placing burdens on target websites' servers and thus increasing their costs.

[71] A related rationale for this stage of the research was to update previous findings. A gap of four years is a significant time for online networks to change in constitution and structure. Also, as described in Chapter Five, new organisations had emerged in 2012 that did not exist in 2008.
[72] See Appendix C.

Another benefit of *Issue Crawler* is the built-in visualisation tool. Once crawls were completed, networks could be viewed online and saved in a variety of formats. *Issue Crawler's* visualisations were easy to understand and clearly laid out and hence were used directly in the analysis[73]. However, despite some flexibility in presentation, *Issue Crawler* offers little in the way of detailed explanation as to how networks were constructed. On reflection, while a hindrance, this was part of the learning process of using such software for SNA and allowed me to develop sound interpretive skills. As a result, the next step to refine the analysis of these networks was to export the data to an interactive visualisation platform – *Gephi*[74] – that permitted a much greater degree of exploration of various network metrics.

4.3.2 GEPHI AND NETWORK METRICS

A key task for the analysis of the hyperlink networks was to identify the most prominent actors in the community. *Issue Crawler* permitted only superficial insight into this. *Gephi* by contrast allowed much greater freedom to manipulate the networks and subject the data to various layouts and calculations, including weighting the edges between nodes to show higher frequency of linking. Specifically, three measures of centrality (i.e. importance) of a node in the network were selected from the toolkit of SNA. Each of these measured importance in a different way and thus allowed for different interpretations of the network.

DEGREE CENTRALITY

Degree refers to the number of unique edges connected to a node in a network. In a 'directed' network (such as a hyperlink network) where edges travel in a specific direction between nodes, in-degree refers to links received and out-degree refers to links sent. These are the simplest ways of ranking importance. *Issue Crawler* was capable of visualising the network according to either in-degree or degree but that was the extent of its capacities. While it was interesting to note those actors in the networks with the highest in-degree, other measures of centrality provided more robust indicators of importance.

EIGENVECTOR CENTRALITY

[73] See Chapter Five for examples.
[74] https://gephi.github.io/

Eigenvector centrality takes into account not only the degree of a node but also the degree of all those nodes directing to it. It is thus a measure of centrality that takes into account all the 'attention' that is being given – directly or indirectly – to an actor in the network. Measuring actors by Eigenvector centrality revealed those organisations that 'are paid attention to by lots of others, who are *themselves* paid attention to by lots of others' (Hansen *et al.* 2011: 150, *emphasis in original*). Moreover, it is of benefit to a network such as one of information politics to expand and draw in more actors. Being connected to a node ranked highly for Eigenvector centrality is an effective way to increase the visibility of an otherwise peripheral network actor. In SNA terminology this is referred to as 'positive network externality'.

BETWEENNESS CENTRALITY

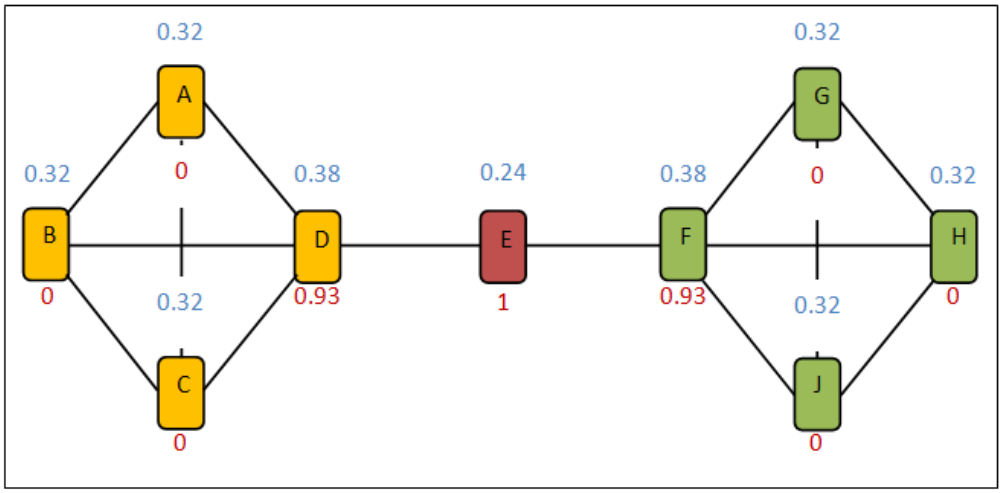
Betweenness centrality is linked to the idea of network 'bridges' or connections between clusters of nodes. It is a measure of how an actor's position in the network affects their access to non-redundant information. Ranking highly for Betweenness centrality means that the node is important for the transmission of information across the network. This was a helpful metric for the research as it conveyed a sense of which actors were important for ensuring dispersed nodes in the network could access information in other places.

Figure 1[75] illustrates these points. The Eigenvector centrality values are listed above each node, in blue, and Betweenness centrality values below, in red. The closer to 1, the higher the ranking. Nodes D and F are most important according to Eigenvector centrality while Node E is in the most advantageous position as a crucial bridge[76].

[75] Adapted from Hansen *et al.* (2011: 150)

[76] It should be noted that this diagram is *undirected*; it assumes information is flowing in either direction between nodes. As mentioned, the benefit of examining a hyperlink ecosystem is that it is *directed*; we can observe the flow of information from one actor to another.

FIGURE 1: EIGENVECTOR AND BETWEENNESS CENTRALITY



The question was whether to be concerned with Internet users navigating the advocacy network online or the benefits for the advocates themselves (such as websites being visited more often, support generated for their organisation). In the context of information politics, it is probably a case of the former. Acting solely out of self-interest is unlikely to achieve the goals of the organisation. At the heart of this is a concern with the *meaning* of a hyperlink, which I return to momentarily.

4.3.3 NODEXL AND SOCIAL MEDIA

The final piece of software used during the course of this stage of the research was *NodeXL*[77]. The decision to engage this software came after analysis of the networks produced by *Issue Crawler* highlighted the prominence of micro-blogging, social media website Twitter (see Chapter Five). *NodeXL* both retrieves data from the Internet (primarily social media) and visualises it via Microsoft Excel. For instance, it was possible to quickly retrieve the entire friends/followers network of any given Twitter account or any tweets, replies and retweets containing a given 'hashtag' over a period of time. Crawl depths could be set to retrieve only friends/followers of one user or extended to subsequently capture second and third degree networks (i.e. friends of friends and so on). There was a greater degree of freedom to manipulate visualisations than with *Issue Crawler,* as centrality metrics could be implemented, however, the platform was not as powerful in this respect as *Gephi*.

[77] https://nodexl.codeplex.com/

Similar to the ethical considerations highlighted by Thelwall and Stuart (2006) there were also limitations placed on the amount of data that could be requested at one time owing to the restrictions put in place on such requests by Twitter.

For that reason it was impossible, despite several attempts, to generate a social network for WikiLeaks (who were of particular interest to me) as their number of followers – at the time in excess of one million – was too large to be processed without waiting an impractical length of time. This limited the examination to Twitter accounts with approximately 1,000 followers. UK-based campaign group No2ID fell into this category and thus *NodeXL* was used to examine their social network and categorise their followers[78]. Methodologically, there was also an element of triangulation to this process, allowing for reflection on whether characteristics of the social networks of advocacy organisations were similar to those of the hyperlink networks. It also produced a more granular picture of the community; the hyperlink networks primarily captured organisations who had a website presence. Using *NodeXL* allowed me to complement this with an understanding of how individuals constituted and interacted with the network.

4.3.4 REFLECTIONS ON SOCIAL NETWORK ANALYSIS

Overall, the network analysis component of the fieldwork was instructive and a useful entry-point to the study. As Dodge and Kitchin (2005) note, the appeal of this approach to data collection and analysis was its fit with theories of nodal governance that guided the research. As Chapter Five goes on to show, there was much that could be taken from the network analysis in respect of understanding governance in the context of surveillance and resistance. This stage of the fieldwork built helpfully on earlier work identified (see Introna and Gibbons 2009). In particular, the use of different platforms for network manipulation and analysis allowed for a multi-layered perspective of communities organised around issues of surveillance. The further development of computational social science research methods will assist greatly in shedding more light on these relations. Towards the end of this stage of the research, a beta-version of the Collaborative Online Social

[78] See Chapter Five.

Media Observatory (COSMOS) platform[79] was trialled, which provided similar functions to *NodeXL* but with the added benefits of harvesting tweets in real-time and allowing for frequency and geo-spatial analysis. While this could construct networks of Twitter conversations relating to Snowden and the National Security Agency, the analysis at that stage was not sufficiently robust to merit inclusion in the thesis. Nevertheless, it is an avenue that can certainly develop our understanding of the response of publics to surveillance-related issues and the ways in which resistance is constructed amongst networks of advocacy organisations.

One particular methodological point to consider concerns the feasibility of examining resistance by looking at hyperlink networks. Underpinning the construction of these networks is the assumption that a hyperlink has a *meaning*. That by directing to another website, this signals an endorsement of some kind of the target organisation. The fact that the majority of organisations appearing in the networks were 'privacy advocates' of one kind or another does support the assumption that linking practices support the building of a community that has a common interest or purpose – to facilitate the transmission of information about harmful surveillance practices and to mobilise support. However, it should also be acknowledged that at times hyperlinks may, either, not be 'intended' to achieve a particular goal or may direct to information that is not 'counter-surveillance' in nature. An example of the latter would be directing to the website of a government organisation responsible for a certain form of surveillance. In this case, the hyperlink is not an endorsement. We should understand the resulting network, therefore, not as one of mutual support and necessarily 'anti-surveillance' in nature but as one where information about surveillance is made accessible, awareness is raised and – it is to be hoped – acted upon.

From a methodological standpoint the question concerns validity of measurement. Rogers' (2009) dilemma is instructive in this respect: how can we study social media and learn something about society rather than about social media use? The value of this insight is not limited to the study of social media. We can extend this problem to ask how we can study interaction on the Internet and learn something about society rather than about Internet behaviour (i.e. hyperlinking practices). Chapter

[79] http://www.cs.cf.ac.uk/cosmos/

Five is designed to remind the reader of this. It emphasises that the divide between offline and online social relations is not concrete. Bearing in mind what has already been said about computational methods, a key task of the chapter is to examine change in the networks over time and also how real-world events (such as media reports) impact on the network. By studying interaction online, therefore, we *are* learning about society. The triangulation of data described here helps flesh out the claims made about interaction and organisation. At the same time computational social science allows us to engage with Rogers' (2009) question by observing large-scale social processes in near real-time.

4.4 DOCUMENTARY ANALYSIS: REGULATION AND RESISTANCE

This section describes the next stage of research that was undertaken. This concerned introducing digital surveillance into the narrative and also served the purpose of 'seeing in action' several of the actors identified during the mapping exercise outlined above. As a result of a particular opportunity presented at the time, the fieldwork focused on the (attempted) enactment of regulation of digital surveillance practices. 'Attempted' is the key word in this instance; the theoretical motivation behind this part of the fieldwork was to gain an appreciation of how legal frameworks have sought to regulate surveillance and how these have generated effects of resistance. As the analysis progressed, it became clear that what was being uncovered in particular was the relationship between the state and private sector in constructing digital surveillance. The regulatory instrument in question was the UK Draft Communications Data Bill (CDB) from 2012. Over a period of approximately five months, a pre-legislative consultation process was undertaken by a Joint Committee to elicit attitudes and opinions from both experts and lay people towards the proposed regulation. All written and oral evidence submitted as part of this process was made available for public consumption (including the text of the Bill and the final report of the Joint Committee) and it was this that constituted the data for the case.

There have been many discussions concerning the utility of documentary analysis for empirical social science that are applicable to this research. Documentary analysis, some have pointed out, has suffered from accusations of inferiority when compared

to 'rich' observational or interview data or lack of neutrality (Coffey and Atkinson 2004; May 2011). Coffey and Atkinson say documents are not 'transparent representations of organisational routines [or] decision making processes' (2004: 58). However the CDB consultation as a 'sedimentation of social practices' (May 2011: 191) challenged that in some respect as it was part of a wider process of deliberation, evidence-gathering, opinion-seeking and, ultimately, rejection of the decision to implement a new regulatory structure for digital surveillance. Coffey and Atkinson's position that documents are not 'surrogates' for other sorts of data (2004: 58) was acknowledged here and thus interviews conducted at the same time aimed to further explore opinions of the CDB to corroborate the findings from the documentary analysis.

The consultation on the CDB fitted into the wider arena of crime prevention and counter-terrorist policy; the changes it proposed to the surveillance regime of communications data in the UK were primarily about managing the risk posed by organised criminals, cybercrime and terrorism. Documentary analysis can provide a useful window into such shifts in policy (Noaks and Wincup 2004). Particularly given its eventual rejection – and from 2014-2015 other significant changes in national and supra-national communications data retention legislation[80] – documentary analysis of the consultation process on the CDB provided valuable insight into the dynamic and rapidly evolving area of surveillance regulation.

Methodologically, the CDB presented several issues regarding documentary analysis. First is the nature of the design. There were elements of the research that could be described as a unique case study (Yin 1984); consultation processes on legislation of the depth demonstrated by the CDB are infrequent and there had been no similar attempts to rigorously elicit the attitudes of the public, experts and governmental officials towards surveillance regulation[81]. Previous research (for example Akdeniz *et al.* 2001) has examined the implications of surveillance-focused regulation but has not systematically analysed the process of its creation in the same way as the CDB allowed – and nor have the circumstances arisen to do so. However, situated within the broader work of thesis, the approach to the CDB is perhaps best described as an

[80] See Chapter Six.
[81] The Draft Investigatory Powers Bill (2015) underwent a similar consultation process.

exemplifying case (Bryman 2004); the CDB was simply a suitable context to examine the rationale behind the regulation of surveillance and resistance to it, albeit a highly opportune one.

Noaks and Wincup (2004: 117) emphasise the need for 'reflexivity and methodological rigour' in approaching documents as sources of data. Given the use of the CDB as one specific instance of negotiation of surveillance, reflexivity was not a primary concern insofar as Noaks and Wincup mean to refer to the relevance of a *variety* of documents. In a broader sense, however, the consultation documents were a satisfactory and appropriate reflection of the process of regulating and resisting surveillance. Scott's (1990) four criteria for assessing documents – authenticity, credibility, representativeness and meaning – were also instructive. The origin and nature of the documents (i.e. their use as formal evidence by the Joint Committee) validated and gave value to the documents as a source of evidence. Only infrequently was the evidence incomplete, where some oral submissions were redacted during transcription for confidentiality reasons on the part of witnesses. Scott (1990: 35) advocates constant reappraisal of the quality of documents and acknowledges the variety of problems researchers will encounter in dealing with them. A number of methodological and analytical hurdles were encountered here, but overall the contribution of the documentary analysis was invaluable to the research.

4.4.1 ANALYTICAL PROCESS

Although the consultation process was distilled into two primary documents – the oral and written evidence – it is more accurate to consider these as a collection of a larger number of documents as each is attributable to a single author/organisation (in the case of the written evidence) or a panel of interviewees (in the case of the oral evidence). Consequently, the written evidence consisted of 145 documents (separate submissions to the committee) and the oral evidence 23 documents (separate sessions with the committee at the House of Commons). Implicit throughout the consultation process was also the intertextuality (Coffey and Atkinson 2004) between the evidence documents and the text of the Bill itself as many of the points of objection raised referred to specific aspects of the proposed

legislation. Consequently, some attention was also given to the text of the Bill itself, its predecessor the Regulation of Investigatory Powers Act 2000 (RIPA) and the final report of the Joint Committee.

The consultation documents were accessed online from the UK Parliament website[82]. Scott (2004) provides a number of ways in which the documents can be classified. All documents were textual and of four kinds: written evidence submitted by individuals or organisations collated in one document; oral evidence transcribed and compiled in a second document[83]; the final report of the Joint Committee and last; the text of the Bill itself. Scott (2008) also categorises documents by access and authorship. In respect of the former, the documents were 'open-published' (available for public consumption). For the latter, while the documents represent official records of a parliamentary process and were published by the government, authorship of the documents can be described as each of Scott's three categories, public, private and state, owing to the fact that the evidence contained within them was written by members of the public, private and charitable organisations and government departments and officials. It is important to note these distinctions as the analysis was constructed around identification of the contributions of different groups of actors (i.e. authors).

The analysis was first directed at the written evidence submitted to the Joint Committee. In total 145 submissions were made, of varying lengths. The entire collection of written evidence totalled more than 600 pages. Altheide (1996) outlines an approach for analysing documentary sources, which guided the systematic appraisal carried out here. Consequently a protocol – 'a list of questions, items, categories, or variables that guide data collection from documents' (Altheide 1996: 26) – was designed to effectively deal with the large volume of data. The first stage was to categorise respondents to the consultation. This was a reflexive process, beginning with eleven categories and eventually refining this to seven:

- Individual/Non-Expert
- Advocacy/Non-Profit

[82] http://www.parliament.uk/draft-communications-bill/

[83] Visual evidence was available in the form of webcasts of oral evidence sessions. For practical reasons it made more sense to use the textual transcripts.

- Telecoms Industry
- Experts
- Media
- Official/Governmental
- Independent Authorities

For the purposes of analysis seven categories were both a sufficiently large number to allow for differences to be shown and small enough to allow for ease of analysis. The next stage was to apply the same process to the oral evidence, which consisted of 23 interview sessions with 55 respondents. The categorisation of respondents was suitable for incorporating the oral evidence and as a final step sub-categories of respondents were devised where appropriate.

The majority of the analysis of data was consistent with a qualitative approach. However as a precursor to this a brief quantitative content analysis was carried out on the written evidence. As well as noting the number of respondents in each category, this took account of the weight of each category's contributions to the evidence. For analytical purposes, this was valuable as it indicated who was most 'visible' and active in supporting or resisting the proposals of the Bill. The protocol for qualitative analysis of the documents consisted of a series of questions:

- What were the key arguments made for and against the Bill?
- What arguments were made most frequently by each category of respondents?
- To what extent did different categories of respondents make the same arguments?

Thus, the analysis of the content of the documents was thematic and comparative. Time constraints made it impractical to develop a formal coding strategy and apply this to every written and oral submission (i.e. every document). Instead, a sampling approach was used, producing a selection of each category's responses: five written submissions from each category of respondent and six of the oral evidence sessions, across a variety of categories (approximately one quarter of each of the types of evidence). In the case of the written evidence, this entailed the entirety of two category's responses given the small number of respondents from each. From this

developed an initial thematic framework, which was also informed by personal knowledge of the issues of concern to advocacy groups. The thematic analysis was driven jointly, therefore, by deductive and inductive imperatives.

This enabled identification of which categories of respondents discussed certain themes more prominently than others and this guided subsequent examinations of the texts. Searching for key terms derived from these themes in both the written and oral evidence – an affordance of having electronic documents – allowed identification of where important themes reoccurred. Moreover, it permitted insight into the last of the protocol questions above. As a result, the analytical process came to focus primarily on three categories of respondents: 'Telecoms Industry', 'Experts' and 'Advocacy/Non-Profit'. In itself, this outcome of the process was an important finding and Chapter Six discusses the main contributors to the debate around the CDB. Ultimately, identification of the most prominent themes justified focusing more attention on some categories of respondents than others. This was particularly the case with 'Individual/Non-Experts'. This category was by far the largest proportionally although the data presented in this category was of less (but by no means zero) analytical interest.

The process of documentary analysis employed during the fieldwork was an exercise in effective management of a large body of data. Methodological rigour was paramount to avoid becoming overwhelmed by what was a comprehensive and unparalleled account of how digital surveillance and online space is negotiated in practice. It also allowed reflections on the methodological issues inherent in documentary analysis. Specifically, part way through the analysis it became clear that the oral and written evidence documents had different characteristics. The former were much more 'engaging' owing to the method by which the data were captured. For all intents and purposes, the oral evidence was secondary interview data albeit gathered for purposes beyond social research. Indeed, many of the practicalities of documentary analysis encountered while engaging with the CDB consultation were those identified by McGinn (2008) in respect of secondary data: easy access and savings in time and labour. More than that though, the oral evidence was richer than the written evidence. While both supplied valuable data, the oral evidence exhibited questioning, probing, explanation and elaboration. Thus

the qualities of these data compared to the written data were the same as comparing primary qualitative interview data to written responses to open ended questions in a survey. The written evidence was more formulaic and precise, particularly in the case of responses from advocacy organisations, having been planned thoroughly for maximum impact. With this said, it was also interesting to note the occasions when respondents to the written evidence were later invited to give evidence to the panel (or in fewer cases, vice-versa).

4.5 MORAL PANICS AND THE MEDIA: EXPLORING WIKILEAKS

The final site for the data collection was the media. The two primary focal points were whistleblowing organisation WikiLeaks (a 'new media' platform and a potent agent of resistance) and 'traditional' mainstream press. As outlined in Chapter Two, there has been little systematic academic attention given to WikiLeaks, particularly with regards to (resisting) surveillance. The data collection first aimed to describe the phenomenon of WikiLeaks to theorise its contribution to our understanding of digital surveillance and resistance. Subsequently, echoing previous studies of social control – namely Stan Cohen's (1972) *Folk Devils and Moral Panics* – the fieldwork sought to examine the recent history and presentation of WikiLeaks and surveillance issues in the mainstream media. This discussion describes the choice to emulate aspects of Cohen's approach as well as methodological issues concerning media analysis. There is a final anecdotal reflection on the experience of investigating WikiLeaks through qualitative interviews with a former employee and a collaborator as well as attempts to make contact with Editor-in-Chief Julian Assange.

4.5.1 TRACKING DISCOURSE

The media are 'consequential in social life' (Altheide 1996: 69). Reports in the news media control cognition (Cohen 2002); they affect public perceptions and the construction of social problems – a core aspect of the negotiation of modern surveillance. Altheide (1996: 69) also emphasises the presence of 'powerful cultural symbols' in the news – a theme that is particularly relevant to the study of surveillance and resistance.

To a degree, a similar documentary approach was adopted during this stage of data collection as for the analysis of the CDB. The emphasis was on charting the change over time in media presentations of surveillance and resistance. This is called 'tracking discourse…following certain issues, words, themes and frames over a period of time' (Altheide 1996: 70). This does not equate to implementing a traditional 'discourse analysis'. While *some* aspects of language use in news reports were considered – tone and symbolism for instance – the primary agenda was to track the frequency and prevalence of news stories relating to the topics of interest, rather than the constructive or performative characteristics of language (Willig 2014). The Nexis database provided the mechanism for searching and retrieving relevant stories. Nexis is an invaluable resource for social research (Altheide 1996; Hewson *et al.* 2003; Ó Dochartaigh 2007; Schulz 2008). The depth of its historical coverage from the US and UK, availability of full-text news articles, powerful and flexible search capabilities and ease of downloading and saving search results all recommend Nexis as a resource for social research involving news media.

Queries of the Nexis database limited the search to 'UK publications'[84] as the volume of data generated by a search of all publications (i.e. worldwide) would have been unmanageable. Equally for the context of the thesis, this helped to ground the study in a UK context. WikiLeaks was used as the primary organising search term. Thus the time-frame of the search was dictated by the emergence of WikiLeaks in the press in January 2007. The time of the initial search (August 2012) naturally acted as the end-point although the ease by which reports could be retrieved from Nexis meant this was constantly updated as the research progressed. This was particularly crucial when, in June 2013, surveillance became a headline issue with the revelation of information concerning the NSA and GCHQ from Edward Snowden. These important and highly relevant events were able to be incorporated with little effort into the analytical process. Again, opportunity played an important role in the research process.

A small set of search terms (with Boolean operators where required) were devised to chart the reporting of various topics in the press. The search was directed at

[84] The category 'UK publications', in contrast to 'UK newspapers' also includes a selection of magazines that were considered reliable sources of information.

keywords within articles rather than headlines to ensure a broad coverage. Initially, three search terms were used:

- '*WikiLeaks*'
- '*Assange*': initially 'Julian Assange', this was revised as it was clear the press quickly began referring to him primarily by surname.
- '*Surveillance* AND *Privacy*': using only 'surveillance' retrieved far too many reports to be of use. Moreover, the term was imprecise and captured articles that were not related to the type of surveillance of interest to the research. 'Privacy' was included as it was considered to be the most appropriate coupling to obtain articles that discussed surveillance technologies and their (potentially) harmful consequences. Arguably, this could have skewed the results in favour of reports that presented surveillance in a negative light, e.g., 'privacy concerns over new surveillance tools'. However, it is not in the nature of the news media to be overtly supportive of government or corporate surveillance and thus it is fair to say that searching for articles containing 'surveillance AND privacy' would generate an accurate reflection of the volume and nature of news media reporting on the topic.

Nexis enabled automatic filtering of results so repeated articles were removed, improving the accuracy of the number of articles returned. The next step was to count the number of articles featuring the keywords each month and tabulate these in Microsoft Excel for converting to graphical format. Nexis has an inbuilt limitation on the number of articles it will return (3,000). Thus, when WikiLeaks was featuring minimally in the news, searches could cover a period of one year each month tallied accordingly. As WikiLeaks appeared more frequently, this approach required refining to month-by-month searches. In some months, the total number of articles exceeded 3,000 and so fortnightly or weekly searches were conducted until the volume of reports for that month could be calculated. This had the benefit of highlighting early on key 'moments' (i.e. large fluctuations) in the reporting history.

When Snowden's leaks made the news in mid-2013 the search terms were expanded to include the following:

- '*Edward Snowden*': unlike 'Julian Assange', Snowden's full name was used as his surname was more common and returned a wealth of irrelevant articles.
- '*NSA* OR *GCHQ*': given that many news reports concerning Snowden's leaked documents mentioned both the NSA and GCHQ, it was feasible to use 'OR' as opposed to 'AND'.

The search was backdated to 2010, thereby placing reporting trends concerning the NSA and GCHQ in their historical context[85]. Owing to the infrequency of reports featuring WikiLeaks and Assange from 2007 to 2009, the analysis focused on the period from 2010 to 2013, when the impact of WikiLeaks in the press was most visible. One final addition to the search criteria aimed to extract from within the search results a subset of articles specifically addressing surveillance and/on the Internet (i.e. 'digital surveillance'). Each set of results for 'surveillance AND privacy' were also searched for 'online' or 'Internet'[86]. This reduced the number of relevant articles (an important finding in itself) and also allowed for more thorough analysis.

As with the previous case, volume of data was a hurdle. This was particularly the case with WikiLeaks; at the height of their popularity in the news, there were more than 3,000 news articles in the UK in one month. A similar approach as before was adopted to effectively parse the data from Nexis. Nexis results were sorted by relevance (the number of times search terms are mentioned in an article) and the 25 most relevant articles from each set of results were reviewed. In the case of online/Internet-related surveillance articles, there was some repetition and so this process also involved filtering these and combining the two sets of search results to identify the most relevant. Finally, scanning the headlines proved to be a reliable indicator of the topic and tone of each article. This supplemented the frequency analysis of articles with an appreciation of their topic and tone.

Regarding the theoretical framework, the process of 'tracking discourse' allowed an emulation of Cohen's (1972) analytical approach to understanding the creation of 'folk devils' and 'moral panics'. Cohen adapted a framework from research on natural disasters to explain the construction in the news media (as well other social

[85] Edward Snowden, naturally, did not appear prior to June 2013.
[86] Boolean operators did not work for the 'search within results' function and so each term had to searched for separately.

arenas) of social problems – specifically those related to crime and disorder. Drawing on this approach allowed me to theorise the relationship between WikiLeaks (and later Snowden) and surveillance with respect to their construction as social problems and to what extent it was possible to characterise these phenomena as moral panics. Locating this final case around the news media was therefore valuable and drew on a long-established tradition of examining the media as a forum for the creation of public anxieties and concern and the construction of deviance and control (for example Young 1971; Cohen and Young 1973, Ericson *et al.* 1989, 1991; Ferrell and Websdale 1999; Loseke 2003). It proved to be a useful mechanism for appreciating the social and political impact of WikiLeaks and Snowden and helped to condense what was a relatively rapid succession of high-intensity events into a comprehensible story. As with the CDB, the quantity of material precluded in-depth content analysis. However, the approach captured the essence of the media trajectories in a meaningful way for the broader aim of the thesis.

4.5.2 CHASING THE CYPHERPUNKS

The second component of the fieldwork in this site was directed specifically at WikiLeaks, investigating its position as a new platform in the changing landscape of media and communication and technologies. Primary and secondary interview data constituted the basis for this and so the final part of this recitation of method returns to the observations above concerning the interviews that helped to inform all three of the research sites. This aspect of the research required significant persistence at times – also a fantastic learning curve – but ultimately produced primary data that added tremendous value to the thesis.

Two of the interviews conducted as part of the research were with individuals who had worked in the past with WikiLeaks: Daniel Domscheit-Berg and Smári McCarthy. The experience of interviewing the latter in respect of Skype was described earlier; it was on this occasion the efforts to record audio and video caused more problems than they resolved. As he lived in Germany, Daniel was also contacted via Skype. His account of the time he spent with WikiLeaks (Domscheit-Berg 2011) was motivation to include him in the research. Until he quit in late 2010 following internal conflicts in the organisation Daniel was a core member of WikiLeaks, having

been one of three people responsible for much of their operations since it began in earnest. This unique background situated Daniel as a valuable contact for the research and justifies having only two interviewees with a connection to WikiLeaks. There is a tradition in social science (and criminology specifically), characterised most prominently by Clifford Shaw's *The Jack Roller* (1930), of case studies of individuals and narrative style interviews. The interview with Daniel was not a narrative analysis, nor was the research a longitudinal case study of WikiLeaks. However, Daniel, as indicated above, was the only person realistically available to describe the operation and motivations of WikiLeaks in its early days. Of the other two, one continues to reside in the Ecuadorian Embassy in London and the other remains anonymous. While small interview samples are typically seen as limited in the insight they can provide, in the case of this research the opposite was true. Here, 'n=1' (see Maruna and Matravers 2007) was of enormous benefit to the research.

After leaving WikiLeaks Daniel began his own platform for the receipt and transmission of leaked material, *OpenLeaks*. This was the first point of contact[87]. A response was received from 'Max' who, alongside saying he would pass the request to Daniel, queried several aspects of the research topic. A few emails were exchanged in this manner but a response from Daniel was not forthcoming. Eventually, he was emailed directly; his address appeared in one response from Max in the 'Cc' section of the email header. Daniel responded positively but shortly after email responses ceased, despite prompting. In addition, emails returned undelivered and the OpenLeaks website was found to have been taken offline. As a last resort, contact details were located for Daniel's wife who was asked if she could help to get back in touch with Daniel. Fortunately a positive response was forthcoming and Daniel re-established contact, explaining problems the organisation had been experiencing with their servers. While it took two and a half months, obtaining this interview was a highlight of the entire research and a valuable lesson in persistence.

[87] See Appendix D: OpenLeaks emails for the majority of this correspondence. Owing to technical difficulties, some of these emails were irretrievable.

The next logical step was to attempt to make contact with Julian Assange. Having said that, this was initially borne out of opportunity rather than meticulous planning[88]. What might be called 'a series of unfortunate events' characterised the efforts to recruit Assange. A speculative visit to the Ecuadorian Embassy in London, a formal written invitation to take part in the research[89], a series of requests to WikiLeaks' publishers The Sunshine Press and an email conversation with Assange's (accommodating) mother failed to secure his participation in the research process. Assange's voice does feature in the research but via secondary data: a transcription of a Channel 4 documentary on WikiLeaks, several short clips discussing *The Spy Files* release in 2012, and transcripts of several interviews and lectures. Given the failed attempts to recruit Assange, secondary data was the only viable means of placing his knowledge and opinions in this research. These did not constitute a substantial portion of the data for analysis in this research site, but they were helpful for providing a degree of insight into the rationale behind WikiLeaks and their strategies for disclosing information[90].

4.6 ETHICAL AND POLITICAL DIMENSIONS

The final portion of this chapter deals with ethical and political dimensions of carrying out research around surveillance. The start of this chapter alluded to the parallels between social research and surveillance. Drawing from Lyon (2002: 3) and Haggerty and Ericson (2000), Kemple and Huey note how 'modern social science and modern surveillance were each from their earliest days a means of "keeping tabs on the mobile" and yet today are both components in a much larger assemblage' (2005: 155). By this, they mean to draw attention to the potential for reflexivity in social science that studying surveillance allows, and the simultaneous positioning of the researcher within 'flows' of observation and visibility that characterise surveillance relationships. This research exposed and alerted me to a number of the ethical and political dimensions surrounding (online) surveillance research. These overlap to a great extent with issues inherent to the nascent fields of computational social science and 'big data'.

[88] For a full but more anecdotal account of this process, see Appendix F.
[89] See Appendix E.
[90] See Chapter Seven.

4.6.1 PRIVACY, ANONYMITY AND CONSENT

Privacy is an emotive issue at the heart of discussions around surveillance and the consequences of the continual trend towards online interaction (including 'big data'). It is also an intrinsic consideration for any social research. The combination of the two – online social research and particularly that which involves social media – is thus characterised by lively debate. Solove (2007b) and Albrechtslund (2008) among others point to the shifting nature and expectations of privacy in online social spaces. In part, this could be the result of changes in online relationships and surveillance. Andrejevic's (2005) three types of 'lateral surveillance' (romantic interests, family and friends) emphasise *mutuality* as opposed to the traditional disempowering, top-down conception of 'watching over' people. Audiences online are many and it can be a challenge to keep tabs on the sorts of information we share and with whom we share it. Underpinning and fuelling much of this are corporate 'consumers' of our data – an 'audience' perhaps overlooked by many people. Such changes highlight the *contextual* nature of privacy online (Nissenbaum 1998, 2004, 2009; Zimmer 2006; boyd 2008); what we expect and understand by privacy and the related issues of anonymity and consent differs according to online setting and audience. It is also apparent that what is 'public' and 'private' is relative in the context of social media; we may choose to share information on Facebook with audiences we would not usually engage with in normal social interaction or likewise, we may share more personal information on some sites as opposed to others.

The increasingly public nature of our data online poses many difficulties, therefore, for understanding privacy. It can be difficult in this context to classify or quantify what a breach of privacy is (boyd and Crawford 2012). For instance, is there an immediate impact or will one be felt several years later? The ethics of online social research are equally complex (Ess 2002; Markham and Buchanan 2012) and need careful consideration in this age of proliferating and accessible data (see also COSMOS 2014). The typical response to the question of how to treat online/social media data is that 'it is already public' (Zimmer 2010) and so there should be few ethical concerns with the collection of these data for research purposes. It is a question of informed consent. Publicly available data of the sort found on social media compels us to reconsider what it means to give consent to the collection and

analysis personal information. While social media users accept the terms of service when they register (most likely without reading them at all or at least to any large extent) this should not necessarily be taken as tacit agreement for the use of their data in settings beyond those of the service they signed up for. It is a question of audience again and the case of Lewis *et al.* (2008)[91] illustrates this. As Zimmer's (2010) critique of the ethical basis of that research argued, while users may have agreed to their personal information appearing on Facebook, it is unlikely many would expect their data to be removed from this setting (despite anonymity) and published in academic journals. As Zwitter (2014: 6) has also observed, somewhat reminiscent of the issue of 'social sorting' (Gandy 1993; Lyon 2003b), 'uncomfortable truths' about social groups who are identified and studied on Twitter can return negative impacts upon those groups.

This research was not based significantly around the collection and analysis of individual social media data but there are some aspects of the fieldwork that do merit consideration in light of these issues. Sufficiently so that during a round of questions following a paper related to this thesis presented at the Surveillance Studies Network conference in 2012, one delegate asked how I reconciled being a surveillance researcher (usually taken to imply a degree of anti-surveillance) with the use of research techniques that were tantamount to surveillance practices in their own right. There is not a straightforward answer to this kind of question. Neither is it true that using such tools is 'surveillance'. The work of Kemple and Huey (2005) again helps us to understand that researching surveillance places the researcher within a series of flows between observers and observed and at any one time we can be situated in both of these positions. We do not have to categorise ourselves as either 'observer' or 'observed'. The key point to take from this illustration is that using *NodeXL* and similar computational platforms does not have to equate with 'doing surveillance' rather than 'doing research'. The distinction is a hazy one in truth but, taking lessons from the above discussion, evidently it is the obligation of online/social media/surveillance researchers to account for the contexts and people

[91] The *Tastes, Ties and Time* project (Lewis *et al.* 2008 and see also Lewis 2008) involved the location and downloading of over 1,000 Facebook profiles of a US college student cohort. Profiles were anonymised and fed into a codebook dataset that identified, among other demographics, gender, ethnicity, political views and college major. Despite anonymisation, Zimmer (2010) describes the relative ease by which profiles were 're-identified' – the college was identified as Harvard and many of the students were able to be identified.

they study and consequently how privacy, anonymity and consent are to be managed.

The research methods used here did not seek to collect personal information or first-hand accounts from social media. They mapped out connections. This use of publicly available data does not pose any harm to service users; admittedly it is carried out in accordance with the 'it is already public' line of thought but this is one context where the argument can be supported. One issue does arise, however, that researchers employing computational methods should be aware of: inadvertent collection of personal data and the revelation of information beyond that which was intended or anticipated. In the context of this fieldwork, capturing social network connections using *NodeXL* meant simultaneously collecting a wealth of data beyond that of 'who follows whom': most recent tweets, geo-location data and profile pictures to name a few. These data were not intended to be collected, nor were they used in the research, but they were collected nonetheless. What obligation does this place on the researcher? Likewise, with the increasing sophistication of computational research tools it is entirely plausible that information about people and their networks could be gleaned beyond that which is explicitly stated in any data. This process of 'triangulation' or 'homophily'[92] is a trait of big data analysis. Some might argue that this is the purpose of research; interpreting meaning behind actions and statements and uncovering unseen social processes are traditional social science pursuits. However, with the scale and depth of data available to social scientists (and any other consumers of big data) and capabilities of algorithmic analysis these interpretations become certainties. Our data can reveal far more than they appear to. As social researchers we should consider what privacy means and how it is experienced in different contexts. As Zimmer (2010: 324) concludes, *'*[c]oncerns over consent, privacy and anonymity do not disappear simply because subjects participate in online social networks; rather, they become even more important.'

[92] See Chapter Six.

4.6.2 SUBJECTIFICATION AND SUBJECTIVITY

Kemple and Huey (2005) describe their experiences of researching patterns of surveillance and counter-surveillance in a deprived ('Skid Row') neighbourhood. They argue that researchers in such environments can become implicated in these relationships – identified as agents of surveillance and as appropriate targets for counter-surveillance (resistance). The risk of being labelled as an agent of social control is one that must always be managed when researching surveillance of any kind – both in physical and virtual places. I experienced this during Masters research prior to this thesis when attempting to recruit participants from a public, online forum of an anti-surveillance campaign group. These efforts were met with scepticism and a degree of distrust; ultimately the best solution was to carry out the intended 'focus group' within the website forum rather than on an external website. For people who are naturally distrustful of surveillance meeting them on their 'home turf' was vital (although was by no means a panacea). There is, however, a noticeable difference in attitude between administrators/staff of advocacy groups and their member base. The former – recruited during this fieldwork – appear much more willing to engage in research. Again, Kemple and Huey's (2005: 155) observations shed some light on why this may be.

> 'Among the ironies of the supposed 'democratization of surveillance' is that many of the most marginalized and mobile subjects of observation are already hypervisible and hypervigilent by virtue of their lack of access to private and protected places, and yet at the same time they remain largely unseen and unaccounted for, forgotten and unheard from (Archand, 1979).'

In the context of digital surveillance 'marginalised and mobile subjects' are understood to be members of the public – everyday 'Internet users' subject to many forms of tracking and monitoring. Distrust of researchers asking about surveillance, particularly in online places where identity cannot be verified, is understandable. Chapter Six addresses the issue of 'unheard voices' in surveillance relationships; the pre-legislative consultation provided a valuable arena in this respect where the 'lay public' could willingly and trustingly share their opinions. To borrow Kemple and Huey's phrase, we should acknowledge the 'dialectic of visibility and invisibility which envelops the lives of each and every one of us' (2005: 155). This research has allowed me to develop my own appreciation of the complexity of the relationship

between surveiller and surveilled and how I occupy both sides of this as a researcher of/doing surveillance and as a citizen concerned about the risks of surveillance.

The other side of this coin is the risk of researchers being subject to undesirable forms of surveillance. I do not appear to have suffered any negative repercussions during the research. However, it is prudent (if not a little paranoid perhaps) to acknowledge the fact that repeated attempts to contact Julian Assange and contacting his former associate Daniel Domscheit-Berg, among other aspects of the research, may have increased my 'visibility' as a subject of surveillance. Had I been successful in gaining access to the Ecuadorian embassy, this would certainly have been the case.

During the course of this research – undeniably a product of immersing myself in the area for a period of years – I have also become increasingly aware of the ubiquity and risks of online surveillance. This has had the effect of changing my behaviours regarding various protective measures online. The outcome of this research, therefore, is that acknowledgement of my position as both researcher and 'citizen' in respect of the surveillance relationships under study. Becker's (1967) classic question springs to mind. Social research is never value-free; indeed, it appears to be the tendency of surveillance studies to raise awareness of the risks surveillance poses rather than endorsing the benefits that do exist. I did not begin this research with strong 'anti-surveillance' values but as my awareness of the field has developed my opinions have crystallised around the profoundly negative implications of modern surveillance practices. I am now a member of the Open Rights Group, who campaign for digital rights. We should consider, therefore, that not only can researcher values impact on research participants or projects but so can the research problem impact on the researcher. Neither of these outcomes invalidates research. Studying surveillance has allowed me to question my own values regarding the protection of digital rights and privacy and this is an intrinsic part of the research process.

4.7 CONCLUSION

This chapter has provided a reflexive overview of the design and implementation of the research process of this thesis. The multi-strategy/mixed-methods approach

employed was designed to capture the diversity of relationships and settings in which modern digital surveillance and resistance to surveillance occur. Alongside eliciting contributions from expert participants in this arena using traditional qualitative methods, computational social science research added an innovative aspect to this methodology by allowing for the exploration of near real-time changes in some of the networks that constitute this contested environment. Illustrated throughout this chapter is the overlap between the methodological and theoretical aspects of this research. Specifically, how the study of digital surveillance and resistance, the socio-technical system of the Internet, the use of online research methods and the importance of the concept of privacy interact in a complex but continually fascinating way.

- .... . -. . .-- .... --- -- . --- ..-. -- .. -. -.. .-.-.-

CHAPTER FIVE

THE ORGANISATION OF RESISTANCE: NETWORKS AND NODAL GOVERNANCE

5.1 INTRODUCTION

This chapter begins the empirical component of the thesis. The aim of this first stage of the analysis is to examine the online social organisation of resistance to surveillance. It is based on the idea that as digital surveillance is characterised by globally distributed networks and information flows, so too must resistance be understood in the same way. To borrow a term from Bauman and Lyon (2013), because modern surveillance is 'liquid', characterised by mobility and flexibility, it follows that so too ought resistance to be a fluid, adaptable process. For this reason, the chapter develops as its basis the theory of nodal governance that guides the research as a whole. Previous research has sought to demonstrate the workings of nodal governance by focusing on public and private providers of security (Shearing and Stenning 2003; Burris *et al.* 2005; Wood and Shearing 2007). The rationale behind this part of the fieldwork was to expand those traditional notions of nodal governance by looking to civil society and, specifically, those settings and nodes who resist the various forms of governance exercised elsewhere – namely, techniques of digital surveillance. The subjects of this chapter, therefore, are the members of a global network of 'privacy advocates' (Bennett 2008) who campaign around a host of issues related to digital surveillance. The chapter clarifies in what sense we can consider these organisations, and civil society more broadly, as governing nodes. It also shows, through visualising online network data, that resistance to digital surveillance can be understood as both a macro-level social process and a micro-level series of interactions and exchanges.

The data that support the observations in this chapter are drawn from some of the sources outlined in Chapter Four. The primary source is hyperlink network data, retrieved and visualised using *Issue Crawler* and *Gephi*. These data are

supplemented, where appropriate, with qualitative interview data from members of advocacy organisations. The analysis in this chapter employs concepts from nodal governance theory and social network analysis (SNA), outlined in Chapters Three and Four respectively[93]. While SNA metrics quantitatively illustrate communication and organisation within the network, these can be contextualised with reference to nodal governance theory and the other qualitative data. Together, these concepts allow us to gain an insight into the prominence of various groups within the community of privacy advocates, the structural features of the network, its potential to change over time and adapt to emergent issues and the ways in which its members go about resisting digital surveillance. Previous studies of privacy advocacy (Bennett 2008) and networked organisation (Introna and Gibbons 2009) have sought to delineate these features. The network analysis presented here is a necessary update to these efforts, as new sites of resistance have emerged. Gaining an understanding of the mentalities, technologies, resources of the nodes within the network and the presence of 'superstructural nodes' (Burris *et al.* 2005) adds to the analysis by illustrating how those who resist surveillance interact with other nodes tradtionally illuminated in studies of governance of security.

5.2 INFORMATION POLITICS AND HYPERLINK NETWORKS

The purpose of the network of privacy advocates, broadly speaking, is to resist the expansion of unwarranted or invasive surveillance practices and to protect individual privacy. While over-simplified, this represents a useful starting point. A key strategy by which they aim to do this is what Bennett (2008) refers to as *information politics*, 'the politics of persuasion…speaking truth to power.' More specifically in the context of surveillance and privacy, this strategy:

> 'often involves extrapolations from the experiences of similar surveillance systems in other times and places…It often requires a leap of faith, that many are unwilling or incapable of making, from a particular provision under discussion to larger arguments about the slow and incremental slide toward the "surveillance society"' (Bennett 2008: 98).

[93] Sections 3.2.3 and 4.3.2.

Online as well as offline, this entails the transmission of information to the public about particular surveillance-related issues. Interview data from representatives of Privacy International and the Open Rights Group (ORG) support this:

> 'We're a charitable organisation so our resistance is in the form of public discussion, raising awareness, public education and helping to assist policymakers in ensuring they have an informed understanding of policies they're trying to introduce…We do a lot of public out reach to enable an understanding both in the human rights communities and other non-profits to ensure that they're appropriately protected…' (Eric King, Privacy International).

> '..we do a lot of blogging and advocacy work ourselves…in-house policy work where we talk to policymakers and politicians…getting our 30,000-odd active supporters interested and informed enough so that they get worked up enough to do something about it…to try to foment the public disquiet…' (Pete Bradwell, Open Rights Group).

An important avenue for transmitting information and keeping such issues in the public eye is the Internet. Both Privacy International and the ORG have an active web presence – as do many other organisations, as this chapter illustrates – and therefore the online environment is an important factor to understand in the organisation of resistance.

The hyperlink structure of the Internet means that Internet users can follow links between websites to other related sources of information. It is to be expected that advocacy groups with similar interests or working towards similar goals will show some degree of mutual support through linking to one another's websites[94] or to the same collaborative campaign website. Additionally, should Internet users want to find out more about a particular surveillance practice the use of a search engine will present a list of results that are ranked according to those websites linked to most frequently by others. Software such as *Issue Crawler* gathers these links and allows us to visualise networks according to these patterns of connectivity.

Another key aspect of information politics, and more broadly of social control online, is the presence in the network of non-advocate groups. As the theory of nodal governance dictates, governing nodes in civil society do not act in a vacuum but interact with other nodes in different sectors. The role of governmental bodies, regulatory agencies, the traditional news media and social media should therefore

[94] This of course is not to be taken as a given. Hyperlinks do not necessarily convey meaning and for that reason cannot be assumed to be an endorsement of the destination website (see Chapter Four).

not be neglected. The data gathered suggest there are a number of prominent nodes in this regard.

Previous research in this field suggests that the behaviour of the advocacy network may 'transcend the intentions and possibilities of individual actors' (i.e. pursuing their own political agendas) and to become an 'expanding and cohesive online network for information politics and meta-surveillance' (Introna and Gibbons 2009: 234). 'Meta-surveillance' in this context is what, in Chapter Three, was discussed as 'resistive surveillance' – watching the watchers as it might be termed. Consequently, the potential to expand and incorporate a cohesive body of civil society nodes could be the key to effectively resisting surveillance. Nodal governance theory would see this as incorporating in to the network institutions with a more diverse range of mentalities, technologies and resources (Burris *et al.* 2005). The consequence of which would be, arguably, to make the network more flexible and adaptable to resisting diverse surveillance practices in different geographic locales. At the same time, network metrics allow us to assess whether this 'transcendent' ability of the network exists. These are briefly recapped from Chapter Four, alongside the organisational characteristics of the network that are of interest for the analysis.

5.2.1 METRICS, MEASURES AND NETWORK STRUCTURE

There are three types of network centrality that can be identified: degree, Eigenvector and Betweenness[95]. When constructing the advocacy community these measures are helpful because they allow us to see which members are paid attention to the most and which are useful for the relay of information. This matters for the online advocacy community for two reasons. First, it can indicate who may be influential in shaping the framing of a particular issue. Second, if we consider an Internet user searching for information about a given surveillance issue it is likely they will end up being directed to those with higher Eigenvector centrality or being able to access related information by virtue of a bridge existing between two sub-communities.

[95] See Chapter Four (4.3.2) for a description of these metrics. Figure 1 provides an illustration of Eigenvector and Betweenness centrality.

Where centrality helps to identify prominence and position in the network, the overall structure of the network is also an important consideration. For instance, the effect of clustering together nodes in the network according to frequency of linking is to produce areas of varying density. As Introna and Gibbons (2009: 236) observe:

> 'we are likely to encounter a relatively stable *core* of actors that are steadily affecting changes in the *periphery*[96] through their on-going linking practices. These *core* actors tend to have a high level of visibility…and as such are disproportionately likely to be visited and linked to repeatedly, thus, affording them growing importance or centrality in the network' (*emphasis* in original).

These structural characteristics of the network are not fixed; they fluctuate as a result of hyperlinking practices. If a node in the core links to one in the periphery , the effect is to draw them in closer to the centre of the network. The result for the network, as a modality for resisting surveillance through information politics, is that more information is available to be brought to bear on the issue. This phenomenon is referred to as *positive network externality*: benefits for the network as a whole as result of these linking practices. The distinction between the core and the periphery is not clear-cut in the analysis below and an intermediate zone between the two is highlighted. Furthermore, there are sub-communities within the core and elsewhere that are important features in their own right. The shape and structure of the network is also dictated by real-time response to current surveillance issues[97].

Last are three structural characteristics that may affect the ability of the advocacy community to achieve its goals: density, stability and reciprocity. Density, or fewer 'degrees of separation'[98] will permit information to travel around the network more quickly because fewer links will be required to connect separate nodes. The core is the densest area of the network. Stability would prevent the network (and such density) dissipating over time. The ability of the network to remain cohesive over time is potentially a crucial factor in resisting surveillance (Introna and Gibbons 2009). Similarly, nodal governance theory would suggest in this case, where there is

[96] The changes in the periphery to which the authors refer are dealt with in section 5.3 and 5.6 of this chapter.
[97] Section 5.6
[98] The shortest distance between two nodes in a network. Based on the 'small world hypothesis' that suggests any two people in the world are connected by no more than six links. When calculating network metrics, *Gephi*, the average number of degrees of separation is referred to as the average geodesic distance; the lower the number, the denser the network.

a broadly shared mentality about the dangers of surveillance, *cooperation* and not *competition* is the key to effective governance from within civil society. However this assumption is questioned later. Reciprocity would also signal a cooperative approach to networking, as opposed to only receiving links and not directing Internet users elsewhere. Reciprocity in this instance need not necessarily mean linking directly back to a website that a link is received from. However, nodes should not act as 'cul-de-sacs'.

Exchange and transmission of information within the network is vital for the privacy advocates. This was made clear in one interview:

> 'One of the main roles we've taken on has been…Co-ordinating civil society for want of a better word and helping set up the email lists and the meetings between people like ORG and Privacy International and Liberty and so on to help us understand what we're doing respectively…sharing intelligence, understanding who sits where, whether anybody's moved, put together a picture of where we're being effective' (Pete Bradwell, ORG).

This emphasises again the importance placed on cooperation, both online and offline. It also acknowledges that different organisations may have different mentalities, technologies and resources that can be co-ordinated for greater effectiveness. In quantitative terms for the network analysis, density, stability and reciprocity, then, are all features that could contribute to such effectiveness of the community in resisting surveillance. Of these, the first two have been highlighted in early research into the online advocacy community (Introna and Gibbons 2009). The authors point to a small, stable and 'geographically biased'[99] core consisting of prominent advocate groups such as Privacy International, Statewatch and the Electronic Frontier Foundation (EFF). As suggested above, non-advocate groups may also have a key role to play, but Introna and Gibbons (2009: 248) suggest that in 2008 the ability of the network to draw in such nodes was limited.

[99] The issue of geography is revisited below, with particular reference to the German socio-historical context for surveillance and resistance.

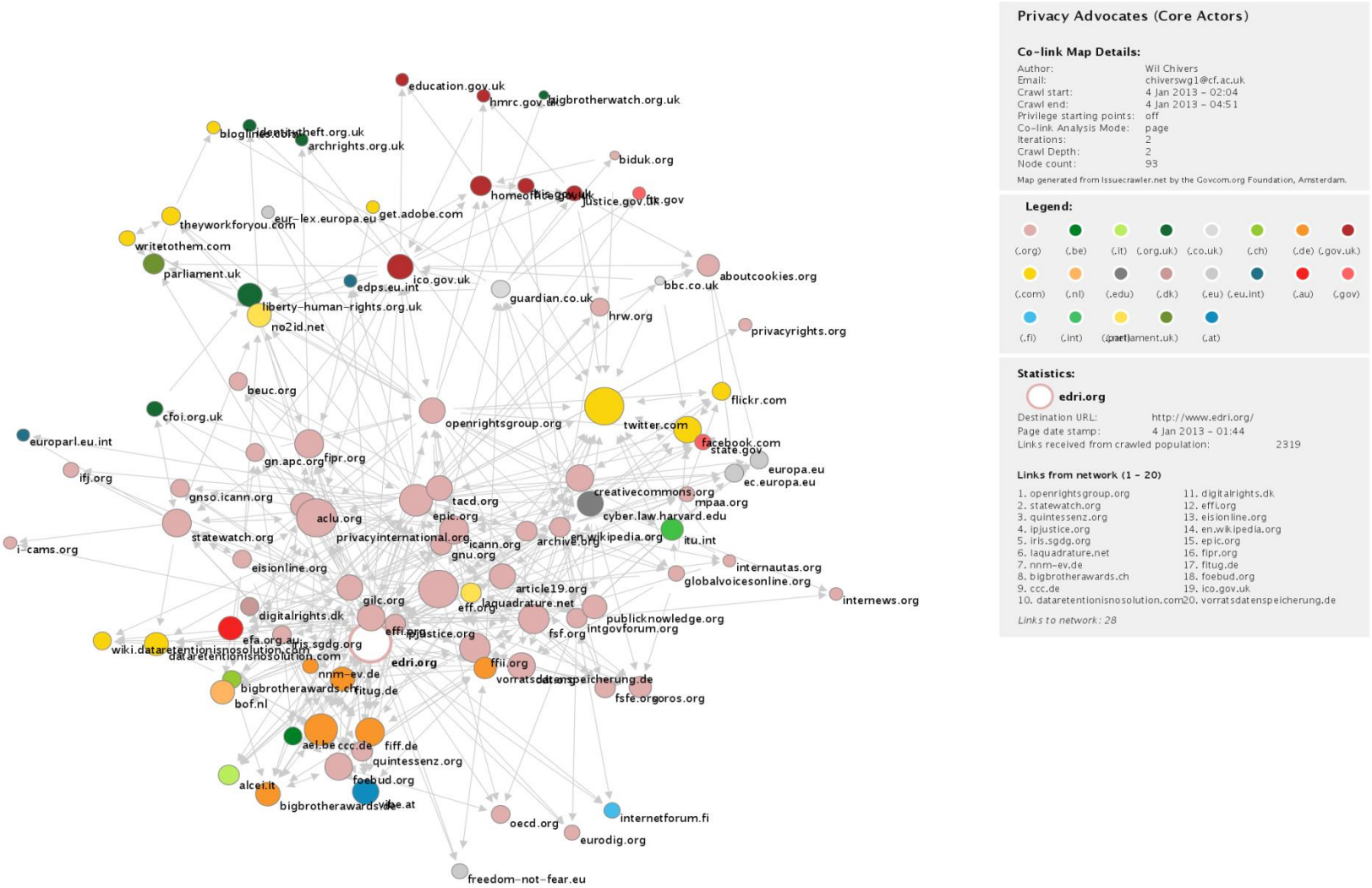
5.3 ONLINE CIVIL SOCIETY: KEY NODES

5.3.1 THE CORE – DEGREE CENTRALITY

The logical place to begin examining patterns of organisation and communication within the online advocacy community is the 'core'. It is here where the majority of advocate groups are to be found and, as described above, it is also the densest area of interaction in the network. Figure 2 below is a snapshot of the network on the 4th January 2013. The nodes in this diagram are scaled according to in-degree; the larger the node, the more links received[100]. The lower left corner of the network is the core; there are a visibly higher number of linkages between nodes here. A brief examination of the core defines several key nodes by in-degree: the European Digital Rights Initiative[101] (EDRi), the Electronic Frontier Foundation[102] (EFF), Privacy International[103] and the Electronic Privacy Information Center[104] (EPIC). These four organisations are prominent advocate groups. The preponderance of other nodes situated in the core are also advocates concerned with some aspect of privacy and digital rights – the Global Internet Liberty Campaign[105] (GILC), Article 19[106], Electronic Frontier Finland[107] (EFFI) and La Quadrature du Net[108] are all good examples. There are also nodes who are not advocates by nature, but whose work has an overlap with the interests of these groups; GNU[109] is a free Unix-based operating system developed in accordance with the ethos of the Creative Commons (free access, development and distribution of software). Other nodes of interest situated on the border of the core area such as the Chaos Computer Club[110] (CCC) and the Informatics Centre for Peace and Social Responsibility[111] will be discussed in due course.

[100] Links received refer to those from discrete websites as opposed to pages *within* those websites.
[101] edri.org
[102] eff.org
[103] privacyinternational.org
[104] epic.org
[105] gilc.org
[106] article19.org
[107] effi.org
[108] laquadrature.net
[109] gnu.org
[110] ccc.de
[111] fiff.de

FIGURE 2: NETWORK ON THE 4TH JANUARY 2013, NODES SCALED BY IN-DEGREE



Privacy Advocates (Core Actors)

Co-link Map Details:

Author:	Wil Chivers
Email:	chiverswg1@cf.ac.uk
Crawl start:	4 Jan 2013 - 02:04
Crawl end:	4 Jan 2013 - 04:51
Privilege starting points:	off
Co-link Analysis Mode:	page
Iterations:	2
Crawl Depth:	2
Node count:	93

Map generated from Issuecrawler.net by the Govcom.org Foundation, Amsterdam.

Legend:

(.org) (.be) (.it) (.org.uk) (.co.uk) (.ch) (.de) (.gov.uk)
(.com) (.nl) (.edu) (.dk) (.eu) (.eu.int) (.au) (.gov)
(.fi) (.int) (.parliament.uk) (.at)

Statistics:

edri.org

Destination URL: http://www.edri.org/
Page date stamp: 4 Jan 2013 - 01:44
Links received from crawled population: 2319

Links from network (1 - 20)

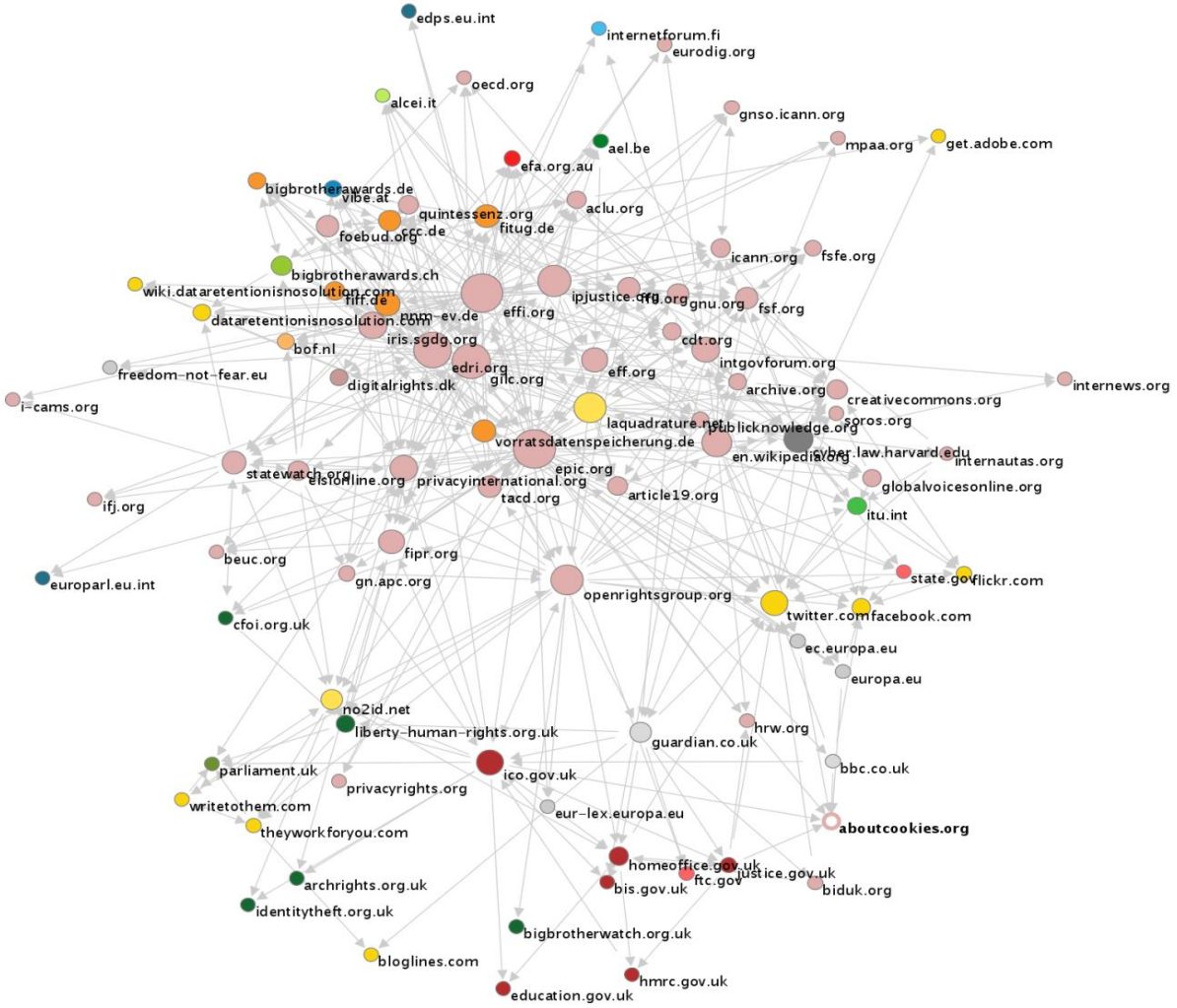
1. openrightsgroup.org
2. statewatch.org
3. quintessenz.org
4. ipjustice.org
5. iris.sgdg.org
6. laquadrature.net
7. nnm-ev.de
8. bigbrotherawards.ch
9. ccc.de
10. dataretentionisnosolution.com
11. digitalrights.dk
12. effi.org
13. eisionline.org
14. en.wikipedia.org
15. epic.org
16. fipr.org
17. fitug.de
18. foebud.org
19. ico.gov.uk
20. vorratsdatenspeicherung.de

Links to network: 28

Exploring the network online also shows where links to these key nodes come from and conversely whom the key nodes link to. The key in Figure 2 identifies the 20 nodes who linked to EDRi – the majority of whom are advocate groups, of which several are also located in the core. The same is largely true of the EFF, EPIC and Privacy International. Each of their situations within the core should also be noted, however, as this gives some indication of where links are received from and given to in the network. For example, EDRi is more connected to the organisations in the lower left section of the network whereas Privacy International and EPIC are more connected to the actors in the top half of the network.

There is, therefore, a high degree of interlinking within the core (high density). Additionally, the majority of nodes within the core are advocates of one sort or another. There are a couple of implications for understanding this network in respect of nodal governance at this early stage. The population of the core of the network solely by advocacy groups indicates a broadly shared mentality within the community. As Burris *et al.* (2005) describe, mentalities are specific ways of thinking about the matters that nodes (in this case advocacy organisations) have emerged to govern. Governance in this respect is engaged in by way of challenging the actions of those public and private entities that seek to implement digital surveillance practices. The various nodes within the core (and the rest of the network) do all have their own specific interests, goals and expertise, as will shortly be illustrated. However, in general terms we can argue that there is a shared counter-surveillance/digital rights mentality, particularly within the core of the network. This acts as a distinct centre of gravity in the community around which more dispersed nodes can coalesce. Another implication concerns the visible existence of networking. Wood and Shearing (2007) suggest that whether nodes come together to form networks is an issue to be explored empirically. The core of the network – as the data go on to show – remained largely stable. Online, therefore, it seems that the nodes that comprise the privacy advocacy community do indeed come together to form networks. To what extent this signifies more formal processes of cooperation is yet to be seen.

FIGURE 3: NETWORK ON THE 4TH JANUARY 2013, NODES SCALED BY IN-DEGREE AND OUT-DEGREE



Privacy Advocates (Core Actors)

Co-link Map Details:

Author:	Wil Chivers
Email:	chiverswg1@cf.ac.uk
Crawl start:	4 Jan 2013 - 02:04
Crawl end:	4 Jan 2013 - 04:51
Privilege starting points:	off
Co-link Analysis Mode:	page
Iterations:	2
Crawl Depth:	2
Node count:	93

Map generated from Issuecrawler.net by the Govcom.org Foundation, Amsterdam.

Legend:

(.org) (.be) (.it) (.org.uk) (.co.uk) (.ch) (.de) (.gov.uk)
(.com) (.nl) (.edu) (.dk) (.eu) (.eu.int) (.au) (.gov)
(.fi) (.int) (.parliament.uk) (.at)

Statistics:

aboutcookies.org

Destination URL:	http://www.aboutcookies.org/
Page date stamp:	4 Jan 2013 - 03:12
Links received from crawled population:	52

Links from network (1 - 20)

1. europa.eu
2. ico.gov.uk
3. ec.europa.eu
4. justice.gov.uk
5. hrw.org
6. bbc.co.uk

Links to network: 0

There are also clues emerging as to where bridges are beginning to be made to the wider network. The next step to furthering our understanding of the core of the network is to examine it in light of other measures of importance. Figure 3 below is the same snapshot of the network – January 4th 2013 – but with the nodes scaled by *both* in-degree and out-degree. The result is that rather than the attention paid to an actor being the decisive factor by which its importance is categorised, their linking to other nodes is also taken into account. Larger nodes in Figure 3, therefore, indicate those nodes who both give and receive a high number of links. This is important as we can begin to think about the flow of information around the network.

Examining Figure 3, EDRi and EPIC both remain two of the most prominent nodes. This tells us that the frequency with which they link to others does not diminish the established importance of receiving a large number of links – which *is* the case for Privacy International and the EFF. In their place, other key nodes now emerge. GILC and EFFI are both visibly more prominent, a change that is the result of a higher frequency of linking to others as opposed to receiving links. This indicates the relevance of reciprocity as a structural network characteristic. Other networks produced during the time-scale of the research demonstrated similar patterns.

Table 1 summarises the most prominent nodes in this network according to in-degree, out-degree and degree (the sum of the previous two). EPIC, for instance, receives links from 40 distinct websites and links out to 13. The figures demonstrate the point made previously; EFFI and GILC receive only nine and eight links respectively yet link out to 43 and 35 websites. This suggests that the importance of an actor in the network cannot be solely attributed to how many links it receives from others. This runs parallel with the assumption of the purpose of a network of information politics; communication and transmission of information is the fundamental task at hand. The important nodes in the network are those who contribute to this aim.

TABLE 1: SUMMARY OF DEGREE OF NODES

Organisation	*In-Degree*	*Out-Degree*	*Sum (Degree)*	*Total links received*[112]
EPIC	40	13	53	238
EFFI	9	43	52	275
EDRi	20	28	48	2,319
GILC	8	35	43	312
ORG	8	24	32	94
IP Justice	5	27	32	18
La Quadrature	5	24	29	151
Privacy Int.	19	0	19	592
EFF	18	0	18	418

Until now, one advocacy group in particular has escaped attention. The Open Rights Group[113] (ORG) is not situated within the core of the network in Figures 2 and 3 and nor does it ever appear as such in other networks. The same can be said of other advocates such as Statewatch[114], No2ID[115] and Liberty[116]. The next step in identifying key nodes therefore is to examine measures of Eigenvector and Betweenness centrality.

5.3.2 THE CORE – EIGENVECTOR AND BETWEENNESS CENTRALITY

Using *Gephi*, it was possible to visualise the above networks using the metrics of Eigenvector and Betweenness centrality. Figure 4 is drawn from the same data as Figures 2 and 3 (4th January 2013). This time, the nodes are scaled and coloured according to Eigenvector and Betweenness centrality respectively; the *larger* the node the higher the ranking for Eigenvector centrality and the *bluer* the node (on a scale from red to blue) the higher the ranking for Betweenness centrality.

[112] This refers to the total number of actual hyperlinks made to the website in question from the entire network.
[113] openrightsgroup.org
[114] statewatch.org
[115] no2id.net
[116] liberty-human-rights.org.uk

TABLE 2: NODE RANKS: EIGENVECTOR/BETWEENNESS CENTRALITY (4TH JAN 2013)

Eigenvector Centrality		Betweenness Centrality	
Actor	*Value*	*Actor*	*Value*
EDRi	1	**EPIC**	1037.094
Privacy International	0.977	**EDRi**	963.161
EFF	0.859	**ICO**	664.276
Chaos Computer Club	0.685	**ORG**	614.504
Twitter	0.613	**EFFI**	487.823

It is immediately noticeable that EPIC and EDRi are the two most prominent nodes in terms of Betweenness centrality, while the Information Commissioner's Office[117] (ICO), the ORG and EFFI also rank highly in this respect. For Eigenvector centrality, EDRi is once again prominent, closely followed by Privacy International, the CCC, the EFF and Twitter. Table 2 summarises the values for each of these.

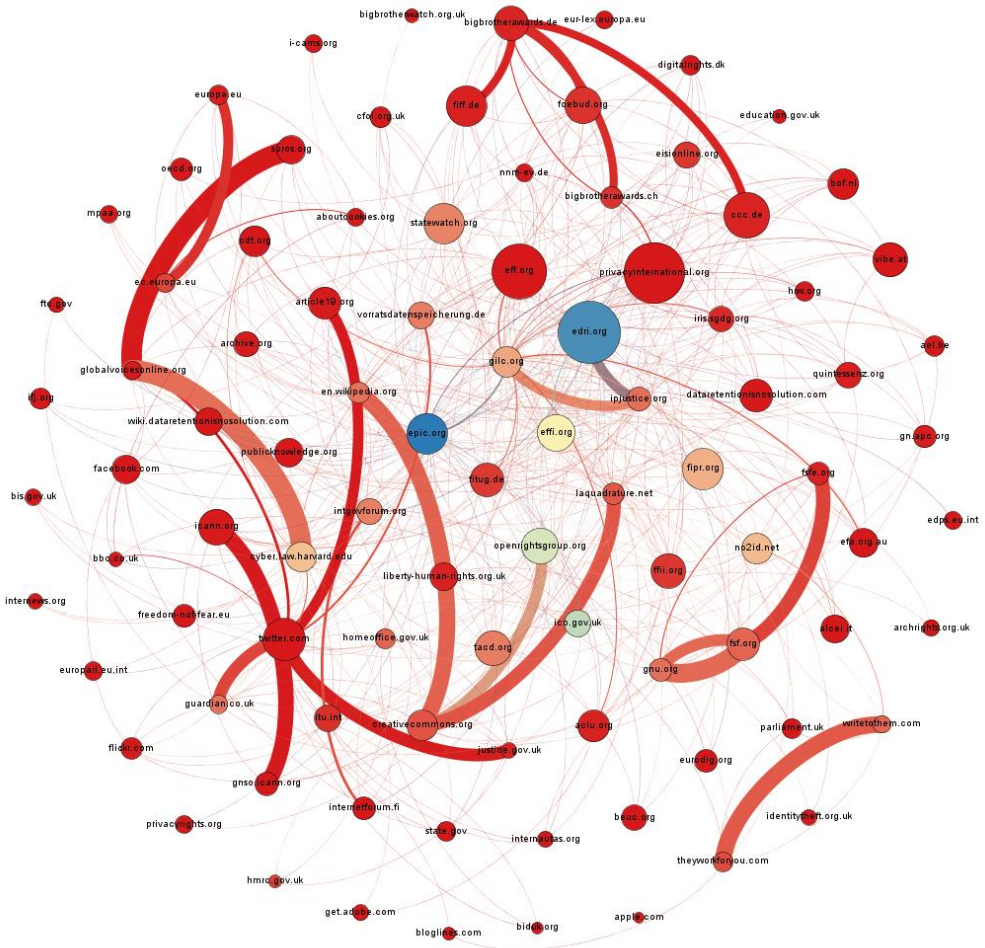
The patterns observed here remain relatively constant across all networks produced in the three-month period. For reference, Figure 5 below is drawn from network data on the 28th February. As can be seen, the key nodes remain the same – if only with a slight variation in relative importance[118].

In addition to the size and colour of nodes, the links between them ('edges') are also weighted in Figure 4. The thicker the edge, the more links exist. The colour of the edge indicates the predominant source of those links. In this instance, there are a large number of links to Twitter from several sites. However, this does not cause Twitter to rank highest for Eigenvector centrality as none of the nodes linking to it are themselves linked to by many important nodes. The most important nodes in this regard, EDRi and Privacy International receive links from (amongst others) similarly frequently linked-to nodes such as EPIC and the EFF.

[117] ico.gov.uk

[118] Changes in the network over time are addressed in more detail in section 5.6.

FIGURE 4: EIGENVECTOR AND BETWEENNESS CENTRALITY (4th JAN 2013)



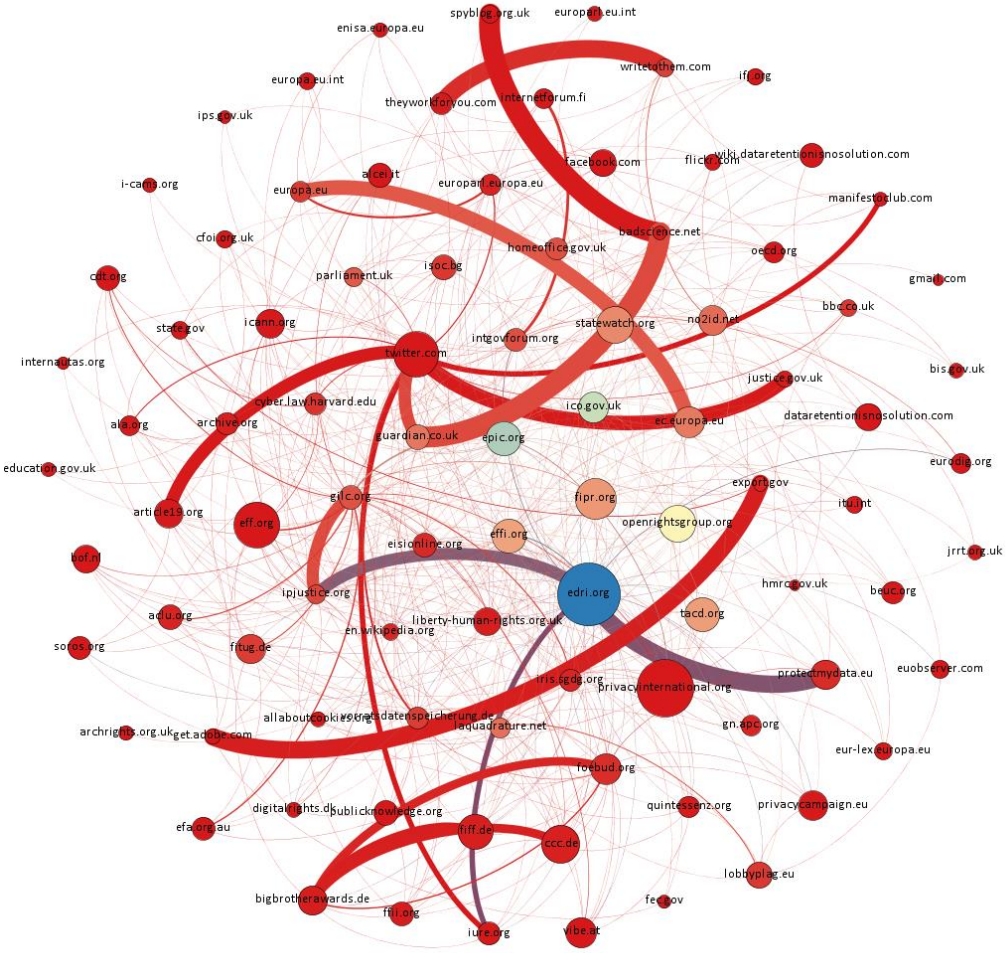
Although informative, it is easy to become too immersed in these figures obscuring the key findings from this network. What we can confidently state is that the most important nodes in the network – those whom attention is paid to the most both directly and indirectly – are advocacy groups with the shared mentality of promoting privacy and the protection of rights in a digital context. The core of this network is constituted primarily of these organisations. An Internet user browsing for information pertaining to these topics is highly likely to end up at one of these websites by virtue of their linking practices.

In terms of nodal governance, we can take the analysis one step further. While the dense core signifies a degree of (online) cooperation between those advocacy groups, the presence of other counter-surveillance groups outside of the core also needs to be accounted for. Being excluded from the core (whether intentionally or

not) is a form of competition as insofar as peripheral nodes will not be easily accessible to Internet users browsing the counter-surveillance community. Alternatively, this may signal a difference in mentalities or technologies of the groups. Take Liberty, for instance, which is situated outside of the core. While the organisation has been involved with campaigns to protect privacy, they are a more broad-based human rights organisation. Counter-surveillance is one of several mentalities that characterise the organisation. It may also be the case that Liberty places less emphasis on its online presence (one of several possible technologies that may be employed) than organisations in the core, which likewise may be oriented more specifically around issues related to digital surveillance. Bennett's (2008) distinction between 'privacy-centric' and 'privacy-marginal' organisations draws attention to the same issues. For Bennett it is their relation to the guiding concept of privacy that define their position. The network diagrams, therefore, may be providing a similar insight into the way in which the various organisations prioritise online connectivity as a technology that allows them to mobilise resources for resisting surveillance.

With this said, the core is not the sole area of importance of this network; there are sub-communities and other nodes to identify as the previous points make clear. Examining the 'connective structures' (Diani 1995, in Tarrow 1998: 124) linking the core and periphery assists with this. We can therefore move out towards the periphery via bridging nodes that have already begun to be identified. The measure for Betweenness centrality points us in the direction of these; beyond the core nodes, those important for relaying information are the Open Rights Group and the Information Commissioner's Office.

FIGURE 5: EIGENVECTOR AND BETWEENNESS CENTRALITY (28TH FEB 2013)



5.3.3 BRIDGING NODES

Several recurrently appearing nodes in the network never occupy a position close to the core but neither are they of little enough importance to be relegated to the periphery. Instead, they are located in an intermediate zone between the advocate community and other sub-groups of the network, an area overlooked in previous research. This area of the network is much less dense than the core but contains several nodes whose role appears to be to act as a bridge between communities (specifically between the advocacy community and other sub-groups). Bridging nodes might operate in two ways. First, for joining together otherwise disconnected sub-groups with similar mentalities. Second, as intermediaries between privacy

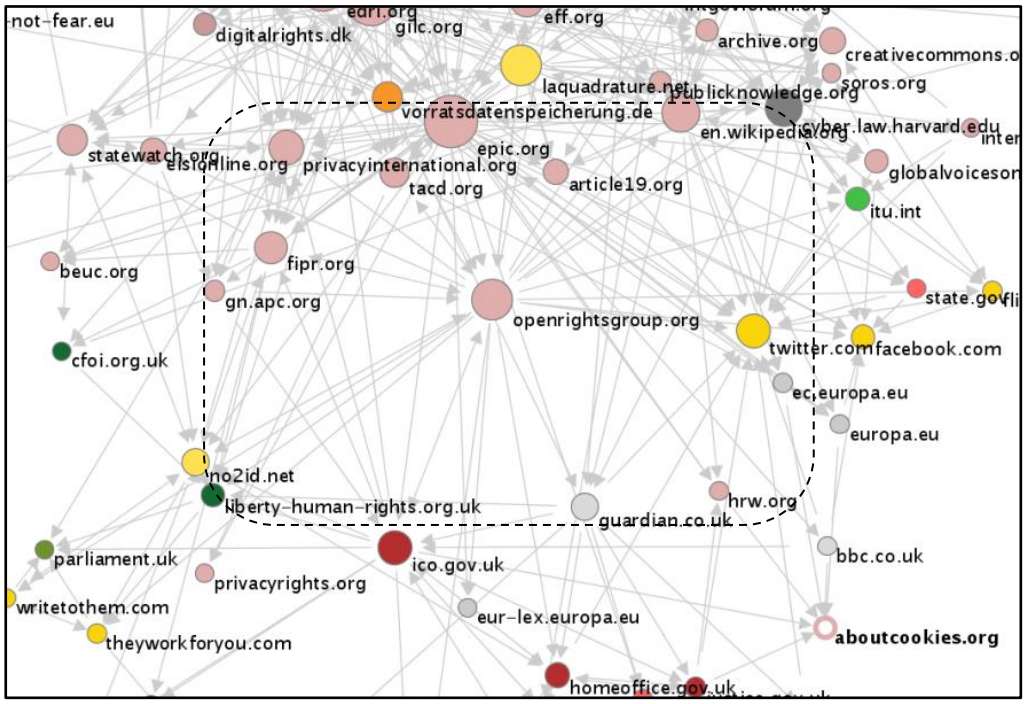
advocates and, for example, public sector organisations able to translate issues of concern into different policy or legislative contexts.

The first of these bridges, the ORG, appears at a key juncture between the core and the UK (quasi)governmental websites such as the Home Office, the Ministry of Justice and Parliament. As previously noted, the ORG is an important node in terms of Betweenness centrality and this is evident from its positioning. It receives links from some of the key advocates in the core including EFFI and EDRi and in linking out, connects not only to advocates in and outside of the core but to social media, governmental nodes, policy advisory bodies and websites aiming to promote democratic accountability and participation. In short, all of these are potentially useful nodes for engaging in information politics. What makes the ORG stand out is this ability to establish lines of communication between different sub-groups and the advocacy-centric core.

While the ORG ranks behind EDRi and EPIC for Betweenness centrality[119], of these EDRi is located at a different intersection with a European sub-group[120] and EPIC is not much more important in terms of Eigenvector centrality (suggesting it does not receive a disproportionate amount of attention to direct elsewhere). Consequently, the ORG serves a useful role in the network as an intermediary. Of note, this role, revealed by the network analysis, was reiterated by the representative from the ORG in interview. In the earlier extract he talks of ORG's current role as 'co-ordinating civil society'. The context of this conversation was the campaign against the Communications Data Bill[121]. This interesting parallel indicates that, at least temporarily, seemingly cooperative patterns of online organisation are reflected offline.

[119] See Table 2.
[120] See section 5.5.
[121] See Chapter Six.

FIGURE 6: SECTION OF FIGURE 4 (4TH JAN 2013) AS INTERMEDIATE ZONE



In a similar fashion, the ICO is located one step further across this divide. As Table 2 indicates, it ranks highly for Betweenness centrality. This is due to the links it makes possible for the network to and from several UK governmental bodies including HM Revenue and Customs, the Ministry of Justice and the Department for Education. It also receives links from news media groups *The Guardian* and the BBC. Although the ICO links *to* fewer nodes than the ORG (both receive the same number of links), it ranks higher for Betweenness centrality by virtue of the fact that its position enables transmission of some information to the core of the network that otherwise would be less immediately accessible. In network terms, it decreases the degree of separation between some peripheral nodes and the core.

The final node of interest in this intermediate area of the network is the Foundation for Information Policy Research[122] (FIPR), situated in Figures 3 and 6 to the left of the ORG. The FIPR ranks more highly than both the ORG and the ICO for Eigenvector

[122] fipr.org

centrality and eighth for Betweenness centrality. Examining its in- and out-links shows it is primarily a hub for several marginal advocacy groups (including Liberty, discussed earlier, and No2ID) and the core, fulfilling a similar function for these as the ICO does for the UK governmental nodes. Interestingly, the ORG, the ICO and the FIPR form a reciprocal triangle, each linking to the other two. This reciprocity appears to reinforce the importance of each of these three nodes in bridging the divide between the core and various peripheral sub-groups in the network. Without these nodes, interaction between the core and areas of the periphery would either be limited or non-existent. Before we turn to examine one sub-group in particular there is a final (and vital) node to discuss; a newcomer to the community since previous research – social media/micro-blogging website Twitter.

5.4 #FOLLOWUS ON TWITTER

The importance of Twitter in the networks is based primarily on its in-degree but also, as indicated by Figures 4, 5 and Table 2, its Eigenvector centrality. Although Twitter only receives links from 18 nodes in the network (fewer than others) its rank for Eigenvector centrality is due to the fact that several of these come from important nodes: EPIC and La Quadrature du Net in the core and the ORG as identified above. Connections also exist to news media groups, government bodies in the UK and US and academic nodes. Where Twitter stands out from other nodes is in the *volume* of individual links (i.e. the total of all links found within each webpage) received from the network. Over the course of the research, on average, Twitter received 2,405 in-links from separate pages and 25,968 individual links. This is compared to an average of only 512 in-links from pages and 2,432 individual links for core advocate EDRi. It is this which places Twitter at the top of every table for in-degree across all networks produced. In contrast to Twitter's in-degree, its out-degree is virtually non-existent according to *Issue Crawler*[123].

Twitter can be considered as akin to the public agora. Characteristic of Web 2.0 technology, production of its content is democratised (user-generated) and is

[123] This is a methodological issue. As a discrete website, Twitter does not link out to other websites. Individual tweets may contain URLs/hyperlinks but *Issue Crawler* cannot detect these. Similarly, *Issue Crawler* misses some of the links sent to Twitter due to the layout of some websites but regardless of this, the fact it remains the highest ranking node for in-degree illustrates its prominence.

generated on an enormous scale; in March 2012 an estimated 340 million tweets were sent every day (Twitter 2012). Moreover, the 'friendship' structure of Twitter is more open than its social media contemporaries Facebook and MySpace where both parties must enter into connections. In the context of understanding how the network fosters communication about current surveillance issues, it is unsurprising that the world's most prominent micro-blogging forum is the most frequently linked to node in the network. Advocate groups know they have an audience on Twitter and that it is easier to interact informally with other organisations via this medium. Both of these are important aspects to consider. In the context of nodal governance, Twitter adds a different dimension. Its presence in the network is not as a governing node *per se*. Twitter (as an organisation) *is* a governing node and will at times use its influence to direct policy or debate about online communication. However, in this instance, Twitter is a location for other nodes to come together and interact with one another (through discursive cooperation and competition) and with members of the public whom they seek to mobilise and recruit. In this sense, Twitter may be understood as a 'superstructural' node (Burris *et al.* 2005) wherein resources and efforts are combined. This idea is returned to later, as the presence of superstructural nodes is important for nodal governance and can be applied to this network in more than one way.

These beneficial aspects of Web 2.0 environments for advocacy groups could be expected to skew the visualised network structure towards the participation and engagement-friendly space of Twitter. On the one hand, this can be controlled for by viewing importance in the network based on other metrics already discussed above. On the other hand, it does not necessarily need to be controlled for in the first place. As the observations thus far have shown, the core is not resultantly re-oriented around Twitter. The advocate groups dominate this area, while Twitter is found in the intermediate zone (although not serving the same purpose as the bridging nodes already identified). Reintroducing the theme of competition and cooperation, what the frequency of linking to Twitter may indicate is recognition of the utility of Twitter for promoting discussion of important issues and maintaining 'sustained relations' (Tarrow 1998: 124) with opponents or collaborators. Both interviewees from the advocacy groups acknowledged the value of Twitter for these purposes.

> '…it is just essential in quite quickly helping us reach people with details of what we're doing…more broadly it's important for us to be in a particular debate or be visible to our supporters and realise we are doing something…So I guess it has two uses, it sort of helps us exploit and utilise our network…to help our supporters take action…and secondly it helps us build our reputation and presence in the debate' (Pete Bradwell, ORG).

Eric King (Privacy International) noted the same, although he also suggested Twitter suited some purposes more than others:

> '…for policy engagement social media is not the appropriate tool but for broad public outreach or communicating our goals, what we've been doing, it certainly is.'

Bruns *et al.* (2010) has examined the effect of social media – particularly Twitter – on participation in democratic political life. He describes a theoretical move from a singular public sphere – 'a universally accessible space where informed citizens engage in the political process' – to multiple 'publics' (2010: 9). These publics are 'constituted via communication' and illustrate how the new dynamics of social media interact with existing forms of rational critical debate. Within this new communication environment the coincidence of mundane interpersonal communication and moments of shared public anxiety allow advocacy groups to direct their efforts in a much more individualised way. Bennett (2012) calls this the 'personalization of politics': a broader trend of the mobilisation of individuals around lifestyle values to engage with a range of social causes. Resistance against surveillance is only one of these observable causes on social media but it is one that privacy advocates, by their equally visible presence, are actively generating and sustaining.

The lone point represented by Twitter in the network diagrams undermines its significance in the current context of collective action. We have begun to understand the nodal characteristics of the broader advocacy network but we must also be aware that within this network – and connecting it to other similar communities of information – is another domain entirely; social media forums like Twitter that are increasingly vital resources for advocacy groups in their efforts to mobilise a diverse range of *publics* against surveillance in its many forms[124]. A brief

[124] The rapid and widespread mobilisation of publics can be seen in examples such as the 'No Make-Up Selfie' and the 'ALS Ice Bucket Challenge' in 2014. These viral campaigns are often short-lived but are effective in engendering mass awareness and participation in a variety of social or charitable causes.

analysis of organisation on Twitter helps to clarify these points and elaborates how governing nodes can execute their functions.

5.4.1 WHO FOLLOWS WHOM?

Figure 7 was produced using *NodeXL*. The entire group of followers for No2ID was collected and filtered[125] to produce the network diagram above. The size of the nodes indicates Betweenness centrality. The larger the node, the more they drew others into *NodeXL's* network[126]. Although a little messy, the density of edges within the network indicates a high degree of connectivity between the nodes (following one another). A clustering algorithm grouped the followers into three communities according to their connectivity to one another. There is some overlap between these clusters but the general trends are as follows: the red nodes primarily consist of privacy advocates and activists; the yellow are mainly affiliated to a political party or are political bloggers; green can be described as left wing/anti-establishment figures[127] and; media groups are dispersed across all three categories.

While this is a microscopic perspective on the nature of the advocacy community on Twitter it does reveal several points of interest. First, some of the most prominent nodes are advocates who also feature in the wider hyperlink community: Privacy International, the ORG and Big Brother Watch. Organisational patterns are thus repeated to some extent. However, there is a stronger UK-bias to this network that is not as evident from the hyperlink analysis. This could be explained by the fact that No2ID was positioned in the previous networks away from the core that was characterised by trans-national connections[128].

Campaigns for digital issues have been less prominent but operate on the same basis; many supporters of net neutrality, for instance, changed profile pictures to a symbolic 'loading' graphic in mid-2014.

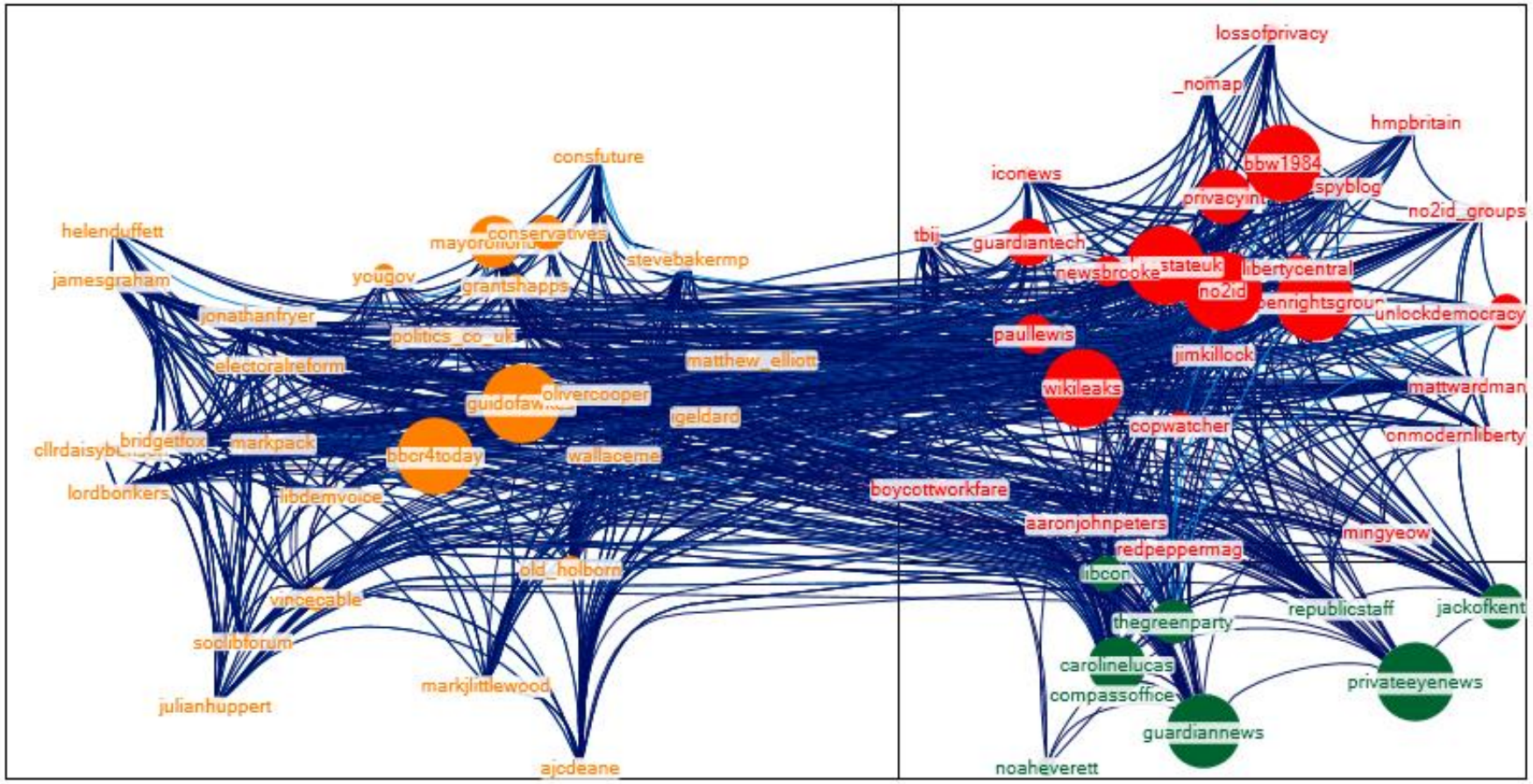
[125] 15th March 2012. UK-based advocacy organisation No2ID was selected out of necessity as their total number of followers was relatively small (~1,500) which reduced the burden on *NodeXL*. To reduce the network noise, No2ID's followers were filtered so that only those with over 100 followers of their own were shown.

[126] See Appendix C for a tabulation of all 64 actors in the network with Betweenness centrality metrics.

[127] This is true in general of the nature of the whole network yet it is interesting that NodeXL identified patterns of connectivity among these actors in particular.

[128] See section 5.5 for more on this theme.

FIGURE 7: A SELECTION OF TWITTER FOLLOWERS FOR 'NO2ID'



Second, many new nodes are revealed. Most commonly this is a result of their lack of a website presence to be captured by hyperlink analysis. Their presence here, however, does indicate potential importance, particularly for those ranking higher for Betweenness centrality: 'paullewis', 'guidofawkes', 'policestateuk' and 'wikileaks'. Third (resulting from this), we see WikiLeaks as the most important actor after No2ID. With 2.37 million followers[129] this is unsurprising yet it also foregrounds the necessity of including WikiLeaks in our conception of the online advocacy community. Despite such prominence on Twitter, they rarely appear in any significant way in the hyperlink networks. This could indicate a lack of recognition from the rest of the community – perhaps a desire to avoid association– or the desire of WikiLeaks to 'go it alone'[130]. Their organisational tactics, shown on Twitter, would support this claim; they do not follow anybody, opting instead only to receive attention rather than directing theirs elsewhere.

Three findings can be derived from this analysis. First, Twitter is an important digital domain for resistance activity in its own right for the advocacy community. It allows for a form of 'connective action' based on communication and individual-level content sharing (see Bennett and Segerberg 2012). Second, Twitter is an intrinsic part of the online network of privacy advocates. It is the most frequently linked-to website in the community and, while its position in the network is not that revealing, the interaction that takes place within this node situates it as an indispensable sub-domain. Third, the examination of Twitter raises a question of the organisational characteristics of the network. The insights from Bruns *et al.* (2010) and Bennett (2012) suggest that the character of an advocacy network resisting surveillance would be less fixed and more fluid and responsive – aspects that are re-examined below in regard to change in the network over time. While the hyperlink networks (at the level of organisations) remained stable over time, we can anticipate that social media networks (on an individual/interactional level) will, by their nature, only expand. In addition, we can see how Twitter adds a *social* dimension to the network, which augments the established *advocacy* network (Tarrow 1998).

[129] As of September 2014.
[130] See Chapter Seven.

5.5 PHYSICAL AND VIRTUAL GEOGRAPHY

Three aspects of the online network of the advocacy community have been examined: the core, bridges and social media (predominated by Twitter). The presence has also been identified of some minor sub-groups to which links are made: UK government nodes and broader civil society nodes. However, the most prominent sub-group that appears consistently is one situated near to the core. Given the nature of the groups that populate it (predominantly privacy advocates) this sub-group may be more appropriately termed a sub-core.

The four most prominent nodes in this group are:

- The Chaos Computer Club, German computer science and advocacy organisation;
- Informatics Centre for Peace and Social Responsibility, German advocacy organisation campaigning for data protection;
- Digital Courage Association[131], German civil rights and privacy advocacy organisation; and
- Big Brother Awards[132], German-based version of a joint initiative between various advocacy groups giving annual 'awards' to government and corporate organisations responsible for infringing privacy rights.

These nodes are not only prominent in their sub-group but also rank alongside or above several other key advocates in terms of Eigenvector centrality. There is also a high frequency of linking (high density) within this group. Across all networks produced, the CCC consistently ranks closely behind EDRi and the EFF in the top ten nodes for in-degree.

Clearly, these are important nodes in their own right, although their prominence raises an interesting point: all are German organisations. As Figures 2 and 3 demonstrate, these groups are situated close to the core of the network, hence the designation of 'sub-core'. Many of the German and other European organisations in the network are clustered together here, suggesting mutual support between the continental European groups. This issue of considering physical as well as virtual

[131] foebud.org
[132] bigbrotherawards.de

geography is significant. Introna and Gibbons (2009: 247-8) suggested a western bias in the network and this is reflected in the data here; the core primarily consists of UK and US organisations. However, the continental European bias in the network was not as apparent in their research.

Introna and Gibbons (2009: 247) also suggest the dense structure of the sub-core could be a result of language – websites linking to one another more frequently as a result of a shared language other than English. With that said, we should also note that some of the core nodes are non-English speaking as well. Consequently, the prominence of this sub-network raises a different issue. At play here is the influence of a shared history amongst some continental European countries of intensive state surveillance during the late 20th century. Public consciousness of surveillance or the digital/privacy rights of citizens is arguably greater in these countries[133]. The data are in keeping with this belief; when it comes to where attention is commonly directed in the network, the German organisations by and large are more prominent than other advocacy groups. Related to this, we should be aware of potential differences between countries in Internet use (particularly regarding social media). Findings from a survey conducted by the Pew Research Centre (2012: 1) indicate that 54% of Britons use social media compared to 40% in Poland, 39% in France and 34% in Germany[134] (2012: 4). However, of those using social media, similar proportions in Britain and Germany used social media for sharing views about 'politics'. A wider lens shows that using social media to discuss political opinions is far more common in Arabic countries, such as Lebanon, Tunisia and Egypt (2012: 4). These findings reinforce the need to remain aware of the links between Internet use, the history of and attitudes to surveillance as well as different appetites for regulation (see Vogel 2012) in different national contexts[135].

Elsewhere, we can see evidence of national and trans-national connections being played out in the network. The UK governmental nodes cluster together, as do the US governmental nodes when they appear in the network. The core, on the other hand, is more transnational, drawing in nodes from the UK, France, the US and

[133] In Germany a strong state-based foundation for individual privacy rights – the *Grundrechte* – has helped a strong network of privacy advocates to develop.
[134] Sample size approximately 1,000 per country.
[135] Also, see Chapter Six.

Germany. This raises the question of resistance to surveillance requires transnational organisation to be effective? It also signifies that to understand resistance to surveillance using nodal governance theory, we need to frame the issue globally at the same time as appreciating how the relationship between tht wo is played out at the national and local levels. The nature of linking within the core would suggest that the most important nodes in the network do bridge national divides. The reason the German organisations are both located close to the core and clustered tightly together could be that the geo-historical context for pro-privacy/anti-surveillance in Germany is stronger than elsewhere. We can infer, therefore, that advocates that find themselves outside of the core are likely to have stronger *intra-national* connections and this does seem to be the case with No2ID and Liberty in Figures 2 and 3.

5.6 CHANGES OVER TIME

The analysis has so far examined to what extent density, stability and reciprocity may contribute to an effective environment for 'information politics' as a form of resistance to surveillance. Each has been evidenced to some extent, particularly in the core of the network. Here, there is a high degree of reciprocal interlinking and there is very little change in the nodes present over time – those in the core and the sub-core are *always* present in those areas. As also indicated, the linking practices of the core can affect changes in the periphery. The bridging nodes identified earlier illustrate how this occurs in this specific network. Drawing on lessons from nodal governance has also helped to suggest why this may be. However, the peripheral nodes referred to so far rarely feature in any way in the network beyond that of marginality. Nevertheless, there are other nodes whose presence in the network does fluctuate more significantly over time and who are resultantly drawn closer towards the core.

Using *Issue Crawler* a tabulated series of outputs allows us to observe changes in in-degree over time[136]. Specific data were drawn out that showed noticeable changes

[136] In-degree in this instance was based on the number of links received from separate pages as opposed to websites as in Table 1. This method was chosen as it demonstrated fluctuations most clearly. Using this alternative measure *does not* create fluctuations where none exist; it merely makes them more visible.

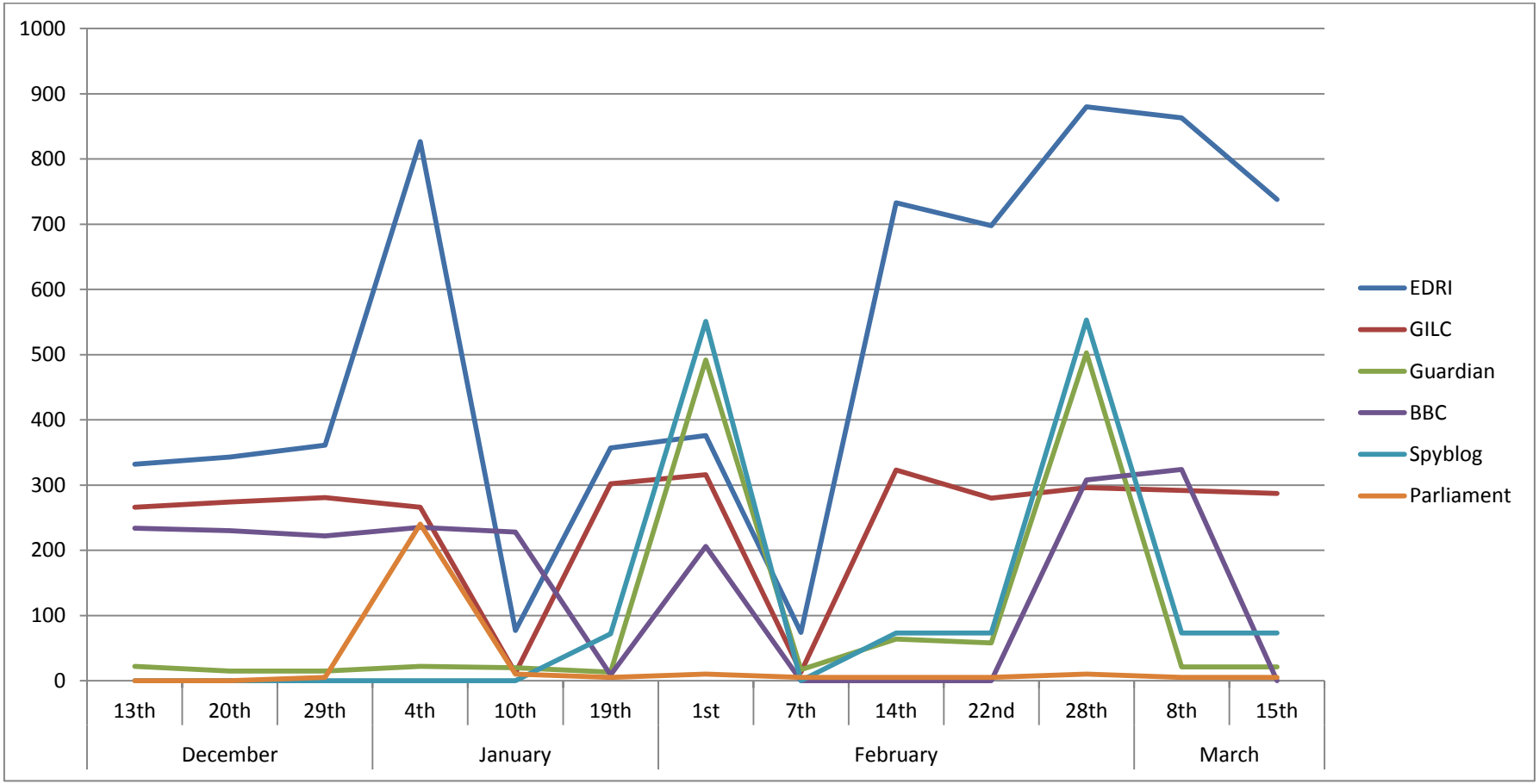
in in-degree for several nodes. The results, in graphical form, are displayed below in Figure 8[137]. The four nodes of interest are news media organisations *The Guardian* and *BBC News*, Spy Blog (a website providing commentary on current surveillance trends and privacy issues) and Parliament.uk (the official website of the House of Commons).

Beginning with the most prominent changes, EDRi varies between receiving 880 and 74 links. As we know it is one of the most important nodes in the network. This variation would suggest a dip in such centrality on the 10th January and 7th February. However, when we observe the data for GILC we can see it follows a similar pattern, albeit with a lower in-degree in general. This pattern was similar for the majority of key nodes in the network. On those dates, for whatever the reason may be, there fewer links in the network as a whole rather than fewer links being directed only to EDRi and GILC.

In contrast to this, the UK Parliament website has only one sudden increase in in-degree on the 4th January, while for the remainder of the research period it remains firmly in the periphery. Inspecting the source file for the network on this date reveals that the large majority of these links directed to summaries of written and oral evidence given to a Select Committee in 2004 responsible for scrutinising the Identity Cards Bill and to a similar process of review for the Identity Documents Bill 2010 which eventually repealed the previous Act. The links directing to these originated from human rights organisation Liberty. What is unclear, unfortunately, is why these links were only revealed in January 2013, more than two years after the Identity Documents Bill was passed into law. Regardless of this, what this case does highlight is the importance that such linking can have for the network. Evidently, as of the 4th January 2013, information was made more easily accessible concerning identity card legislation in the UK.

[137] For comparative purposes – and because they too fluctuate – data for core actors EDRi and GILC were also included.

FIGURE 8: GRAPH SHOWING CHANGES OVER TIME IN IN-DEGREE OF SIX NODES



The two other most apparent spikes in prominence by in-degree are almost mirror images of one another. *The Guardian* and Spy Blog both demonstrate large increases in in-degree on the 1st and 28th February 2013. The only real difference between the two is that *The Guardian* is always present in the network whereas Spy Blog does not appear until 10th January. This is a pertinent point in its own right, and is reflected in the anlaysis in Chapter Seven; the online presence of traditional media outlets helps them retain their power. It is to be expected that the closely matching fluctuations in in-degree could be attributed to the same sources – for instance the same newsworthy events relating to surveillance or privacy. Again browsing the source data revealed that on each of these dates there were a number of potentially relevant news stories published in *The Guardian* to which the increase in in-degree might allude. On the 1st February, stories were published in *The Guardian* concerning Chinese hacking of US companies (Arthur 2013) and Internet copyright (Doctorow 2013). On 28th February stories were found relating to the trial of alleged US military whistle-blower Bradley ing (Pilkington 2013a), the use of Twitter in North Korea (Lee 2013), a UK court order requiring several ISP's to block access to three popular file-sharing websites (O'Carroll 2013) and US defence firm Raytheon's release of R.I.O.T. – software that permits deep data mining of social media profiles (Ball *et al.* 2013). At the same time, there are also visible peaks in the in-degree of *BBC News*. Searches of the *BBC News* website revealed similar coverage of those stories covered by *The Guardian* and others including the dangers of wiretapping cloud computing systems on the 31st January (Wakefield 2013) and the value of virtual currency Bitcoin on the 28th February (BBC News 2013).

Identifying such events for Spy Blog proved less successful, despite its apparent concurrence with *The Guardian*. However, a large number of links to Spy Blog at this time originated from *Bad Science*, a blog interrogating government reports and scientific claims that was a new (but peripheral and infrequent) node in the network on the 1st February. This blog was also the source of some of the links to *The Guardian* at the time which may help to explain the congruence in Figure 8. The peak on the 28th February may be interpreted in similar terms given that both received links from Statewatch, an advocacy organisation monitoring civil liberties in Europe. The link to Spy Blog on this occasion appeared to be concerning the Draft Anti-Social Behaviour Bill from December 2012; Spy Blog's objection was that the

proposed legislation infringed civil rights through 'over-broad catch-all language' (Spy Blog 2013). *The Guardian* ran a story on the legislation just prior to this (Plant 2013).

Identifying and explaining these changes in the network over time is a useful final step in the network analysis of the privacy advocates. It further highlights the links between this online community and its real-world manifestation. We have already noted one such relationship regarding the German/European sub-group. Three of the nodes identified here – *The Guardian*, BBC News and Spy Blog – help to make another connection to real-world *events* and their potential to impact on the structure and stability of the network. Their fluctuating presence in the network is to some degree a sign of instability but it is in no way detrimental to the network – in fact it is quite the opposite. The presence of news media allows us to consider *responsiveness* of the network rather than stability. Much as for new social media outlets such as Twitter, the increased prevalence of linking to these news media nodes on occasion suggests recognition of the importance of these channels of communication on the part of the advocacy community. When it comes to information politics, these nodes could play a significant role in contributing to the goals of the community as a whole.

We could make two further assertions as to how this might occur. First, the positioning of *The Guardian* and *BBC News* is similar to that of the bridging nodes; they create connections between key advocate groups and (quasi)governmental bodies, including the ICO. Furthermore, as Figures 4 and 5 show there is a larger number of links between both of these groups and Twitter, signifying that the potential exists for widespread communication of relevant news stories (indeed, we need only personal experience of news on Twitter to know this is the case). Second, the readership of these groups (particularly *The Guardian*) is noteworthy. No other newspapers appear in the network. *The Guardian's* left-wing tendencies are likely to attract those readers whose sensibilities are more in tune with those of the advocacy community and therefore those who may be more likely to support and engage in resistance to surveillance. Questions regarding the role of news media and their potential to retain influence through an online presence are returned to in Chapter Seven.

5.7 SURVEILLANCE AND RESISTANCE PART 1: INFORMATION POLITICS AND NODAL GOVERNANCE

The final part of this chapter looks in more detail at what the theory of nodal governance has contributed to our understanding of resistance to surveillance in light of the analysis presented, as well as what lessons can still be drawn out in terms of how nodal governance is performedthroug online communities. Some themes have already been highlighted, in particular the idea of competition and cooperation within networks of governance. Others, like the concept of 'superstructural nodes' (Burris *et al.* 2005) warrant further attention.

5.7.1 SUPERSTRUCTURAL NODES

A superstructural node, according to Burris *et al.* (2005: 38) is one 'which brings together representatives of different nodal organizations…to concentrate the members' resources and technologies for a common purpose but without integrating the various networks.' What this signifies once again is a process of cooperation between nodes. To add to this, Wood and Shearing's (2007) observation that such cooperation may be temporary or more permanent is also important. The presence of superstructural nodes signals, in the case of resisting surveillance, joint efforts by advocacy groups that challenge certain surveillance practices. These do not undermine or replace the individual organisations' goals but instead indicates a 'strength in numbers' approach and the recognition that different mentalities and resources can be brought to bear on the issue in question. To understand what this means in practice, we can look at a two examples from the networks that have been explored in this chapter as well as one that emerged after the fieldwork.

Some of the key nodes identified earlier can be considered superstructural nodes. The European Digital Rights Initiative (EDRi) and the Global Internet Liberty Campaign (GILC) were both situated in the core of the network and are both constituted by a collection of other advocacy groups, many of whom also appear in

the network[138]. EDRi 'defends rights and freedoms in the digital environment' **(EDRi 2016)** and comprises 31 European organisations while GILC advocates a broad range of digital rights (including freedom from censorship and access to encryption of communication) and comprises 68 organisations from around the world **(GILC 2016)**. Both are long-term, formalised collaborations having been established in 2002 and 1996 respectively. While both exhibit the defining features of a superstructural node EDRi is more significant in the network according to measures of centrality and is a useful case in point. Governance of surveillance and security in the UK is increasingly a European-level issue, the product of negotiations between EU member states. For instance, as Chapter Two outlined, European law influences regulation of surveillance and Internet communication in the UK. Groups such as EDRi are therefore potentially very helpful for amplifying the voice that otherwise relatively small and nationally based organisations can have in the supra-national arena. In the language of nodal governance each member of EDRi will have their own resources and technologies to draw on for the benefit of the wider group. These may take the form of established connections to government agencies and policymakers, member bases and links to other civil society or activist networks. It is illuminating (and validating for the method) that the network analysis here reveals the significance of superstructural nodes based on prevalence of hyperlinking.

Another superstructural node emerged in 2013, after this stage of the fieldwork had concluded. Don't Spy On Us[139] is a coalition of advocacy groups that came together in the wake of Edward Snowden's revelations. They have since campaigned against mass surveillance in the UK including challenging the Investigatory Powers Bill in 2016, of which the Communication Data Bill in Chapter Six was a precursor. Its founding members are six UK-based organisations[140]. A further twelve affiliates[141] come from the UK and elsewhere. While it does not feature in the networks, this coalition illustrates the continued desire within the community to cooperate through sharing resources and technologies. The example of Don't Spy On Us

[138] See Appendix G for the list of featured advocacy groups. The entries for EDRi and GILC detail their member organisations.
[139] https://www.dontspyonus.org.uk
[140] Article 19, Big Brother Watch, English PEN, Liberty, Open Rights Group and Privacy International.
[141] Access Now, Amnesty, Centre for Investigative Journalism, Electronic Frontier Foundation, Fight for the Future, ifex, Index on Censorship, Open Democracy, Open Media, Public Concern at Work, Sum of Us and the World Wide Web Foundation.

illustrates the existence of a superstructural node whose mentality is oriented solely towards mass surveillance and whose resistive efforts have to date been mainly located in the UK. In comparison, EDRi addresses a wider variety of digital rights issues.

Superstructural nodes, then, allow mobilisation against different problems by adopting a cooperative approach. Whether such coalitions are the 'command centers' (Burris *et al.* 2005: 38) of resistance to digital surveillance is less certain. It is reasonable to say, given the analysis here, that they do play a significant role in the online community at least. Their centrality makes them effective at a particular brand of resistance, namely 'information politics'. Yet there are other forms of resistance. Activism, hacking, whistleblowing and encryption are all other ways that surveillance can be resisted. However narrowly or broadly we may want to conceptualise superstructural nodes, we might then also designate the entire privacy advocacy community as a superstructural node that is part of a wider civil society network, albeit one with looser organisation as geography and mentalities become more dispersed. Fewer or more nodes can be revealed in our observations 'depending of the level of aggregation and disaggregation in the analysis' (Burris *et al.* 2005: 38). Likewise, it was also suggested earlier that Twitter may function in some respect as a superstructural node, given that it provides a space for communication and interaction between other nodes and another channel through which to practice information politics. All of this indicates that the organisation of resistance to digital surveillance happens at a global, national, local and hyperlocal (in the sense of tweeting) level. The fundamental factor is the network as a form of organisation that allows for flexibility and responsiveness as well as a degree of stability.

5.7.2 THE LANGUAGE OF CONNECTIVITY

The language of nodal governance is helpful for beginning to explore the relationship between surveillance and resistance. It will be clear to the reader that there is a significant amount of overlap with other ideas introduced in Chapter Three. Martin *et al.*'s (2009) 'multi-actor framework', Sharp *et al.*'s (2000) 'entanglements' of dominating and resisting power and Haggerty and Ericsson's

(2000) 'surveillant assemblage' all identify similar themes of plurality and connectivity that can be applied to understanding the interaction between surveillance and resistance. The value of nodal governance in particular is that it goes beyond simple network analysis by identifying the real and active institutions that compete and cooperate with one another in shaping debates and practices of digital surveillance.

The analysis in this chapter adds support to a number of claims made so far in the thesis. There is competition and cooperation (Wood and Shearing 2007; Fuchs 2008) within and between the various public, private and civil society entities that engage in surveillance and resistance. One way this has been envisioned is through measures of centrality in the hyperlink networks. Greater centrality can indicate both the desire to be 'seen' online (competition) and also the result of coalitions of organisations (cooperation). We also see that the Internet facilitates connectivity for the advocacy community – both between organisations websites and on social media – which may signal an escalation of 'resisting power' (Sharp *et al.* 2000) to counteract the 'dominating power' of public and private surveillance. There was also evidence that the global nature of digital surveillance and resistance in the information society was reflected in the network. By necessity, if the network of advocates is to be effective – as individual or cooperating governing nodes – it must be able to span national boundaries. The networks here indicate that this process is already in existence. However, one important barrier may be language. This may account for the apparent degree of introspection in the 'sub-core' but this may also be a product of a more hospitable civic setting for privacy advocacy in continental Europe.

The question that remains is whether the network of privacy advocates are effective governing nodes. In other words, are they successful in resisting surveillance? The findings have demonstrated that density, stability and reciprocity of the network – and later responsiveness – are evident and, as such, the online advocacy network is perhaps both a suitably structured environment and modality for resistance in the form of information politics. It is also apparent that this conglomeration is fluid and flexible. Furthermore, nodes are involved whose primary business is not to resist forms of surveillance.

Burris *et al.* (2005) note that nodal governance is typified in equal part by flexibility and reconstitution of networks as much as stability and planning. The network in this chapter needs to be adaptable and responsive to resist the various forms that digital surveillance can take. For the privacy advocacy community, the main tool at their disposal is information politics, which is aided by the practices seen here of connectivity and cooperation. Equally, each organisation has its own agenda and needs to compete for members, for funding and against other organisations that may try to advocate for greater surveillance powers. Their relative prominence in the networks fluctuates over time as new connections are made and real-time events are responded to. On occasion, significant 'surveillance events' can act as symbols[142] that allow for a coalescing effect; instances of unity and greater collaboration, or 'synthesis moments' (Della Porta 2008: 3), that create the opportunity for 'superstructural' nodes to emerge – such as Don't Spy On Us. This empirical exploration of networks and nodal governance has shown some of the ways in which these relationships can be understood and how resistance to surveillance must be approached with respect to networked forms of organisation, flexibility and adaptability.

5.7.3 CONCLUSION

The network analysis of the data in this chapter in tandem with the theory of nodal governance contributes to the thesis by illuminating some structural and interactional dimensions of the social organisation of resistance. Nodal governance alerts us to the multiplicity of institutions involved in guiding social affairs. This chapter offers support for this argument. Alongside the privacy advocates, the network incorporates key *non-advocate* nodes including the news media, regulatory agencies such as the ICO, policy advisory bodies such as the FIPR, organisations promoting libertarian ideologies such as Creative Commons and GNU and new social media forums like Twitter. Revealing and making sense of these interactions helps to develop our understanding of how resistance to surveillance is organised and is what this chapter has begun to achieve.

[142] See Chapter Seven.

The empirical data also aid in developing a critical understanding of the theory of nodal governance. Specifically, they have illustrated how these relationships can take shape *online*. In that respect, the identification of 'bridging nodes' adds a new dimension to nodal governance. These nodes (not solely privacy advocates) appear to have distinct functions in the network that may not simply be about pursuing their own objectives. Instead they facilitate connectivity between sectors with differing mentalities. This insight might be applied to other contexts for theorising nodal governance, particularly as it signals the potential for capitalising on the resources of other institutions.

Resistance, then, is dynamic, global and networked. There are shifting relationships within resistant communities but this arguably increases its effectiveness in resisting surveillance. The institutions within the community have varying mentalities, technologies and resources. The overall goal for many of the organisations present in this community is to raise awareness of, and to work for, a balance between liberty and security. This analysis contributes to knowledge on governance of security using the nodal governance framework by empirically and visually illustrating how networks of nodes who challenge the means of providing security are organised in online spaces. It furthers the work of the thesis by illustrating the online organisation of resistance on a broad scale – which is reflected in the physical world the organisations occupy. This first step is continued in Chapter Six where we see an attempt at digital surveillance reform and the mobilisation of resistant nodes (both from within the community examined here and beyond) that ensues.

--- -. -... . .... .- .-.. ..-. --- ..-. - ....-. ..- - ..- .-. . --..--

CHAPTER SIX

REGULATION OF SURVEILLANCE AS A SITE OF RESISTANCE

6.1 INTRODUCTION

Surveillance is one mode of social control and it interacts with other modes of control. Regulation – controlling and managing risk through the use of law (Innes 2003) – is one such modality. It attends to *process* (Innes 2014) rather than outcome, which is to say it dictates, by varying degrees of persuasion or coercion the way things should be carried out. Naturally, then, key aspects of regulation are compliance-seeking, bargaining and persuasion (Hutter 1988, 1997), as the various public and private entities involved negotiate their respective obligations. Regulation in the information society, as Chapter Two described, encompasses a broad array of social entities (or governing nodes) who are capable of, and responsible for, facilitating digital communication and collecting the data it generates. Consequently, digital surveillance and regulation are inseparable. Faced with the constant need to protect citizens from a range of online harms and terror attacks facilitated by digital communication tehcnologies, governments have actively pursued greater regulation of digital surveillance.

One such case, that exemplifies these broader patterns and trends, is the focus of this chapter – the Draft Communications Data Bill from 2012. One aim of this chapter, therefore, is to examine how legal frameworks have sought to regulate surveillance. The other, crucially, is how these have generated effects of resistance. The chapter therefore comprises two related themes. The first addresses research question two – 'why do individuals and groups who resist digital surveillance identify a need for doing so?' – by examining some of the key arguments made from a variety of standpoints against reform of surveillance legislation in the UK. Resistance in this context is also noteworthy because it represents an opportunity

for individuals and groups to have their concerns codified in law, even should regulation ultimately be passed.

The second theme contributes to the broader discussion around research question three, by illuminating the intersection between regulation and surveillance as modes of control. Examining the regulatory context of digital surveillance is valuable because it draws out a number of important facets of the relationship between digital surveillance and resistance. One of these is the role played by communications service providers (CSPs)[143]. These entities are powerful surveillance agents whose business models rely in large part on the collection and processing of data from customers and Internet users. Harvey Molotch has observed that '[a] bastion of modern security, domestic and foreign, is storing digital data on the lives, habits, and capacities of individuals and groups' (2012: 201). This chapter supports this claim, illustrating how current security measures aim to exploit CSPs through a process of *mediated* surveillance (Bright and Agustina 2013): recruiting and enlisting (typically through regulation) the surveillance capabilities of other actors. However, regulating CSPs (for the purposes of increased security) is hotly contested; these nodes emerge as equally 'resistive' as they are 'surveillant'.

Another dynamic the focus on regulation therefore draws out is the interaction, at a specific point in time, between various nodes with a stake in the governance of the information society. This chapter features some of the nodes from civil society that appeared previously, alongside government, law enforcement, private sector, technological expert and media nodes. The analysis in this chapter therefore attunes us to the negotiated character of this kind of control work (Innes 2003: 136) and therefore, by extension, of contemporary digital surveillance. The case study of regulation in this chapter illustrates these processes, emphasising the significant counter-arguments that were formulated against the necessity and proportionality of the proposed regulatory framework for digital surveillance.

[143] The term being used here to capture all private organisations that provide Internet connectivity as well as online products and services.

6.2 THE COMMUNICATIONS DATA BILL

The Communications Data Bill (CDB) in 2012 was, at the time, the latest attempt by the UK government to regulate in the area of investigation of communications data for the purposes of crime prevention. It sought to address a perceived 'capability gap' of UK law enforcement and intelligence agencies in light of rapidly changing communications technologies and services. Chiefly, it required CSPs to retain more data (i.e. data they did not routinely collect for business purposes) relating to their customers and their communications. Chapter Two[144] relays the recent history of such regulation in the UK and, where applicable, Europe. This is a helpful rehearsal what follows and highlights the key points that: (1) the CDB aimed to update the Regulation of Investigatory Powers Act (RIPA) 2000; (2) the *content* of digital communications has typically been afforded greater protection under surveillance legislation, and; (3) that data protection is a contentious issue at both the national and supra-national levels.

6.2.1 CONSULTATION ON THE COMMUNICATIONS DATA BILL

The CDB was announced in the Queen's Speech in May 2012, in order to 'maintain the ability of the law enforcement and intelligence agencies to access vital communications data' (HM The Queen). The Home Office produced the Bill in draft form for pre-legislative scrutiny. A Joint Committee of six members each from the House of Lords and the House of Commons was appointed to review the CDB in July 2012. A public consultation was issued and written evidence received from 145 respondents. Coupled with this, oral evidence sessions were held and testimonies received from 54 witnesses, both supporting and opposing the Bill. Finally, the Joint Committee visited the Metropolitan Police Central Intelligence Unit and UK network operator Everything Everywhere to observe the procedures for requesting and granting access to data (Joint Committee on the Draft Communications Data Bill 2012: 9-10). A final report was issued by the Joint Committee in December 2012, the main points of which are summarised below.

[144] Section 2.4.4

Drawing attention to the motivation underpinning the CDB, Charles Farr, Director General of the Office for Security and Counter-Terrorism stated in one evidence session to the Joint Committee, '[t]he central plank of this programme is a collaborative relationship with service providers in this country and overseas' (CDB Oral Evidence, p.19). Part One of the CDB was indicative of this[145]. The majority of attention was paid to Part One given that it was, according to one interviewee from the fieldwork,

> 'far too broadly defined in that it doesn't really specify at all the kind of information they want to get from who, about whom' (Pete Bradwell – Open Rights Group).

Importantly, as the analysis below also highlights, the CDB contained provisions to move beyond the scope of the EU Data Retention Directive and compel CSPs to retain data pertaining to third-party/overseas providers (such as Facebook or Google).

The final report of the Joint Committee acknowledged that there was a case for updating the legislation currently represented by RIPA. However, the verdict of the Joint Committee was that

> 'the draft Bill pays insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data' (Joint Committee on the Draft Communications Data Bill 2012: 3).

They also noted, as suggested above, that Part One would grant 'sweeping powers' and that 'potentially limitless categories of data' could be retained (2012: 3). In its current form the draft Bill was rejected on these and other grounds. The analysis that follows picks out some of the prominent themes that emerged from the evidence given to the Joint Committee. The story that develops throughout is one

[145] *Part One:* creates a new power to order CSPs to collect specific datasets, creating them if necessary, and deploying any technical or policy changes needed to do so. It also requires this data to be retained in a secure and confidential manner for 12 months, and destroyed after this period elapses. This power can be used by any principal secretary of state but in practice this would be the Home Secretary.
Part Two: creates a system for assorted public bodies to get access to this data, including 'filtering' arrangements, i.e. the process of querying databases owned/operated by CSPs that hold retained communications data.
Part Three: makes some changes to RIPA, repeals all other existing powers that involve retaining and disclosing "communications data", and makes the Information Commissioner, the Interception of Communications Commissioner, and the Investigatory Powers Tribunal responsible for scrutiny and oversight of the implementation of these powers (adapted from the Open Rights Group 2012).

of managing an uncertain, ambiguous and contested environment, particularly with respect to the relationship between the state and private sector.

6.2.2 WHO HAD A SAY?

Evidence was gathered by the Joint Committee in written and oral form. There was some degree of overlap between the two; some respondents who were interviewed by the Committee later submitted supplementary written evidence, whilst others who responded in writing were later invited to interview with a panel of others with similar expertise. This section briefly outlines a categorisation of the responses received. This categorisation is weaved into the subsequent analysis to illustrate the various contributions to the process of negotiation[146]. Given its larger scale, a categorisation was first developed from the written evidence. Initially respondents were placed in 11 categories, this being refined into a more coherent seven categories with appropriate sub-categories[147]. The result was as follows[148]:

TABLE 3: CATEGORISATION OF RESPONDENTS TO CONSULTATION

Category	Written Evidence	Oral Evidence	Total
Official *(*Government and Law Enforcement)	11	19	30
Independent Authorities	5	4	9
Telecoms Industry	11	13	24
Expert (Technical, Academic and Legal)	28	8	36
Advocacy/Non-Profit	16	8	24
Media	6	3	9
Individual/Non-Expert	68	-	68

[146] The category a respondent falls into is indicated in italics following any direct quotations used in the analysis.

[147] Naturally there is scope for interpretation here; some respondents could be placed in multiple categories. For instance, respondents from the 'Telecoms Industry' are likely to be experts in their field but it was felt that this warranted a category of its own given the subject matter.

[148] Numbers in parentheses indicate total number of respondents in each category from written evidence.

Categorising respondents in this way is helpful as it indicates the diversity of actors involved in negotiating the regulation. Surprisingly the number of 'individual/non-expert' respondents[149] was high. These are voices not typically heard in their own right; the accounts of advocacy groups are usually taken to be representative of the concerns of these individuals.

This initial breakdown indicates the sustained importance (from Chapter Five) of the advocacy community who, as might be expected, were vocal in their criticism of the Bill. Although they did not represent the largest proportion of respondents, the quantity of their contribution to the written evidence was substantial; 25% of the evidence submitted[150] compared to only 10% from official sources. This adds weight to the observation of Lord Carlile of Berriew that '[t]he narrative over these proposals has in my view been inadequate. There has been a much stronger counter-narrative…Government, or successive Governments could have told a much stronger story' (CDB Oral Evidence, p.298). However, the majority of oral evidence taken in interview by the Committee was from governmental or law enforcement representatives, which did provide some balance.

6.3 CENTRALISING AND DECENTRALISING IMPULSES

Some of the points raised so far indicate a theme that reoccurs throughout the remainder of this chapter, and the thesis. Centralising and decentralising tendencies are useful conceptual tools for thinking through not only trends in contemporary social control (revisited in Chapter Eight) but also patterns of governance, surveillance and resistance. This theme emerged from several of the interviews conducted during this research. These voices are introduced to the analysis at this stage. Three broad conceptualisations were identified throughout the analysis: centralisation versus decentralisation of Internet architecture; centralisation of information, and; centralisation/decentralisation as organisational principles[151]. These three are all related to an extent but each represents a particular concern that different participants held.

[149] These respondents had no professed expertise or loyalties but were nonetheless motivated to respond to the consultation.
[150] Figure is drawn from the total number of pages of evidence submitted and thus is only approximate.
[151] The latter is discussed in more detail in Chapter Seven.

The 'problem' of centralisation of Internet architecture is connected to the liberalism characteristic of many Internet activists, hackers, cypherpunks and advocacy groups. As Chapter Two described, the Internet was designed as a resilient network. Centralisation runs counter to this. One interviewee, Daniel – a co-founder of WikiLeaks – noted that decentralisation permitted the Internet to 'intelligently route around' any problems in the network. Speaking in more specific counter-surveillance terms, he also observed 'it can bypass censorship by design…that's what the Internet was built for.' Such is the attachment to the ideal of a decentralised, 'free' Internet that one cannot help but notice a nostalgic and quasi-utopian impulse in further remarks by Daniel and another interviewee, Joss.

> '… in the late 90s and early 2000s there was a real trend of…peer-to-peer networking, file sharing and there was this utopian vision at that point that we were going to do everything peer-to-peer and so it would remove centralised control and everything was going to be wonderful but there are…fundamental difficulties with the peer-to-peer approach and for convenience sake, centralisation is easier and it allows you to build things like Facebook.' (Joss Wright, OII)

> '…the great thing about the Internet is that there is no hierarchy in some sense…in the face of the Internet protocol men and women are created equal you know, it doesn't matter where you are, what your status is, how much you earn, if you're black, white or yellow or whatever, it doesn't matter if you are a man or a woman as long as you have an Internet protocol address and you're connected and you are the same as everybody else, you have the same potential for having a voice, you have the same say in the Internet you have the same possibilities to do something to consume to produce, whatever, and that is what this is about you know, this is a shift in paradigm for the future that if we don't take it then we're stuck with this old hierarchical stuff forever we have people ruling us and we're not all equal.' (Daniel Domscheit-Berg, OpenLeaks)

Two observations can be made from these remarks. First, based on Daniel's comments, decentralisation of Internet architecture is perceived as a mechanism to achieve equality on the Internet. Underlying this belief is the assumption that the Internet, as a communication medium, affords great potential for participation and democratisation (as Chapter Five has gone some way towards illustrating). Second, Joss' remarks direct us towards centralisation of information. The shift away from peer-to-peer networking in the early 1990s is represented by the emergence (and dominance) of centralised provision of online services such as Facebook, Twitter and Google – actors who appear later in this chapter, largely as a result of their capacities in this respect.

Centralisation of information, then, is a symptom of the growth of online service providers primarily encompassing social media and search engines. These 'walled gardens' (Berners-Lee 2010[152]) allow for collection and processing of enormous quantities of personal data provided by users. In another interview, self-described software developer, hacker and freedom fighter Smári McCarthy observed,

> '…overall, the ability to surveill has been increased because of the centralisation of services. The more people that use services such as Facebook…the fewer points you need to attack. I say attack in the adversarial sense, to gain information about a very large population.'

Additionally they provide, for many, an all-encompassing service; as Joss noted,

> 'there are a good chunk of people I'm sure that you could put in front of a computer that only accessed Facebook…that would be perfectly happy with that. This is a monoculture…centralisation of information, putting all our eggs in one basket. I wish we would start to move away from it but we can't because it's quite difficult to do that.'

The explanation for why this would be difficult appeared to centre on *convenience*, and Smári outlined its connection to privacy and centralisation.

> '…people are very willing to trade their privacy for convenience so we willingly opt into putting our private data on to large centralised hub services or things like that because it's simple, you don't have to worry about your computer crashing, all these kind of convenient habits which actually from various levels…really damage your ability to exercise autonomy.'

A lack of personal privacy and freedoms seems to be the trade-off that the convenience of centralised information and services requires – and that is often taken. Running in parallel to this were concerns over the lack of awareness of what happens to personal data and how centralisation of information impacts upon users. The following remarks are only a snapshot of what participants had to say but they nevertheless convey significant disquiet.

> '…we are giving up and allowing to be gathered and providing to these centralised providers huge amounts of information…and what's happening is we're coming up against this fundamental thing that people don't realise and don't like to realise – that we're very very very predictable and that amount of control, the control that it allows…means that the Internet is just turning into some big command and control centre for people…' (Joss Wright, OII)

> 'So generally I think people need to understand that whatever is centralised is always bad for them because there is too much of them in this one place. They don't know what's happening with this data, you know so I think actually…it's

[152] See Chapter Two (section 2.5.2).

> the same kind of logical step that we have in other aspects of society. Centralisation never helped anybody.' (Daniel Domscheit-Berg, OpenLeaks)

The surveillance capability of such commercial service providers is one issue of concern in its own right. The Intercept Modernisation Programme in 2009[153] was a prime example of an attempt at centralising information for surveillance purposes by the government. Vocal concerns over such a data repository arguably informed the current approach in the CDB to federalise (i.e. decentralise) data storage to CSPs. Equally, we can see how centralisation of information in the private sector informs this process. CSPs already possess the data of interest to government and have the ability to store it (as well as collect more data relatively easily) and thus the decision to couch the CDB in decentralised terms was, arguably, more pragmatic and calculated than out of concern for such views as voiced by the interviewees above.

At the same time, continuing with government motivations, centralisation of *services* but not necessarily information was evident in the public sector, signalling a centralising impulse in the nature of contemporary (online) governance. Two participants from the Government Digital Service (GDS) were interviewed regarding the launch of GOV.uk – a platform that centralises many formerly separate government departments and online services[154]. The motivation behind GOV.uk, in support of the 'Digital by Default' agenda[155], was to improve efficiency and reliability in service delivery and, again, to make accessing government services online more *convenient*. However, in contrast to the approach of centralised corporate services, GOV.uk did not represent a simultaneous move towards centralising citizen data and information.

The interviewees' role was to facilitate identity assurance, the mechanisms by which members of the public verify their identity to the government in order to access/apply for services. The way in which this was achieved was, again, by a federated model, using private sector identity services to verify that applicants were who they said they were.

---

[153] See Chapter Two (section 2.4.4)

[154] As of June 2014, all 24 ministerial departments, five out of nine non-ministerial departments and 84 out of 157 agencies and other public bodies (including, for example, the Driver and Vehicle Licensing Agency) had been merged on GOV.uk

[155] For the 26 criteria of Digital by Default see: https://www.gov.uk/service-manual/digital-by-default

> '…this is about you choosing the private sector supplier, providing them with evidence of your identity, them verifying it and issuing you with a credential to a certain level of assurance…you'll be asked to log in with your credential or your private sector identity or whatever, you'll go off to their webpage, you'll authenticate with them and they will then release a small amount of data not related to any levels of assurance but just enough information that will allow the government department to match who you are in their records.' (Bert, GDS)

This bears some resemblance to the outsourcing of responsibility for data collection to CSPs described in this chapter. Similarly, what we see is an acknowledgement of the 'agility' of the private sector;

> 'it can take advantage of new technologies and respond to threats and opportunities obviously a lot quicker than government.' (Bert)

At the same time, citizens are offered a choice of how to assert their identity. Thus, centralisation of services in this instance does not directly correlate with the concerns voiced by other participants. The difference appeared to be a pragmatic emphasis on engaging users and reflecting their needs.

> 'I understand the philosophy you know why some people say the Internet's a sort of organic entity that will just grow and to actually try and corral different elements into one place runs contrary to that, however, you want people to use those services, you know it's a bit like if users didn't want it they wouldn't have Amazon then why would Amazon would be there as that one place to purchase a variety of goods and services so I understand the philosophy but the approach we've adopted is based in the insight we've received from users and the direction of travel that they've kind of laid down and ultimately you know it is a market and the users will determine if it's wrong, if it's not appropriate they'll stop using it...' (Ernie, GDS)

Centralisation of Internet architecture and information/services are closely linked. While there were persuasive arguments for decentralisation in the context of corporate services, there was an equally coherent position adopted by proponents of centralisation by government.

Thinking about tendencies towards centralising and decentralising patterns of organisation and regulation in this way is helpful for what follows. It has already been indicated that centralisation of services is occurring on the Internet, primarily in the form of social media and other Web-based service providers such as Google (for whom social media is one part of a broader enterprise). Centralisation of this kind is naturally pursued for economic motives: get the customers through the virtual door, then keep them there for as long as possible, extracting as much useful (i.e. monetised) data as possible. The wealth of data possessed by such services

means, in essence, if government or law enforcement wants data on citizens' activities online, they know where to go. Accessing these data requires regulation both in terms of attempting to ensure companies comply with such demands but also – as a reaction of sorts – that such requests comply with other regulation that seeks to protect consumers and Internet users. These processes are illustrated throughout the remainder of this chapter.

At the same time, the private sector is implicated in the processes of identity assurance being introduced by the government. There is a clear parallel here with Lessig's (1999) 'architectures of identification', the trend towards regulating the architecture of the Internet so as to make identification easier and commonplace. Again, *convenience* seems to be a strong undercurrent. It does not require a tremendous leap of imagination to see the connection between centralisation of information and services in this respect. However, it is important to remain that the government and private sector relationship is at times cooperative and other times competitive (Fuchs 2008).

6.4 CONTENT VERSUS COMMUNICATION DATA

> 'If you give me six lines written by the most honest man, I will find something in them to hang him' (Cardinal Richelieu (1585-1642))

A key feature of many written and oral responses to the consultation on the CDB was a dichotomy between *communications* data (CD) and the *content* of communications. In their examinations of witnesses, the Joint Committee repeatedly ventured to uncover respondents' thoughts regarding the distinction between these two forms of data. Was any such distinction considered to exist, or was it a necessary distinction to attempt to make in light of the intentions of the Bill? Did they consider the proposals of the Bill to allow for content of communications (e.g. emails and SMS messages) to be captured? The rationale for this is clear; the ability of government or law enforcement to read the contents of private citizens' communications would be incredibly intrusive. This concern was apparent in one individual/non-expert respondent's evidence:

> 'You seem to want to know what is going in on in every single persons mind in the UK from private conversations on the phone to emails and texts messages. You can build a picture of peoples political tendancies, which websites interest

> them, what they look at and if you deem it to be a threat what would you do,... put them in prison because they looked at a website about the muslim religion so they might just turn out to be a terrorist [sic].' (Lisa Kavanagh – *Individual/Non-Expert*, CDB Written Evidence, p.329)

However, as Justice (2011: 71) note in their report *Freedom from Suspicion* this intention or capability is a misconception; a lack of public understanding of what constitutes communications data, fuelled by speculative media reports (see for example Kirkup 2008). The issue this raises is an undercurrent in what follows; whether obtaining a granular picture of citizens' daily lives was (1) intentional and (2) if not intentional, whether the government were alert to this possibility.

CD are commonly referred to as the 'who, where and when' of a communication and are constituted of three parts: traffic, service use and subscriber data[156]. Traffic data are those elements that are attached or contained within a postal or telecommunication message that allow it to be transmitted. For an email, this will typically include the date and time it was sent and received, the login name of the sender and their IP address (from which can usually be obtained the physical location of the computer). Traffic data from Internet browsing sessions will also include the URL of any website visited[157] and the time spent on this page. Service use data are those produced by CSPs that record users' activity such as itemised bills and activity logs, while subscriber data are those details of customers such as name, date of birth, contact and payment details – everything one provides when signing up to a service. From this brief description, it is clear that CD can reveal a large amount of information about individuals' electronic communications and activities. Their relative value to law enforcement is also apparent; being able confirm that a suspect was at a particular location at a particular time or was in communication with someone else can be vital evidence for an investigation. In his oral evidence session, the Chief Constable of Greater Manchester Police stated that the value of CD was in establishing associations between criminals and groups of criminals. However, as one interviewee argued, the government's stated aims expected too much from CD:

[156] These three parts are defined in Section 21(4) of the Regulation of Investigatory Powers Act (RIPA) 2000 and were retained in the draft CDB.
[157] 'Weblog' data as described above.

> '…the idea that this huge amount of data would be available for detecting, sifting, whatever else, finding the terrorists in the crowd is very unlikely. I wouldn't deny that it would be able to backup data that you would get from somewhere you know, you suspect somebody of being a terrorist, this would potentially allow you to investigate that individual probably very effectively, that's certainly feasible but this idea that you would use this as a system to pull terrorists out of the general population by detection is just completely, mathematically, very unlikely.' (Joss Wright, OII)

The findings here illustrate two key aspects of the data dichotomy. First, while government officials defended their claim that accessing content data was not their intention, the *technical* feasibility of separating CD from content in electronic communications was challenged by several respondents. Second, the *sensitivity* of CD was highlighted; the insight into people's personal lives that could be ascertained from CD was considered equal to, if not greater, than content.

6.4.1 ISOLATING THE 'WHO, WHERE AND WHEN'

Government officials were quick to reassure the Committee that content data would not be captured under the CDB.

> 'I am absolutely clear that the key data we want is the who, where, when and how. That is clear, and there is no intention of going beyond that into content or anything…We have been very clear about that at every stage, and the Bill is not intended to take us any further than that.' (Theresa May (Home Secretary) – *Official*, CDB Oral Evidence, p.399)

> '…we would only be able to store communications data…I must stress, through the Bill it is illegal for us to collect content.' (Richard Alcock – *Official*, CDB Oral Evidence, p.17)

These claims indicate a desire to allay fears and by doing so make some headway in justifying the collection of CD. Despite the fact that CD constitute a breadth of valuable personal data, the message was clear: content data is more personal and as such the government draws the line at CD[158].

Some respondents to the consultation felt that it would only be a matter of time until content-focused powers *were* legislated for and that in itself was sufficient reason to prevent the passing of the CDB.

[158] This is not to disregard the value of content data for crime prevention purposes. Justice (2011) point out that the lack of public understanding about CD is due to confusion with *intercept* data. Intercept data *is* content data but access to this is only possible via a warrant obtained in accordance with s.71 of RIPA (2000).

> '…this is a stepping stone legislation. While content monitoring is not yet included in this bill, it makes it easier to be included in a later one.' (Martin Ammann – *Individual/Non-Expert*, CDB Written Evidence, p.25)

> 'The Government is not presently arguing that we should all be routinely or randomly subject to bugging, covert tracking or interception 'just in case' but, if the present proposal is allowed to pass, proposals for other types of blanket or random surveillance irrespective of suspicion 'just in case' are a logical next step.' (Liberty – *Advocacy/Non-Profit*, CDB Written Evidence, p.364)

The challenge in maintaining the position that content data would not be captured came in the form of the technical feasibility of keeping the two forms of data separate during collection. If technical limitations meant that some content could be 'scooped up' along with CD then the level of intrusion would be unjustified. According to the Director of the Communications Capability Directorate of the Home Office, this problem could be avoided by responsibilising CSPs:

> 'We will be working with them to retain, in some cases, aspects of communications data and, in that case, it is very easy to separate content from CD…We will not be applying any systems that cannot reliably extract CD from content through whatever data streams.' (Richard Alcock – *Official*, CDB Oral Evidence, p.17)

This optimism was not shared amongst other respondents:

> 'Until you have a very clear idea of what the law says in terms of what is communications data and what is content, you cannot try to translate that into a series of technical measures – filtering of the sort that is being suggested in the legislation. Many of us believe that the definitions are far from clear. (Professor Peter Sommer – *Expert (Academic)*, CDB Oral Evidence, p.130)

Placing the onus on CSPs brings to the surface the nature of the relationship between government and the private sector. To that extent the CDB is representative of similar trends identified elsewhere in contemporary formations of control (Garland 2001). Relatedly, a core aspect of social control is blaming (Innes 2003: 139). Arguably, if content data are accidentally captured and subsequently viewed, shared, or lost, culpability lies with the CSPs who collect them. This has implications for understanding control. Through regulation both corporate entities and individual citizens are embroiled in the social control apparatus, directly or indirectly. Hypothetically we might envision a reformulation by government of the 'problem' of capturing content data – what Innes refers to as a 'stylised politics of blame' (2003: 141). To negate the problem, regulation could dictate collection of *all* content and CD and then empower an independent authority to separate the two

upon an authorised request. The resultant expansion of the control 'net' (Cohen 1985) – supplementary/intensified powers of dataveillance – would be justified on the grounds of improved oversight and security of data. Resistance to the CDB from the private sector is therefore understandable and deepens our understanding of the negotiation of social control.

Cooperation, on the other hand, between government and CSPs and security of data are separate issues returned to below. However, it is helpful to draw briefly on private sector observations of the data dichotomy. Many of the questions put to CSPs concerned encryption of data that travels across their networks – particularly third-party data (e.g. data from Facebook or Gmail):

> 'Once we can identify the packets of data, we would need to find a way technically to say, "Okay, we understand that we now need to retain these", but they are encrypted, or not, on an application-by-application basis. If they are fully encrypted, we need to be able technically to unpick it and say, "Here is the traffic data but obviously we have not touched the content", which is very difficult.' (Mark Hughes – *Telecoms Industry*, CDB Oral Evidence, p.179)

Mr Hughes pointed towards two problems here. First, the presence and form of encryption of communications varies and thus the technical procedure to separate content from CD will vary accordingly; in other words there is no single way to do this. Second, 'unpicking' the encryption without viewing the content is troublesome. While Mr Hughes mentions later that some packets of data have the CD labelled in plain text, this is not typically the case. Further to this, in the event that overseas service providers would/could not provide details regarding service users[159], the Bill outlined provisions for placing 'black boxes'[160] between UK-based CSPs and their customers to rectify this problem. Glyn Wintle (CDB Oral Evidence, p.132), noted that by using this technique 'absolutely, categorically, you are going to get some blurring' between content and CD.

[159] See section 6.5 for a discussion of this point in respect of jurisdictionality.
[160] Colloquial – these pieces of equipment are used to carry out Deep Packet Inspection (DPI) and are typically used for the collection of intercept data.

6.4.2 THE 'INTRUSION FALLACY': COMMUNICATIONS DATA IN THE INFORMATION SOCIETY

A primary issue that the research data up until this point have pointed towards concerns the distinction between CD and content data in terms of their respective abilities to reveal sensitive and personal information. The key assumption relied upon by advocates of the CDB was that content data was the more personal and sensitive of the two, hence its protection in previous legislation by the need for intercept warrants. However, there was vocal criticism of this line of argument. In the contemporary technological environment, it was frequently argued, CD were just as revealing (if not more so) than content data.

> 'Promoters of the scheme have made much of the idea that *only* communications data will be open to such routine inspection, not content – the implication being that somehow content is more intimate. This is not true. A timeline of all your contacts and interests, phone calls, reading and browsing, purchases, financial worries, patterns of movement, of waking and sleeping, build a far more complete picture of you than you ever explicitly write down for anyone, perhaps more complete than you have yourself…' (No2ID – *Advocacy/Non-Profit*, CDB Written Evidence, pp.437-8, *emphasis* in original)

> '…one of the huge aspects of the Communications Data Bill has been this disparity between content and communications data – this idea that they're not going to be reading your emails, they're just going to be looking at who you sent them to – and that being an utterly false dichotomy whereby the amount of information that is embedded in what you do, when you do it, who you do it with, what websites you access, when you access them, how you access them, the shape of your social network, the idea that this is not somehow privacy invasive, is just massively false.' (Joss Wright, OII)

An analogy could be drawn here with other forms of surveillance. CCTV for instance, offers the same possibility for monitoring real-world interactions between people – the who, where and when – as CD to a large extent. Equally, the content of people's conversations does not need to be captured on CCTV for a reasonably robust estimation of what occurs in the daily life of any observed individual. What is more, in the context of digital communications there is a wealth of data subsumed under the heading 'communications data' that, when brought together, can create a highly detailed picture of an individual. This concern was central to the critiques of many respondents:

> 'They [communication data] can be far more intrusive and revealing and, of course, far more useful. This is especially so when data is combined to create a broader picture of an individual's movements, personality and social circles…we

> refute the suggestion that communications data does not somehow convey substantive content about a person's life.' (Open Rights Group – *Advocacy/Non-Profit*, CDB Written Evidence, p.448)

> '…social network analysis of communications data can generate sensitive (aka 'special category') personal data, without any knowledge of the content of communications…experiments have successfully demonstrated prediction of users' political affiliation, gender and hobbies.' (Caspar Bowden – *Advocacy/Non-Profit*, CDB Written Evidence, p.94)

The process Mr Bowden refers to is known as *homophily*; the inference of various personal traits based on those of close acquaintances[161] (typically observed through social network analysis). Identification of individual browsing habits and preferences is lucrative for online marketing and advertising companies and the subsequent explosion of academic, media and tech interest in 'Big Data' cannot be divorced from the types of concerns evidenced here. Central to each are the questions of what can be done with our personal data, who can access it and what it can reveal about our personal lives. The Tor Project, in their written submission, highlighted the computational aspect to the collection of CD:

> 'The reason that communications data can be more sensitive than content is that it is more amenable to automated analysis, particularly when collected in bulk (as proposed by the draft bill)…communications data is designed for computers to interpret and so is far easier for computers to analyse, allowing a more accurate and detailed profile of individuals to be built than is possible with current technology to interpret content.' (*Advocacy/Non-Profit*, CDB Written Evidence, p.563)

Automated analysis, to which the Tor Project refers, is indicative of these related concerns of 'big' data analytics. The intrusion presented by the collection of CD can therefore be understood as a product of the combination of multiple data sources. In isolation, various CD may not reveal particularly sensitive information. In combination however, the possibility for inferring sensitive information (with a high degree of accuracy) is greatly increased. This process of triangulation has primarily been critiqued in the context of Big Data; the privacy rights of service users may be undermined if data are used to produce information beyond that covered in privacy agreements. The same assumption provided the basis for the claim that CD was just as intrusive than content. The observations of the Open Rights Group (above) and the following remarks from Privacy International demonstrate this:

[161] Previous research has demonstrated that people interact more frequently with people who are similar to themselves (see McPherson *et al.* 2001).

> '*Bringing together data from such a wide variety of sources*…provides an intimate mapping, allowing law enforcement to identify a person's associates, friends, family and daily habits, even when and where that person sleeps.' (*Advocacy/Non-Profit*, CDB Written Evidence, p.479, *emphasis* added)

6.4.3 EVOLVING DATA

The data dichotomy was one of the most prominent themes to emerge from analysis of the consultation data and was echoed in conversations with fieldwork interviewees. Given its technical nuances, the discussion of the feasibility of separating content from CD primarily occurred between respondents from official, expert (academic and technical) and telecoms categories. The argument for what is denoted the 'intrusion fallacy' was vocalised largely by advocacy groups and activists – although some of these groups do acknowledge these arguments were constructed from consultation with experts in the field. The basis of this issue is thus a computational/technical one, but it is translated effectively into meaningful terms for the public audience who are affected by it. Consequently, we are presented with a simple theme; regulation failing to keep pace with and respond accordingly to changes in technology.

A number of confounding factors meant the separation of content and CD – at least on a technological level – would be complex. It appeared that the technical feasibility of separating content from CD was inherently connected to the concept of the dichotomy between the two forms of data themselves; what is content and what is communication data is not as clear as it was when previous regulation was enacted. Thus even if a system could be successfully implemented to collect only CD, the dangers to users would still exist. The intrusion fallacy helps to reinforce this point. Whether the government were alert to this possibility is unclear. However, what is apparent is regulation was being framed inappropriately for the technological environment.

The crime and terrorism context of this regulation is important to bear in mind. It dictates a balance that must be struck between freedom and security while at the same time ensuring any steps taken are necessary and proportionate. For Brown, 'precautionary mass surveillance' (2009: 132) is neither necessary nor proportionate and regulation that allows for this – such as the CDB – amounts to a failure to

protect both the freedom and security of citizens. Freedom is eroded by the intensification of digital surveillance; gaining increasingly granular pictures of people's private lives as they are constituted by their communications. Although monitoring all Internet traffic is technically impossible (Brown 2010), recent events such as the Snowden revelations indicate that the capabilities of intelligence agencies are significantly greater than previously acknowledged. Security meanwhile is undermined by the continued failure to enact satisfactory legislation that appropriately updates the capacities of intelligence and law enforcement agencies. Approaches to conducting surveillance via developing regulation such as the CDB will always be met with resistance. As an alternative, Brown (2010) advocates a targeted, proportionate and court-authorised model for communications data surveillance that would strike the necessary balance between freedom and security.

6.5 JURISDICTIONALITY

Dealing with multiple regulatory jurisdictions was an unavoidable aspect of the type of powers the CDB attempted to provide; while a good deal of communications data of interest to law enforcement would originate in the UK/relate to intra-UK digital interactions, a large amount would involve extra-UK interaction with overseas service providers. While specified legal processes[162] exist to access data held overseas about service users in the UK, the CDB made provisions for UK-based CSPs to retain data relating to

> 'ii) the services of overseas providers used by people in this country which transit systems but which the system provider currently has no business to retain.' (House of Commons 2012: 12)

This is the issue of third-party data. As a contextual example, this would consist of BT (based in the UK) collecting and retaining data about their customers' use of Gmail (based in the US) as it travels across their network within the boundaries of the UK. While this may seem a reasonable and tempting step to take (MLATs are

[162] RIPA is one such process. Another key method discussed in evidence sessions with the Joint Committee was the Mutual Legal Assistance Treaty (MLAT). This is a formal request for information made between different sovereign jurisdictions and legal systems. It acknowledges and is designed to overcome the barriers to information sharing between states. In some cases, bilateral or multilateral treaties may obligate states to comply with MLAT requests issued from corresponding states, such as the 1994 UK-US MLAT.

not a swift process), there were a number of barriers to this, not least UK and overseas CSPs' reticence to accept such measures. The issue of jurisdictionality also brings into this discussion the valuable contributions of overseas actors in the 'Telecoms Industry' category of respondents. Their position is unique in that they possess first-hand experience of complying with RIPA and MLATs in an international context, and consequently offer clear indications as to the reception of the Bill amongst their community.

6.5.1 IF IT AIN'T BROKE, DON'T FIX IT

Representatives from Google, Hotmail/Microsoft and Yahoo! presented a straightforward argument: there are limits to what data the UK is allowed to obtain directly; there are existing routes to follow in order to obtain data it is not permitted to access and; while there may be room for improvement, these routes provide some clarity and legal protection in an already complex regulatory arena. Expanding upon this, Emma Ascroft of Yahoo! was concerned on two related grounds.

> 'The UK would be the first country to extend its jurisdiction and take a reserve power to require UK providers to retain data that they could not obtain directly. We believe that other countries would follow, including countries that would use legislation of this kind to limit free expression and infringe privacy rights of internet users. From our perspective, that would create a bewildering patchwork of overlapping and potentially conflicting legislation.' (*Telecoms Industry*, CDB Oral Evidence, p.214)

First of all, then, the Bill could generate copycat legislation – muddying the regulatory waters more than they currently are. Second, the countries that might do so could be those whose intentions are more restrictive of civil liberties. Adding to this, Yahoo!'s Director of Public Policy made clear the reason why maintaining clarity in this arena was important.

> 'Companies like us would face impossible decisions about how to be consistent in how we protect our users and operate our businesses in the 57 markets around the world where we operate…we are a company that is built on consumers' trust and confidence, and in order to honour that commitment we aim to be consistent in how we engage law enforcement around the world.' (*Telecoms Industry*, CDB Oral Evidence, pp.214 and 223)

This outlook, shared by representatives from Microsoft and Google, positions overseas CSPs as accountable, first and foremost, to their consumers[163]. This issue of trust between CSPs and service users is an important one and is played out visibly in respect of jurisdictionality.

There was also the problem of *encrypted* third-party data. Encryption of data for CSPs is typically proprietary; consequently, when retaining their own data, decryption would be straightforward for (UK) CSPs but would not be the case for third-party data. Asserting their position on this issue, overseas CSPs stated that they are usually willing to decrypt these data when issued with a valid RIPA/MLAT request.

> **Sarah Hunter (Google)**: 'From a Google Inc. perspective, we are very confident about the security of our encryption. If a valid RIPA request comes in or UK law enforcement goes through the MLAT, receives a court order and in turn gets Gmail user data, we will obviously provide that data decrypted. If it was to use a third-party provider to gather the encrypted data, I think it very unlikely that Google Inc. would provide anyone outside Google Inc. with that key. That is simply because, as everyone said earlier, security is our most important asset. Our relationship with our users is predicated on trust. Without that, we have no business.'
>
> **Emma Ascroft (Yahoo!)**: 'I would say the same thing…The encryption question is rather a red herring because the UK law enforcement agency can obtain the data direct from us using international legal channels such as the MLAT. If it came to us through those channels, we would disclose those data in the clear. If those channels work properly, this backstop power is unnecessary.' (*Telecoms Industry*, CDB Oral Evidence, p.226)

This stance reinforces the position that the current methods for requesting data are sufficient. Encryption appears as a bargaining chip of sorts, with the justification that this is in the best interests of service users. By attempting to circumvent the lengthy RIPA/MLAT process, UK law enforcement (via UK CSPs) would need to decrypt the data themselves, which is both time consuming and costly. To do so would require some form of 'man in the middle[164]' attack but this too could have negative consequences on trust and security. As the Chief Technology Officer for Timico noted during a fieldwork interview,

---

[163] While increased faith in personal data protection is favourable for service users, it is not cynical to suggest CSPs' motivation is retaining a valuable customer base.

[164] A man in the middle attack is a means of intercepting digital communications by creating independent connections to both sender and receiver and relaying the messages between them. As far as the parties are concerned, they are talking to one another but in actual fact they are talking via the 'man in the middle' server.

> '…notwithstanding the fact that to be able to do so at any scale would need massive computing power, when you start messing about with things like that [HTTPS[165]] you start undermining the trust in the banking system for example, you know, how do you know that your HTTPS link between you and your banking is not being monitored by somebody?' (Trefor Davies – CTO, Timico)

The broader ramifications of this part of the discussion begin to appear. Trust between service user and provider is crucial to the operation of the Internet. However, the reason that this is crucial is because the Internet has evolved as a space where trust is required – specifically, a commercial space. As Lessig (1999: 64) says, 'Spaces have values. They express these values through the practices or lives that they enable or disable.' Cyberspace is primarily a space for consumption. Of course, it is also a space for communication but in large part communication relies upon forms of consumption. The dominant form of practice enabled on the Internet is consumption and for this to be sustained and to grow, trust and security are required. More recent events illuminate this juxtaposition of space/territory and trust, security and digital rights. The on-going debate about the General Data Protection Regulation in the EU for instance signifies the interests that both states and corporations have in restrictions on the transfer of personal data between jurisdictions, with each pursuing a specific agenda (whether that is increased profit or prevention of crime) while trying to negotiate the terms of their relationship *and* balance the privacy rights of citizens. Online spaces are consequently multiple, overlapping and contested and it is clear why attempts at regulation of these spaces produce such struggle.

6.5.2 NOT IN OUR CYBERSPACE!

One final observation serves to ground jurisdictionality in more popular debates. Jurisdictionality as representative of place and territory is a useful conceptual tool for anyone wishing to make comparisons between the UK and other states in respect of the extent of surveillance. For that reason, it was a tool employed often by advocacy groups in pursuit of a persuasive counter-surveillance narrative. These groups tended to identify the proposed use of a specific technology – DPI – as comparable to other states, while individuals/non-experts (and again advocacy

[165] Hypertext Transfer Protocol Secure: Rather than a different protocol, HTTPS is a layering of standard HTTP communications with SSL (Secure Sockets Layer), thus ensuring more secure data transfer over a network.

groups to some extent) gravitated towards notions of democracy and popular representations of pervasive state surveillance. The following extracts are indicative of these respectively:

> 'The collection of data through black boxes at ISPs in order to monitor activities within a country and beyond a country has only been implemented at a national scale in China, Iran and Kazakhstan. DPI—deep packet inspection—and black boxes have been used on a local scale, and we have cases in Egypt, Pakistan and Tunisia. The idea of a black box run at a national scale, at an organised centralised level, as to what will actually be monitored, has not yet been done in a democratic country.' (Dr Gus Hosein – *Advocacy/Non-Profit*, CDB Oral Evidence, p.49)

> 'The Home Office has failed to make any case about why Britain should be the first democratic state to implement this kind of policy. Nor has the Home Office responded to the legitimate concern that this policy adds legitimacy of the surveillance pursued in China or Iran, which British foreign policy has sought to prevent in other countries.' (Big Brother Watch – *Advocacy/Non-Profit*, CDB Written Evidence, p.63)

In these remarks we see advocacy groups' awareness of the instrumental value of appealing to notions of Western democracy and liberalism, particularly when placed in contrast to authoritarian regimes of the likes of China and Iran. The same theme was taken up by other categories of respondents:

> '…this is the kind of oppressive policy that one might find in a much less libertarian nation, such as China or Libya, where electronic communications were monitored until the government was overthrown.' (Peter Cromie – *Individual/Non-Expert*, CDB Written Evidence, p.140)

What is also clear from these extracts is that cyberspace *is* perceived in territorial terms – there are models of cyberspace to aspire to and there are those to avoid. Comparisons with China and Iran are therefore designed to send the message that 'we don't want our cyberspace to be like their cyberspace.'

Nevertheless, not everyone who discussed the analogy perceived it in these terms. The Director of the Centre for Social Media Analysis at think tank Demos noted:

> 'I do not think that analogies with China, Iran and Kazakhstan are very helpful. We regulate the ways in which privacy is breached in a way that those countries do not, even if they use some of the same technologies, which they do already, for all types of snooping. Also, there needs to be that way in which the police know what they are doing, so that we do not have the risk of inadvertently breaching various regulations, which is probably easier now than ever.' (Jamie Bartlett – *Advocacy/Non-Profit*, CDB Oral Evidence, p.290)

Here, the difference between the proposed measures in the Bill and the regimes existing in other countries was that the Bill was an attempt to put state intrusion into privacy on a legal footing and to clarify – for public reassurance and for law enforcement guidance – precisely 'what can be done, why, under what conditions and by whom' (p.290).

Beyond the case in question, using different jurisdictions as emblematic of a type of surveillance has broader significance for understanding the process of negotiating social control and social order. They provide insight into culturally embedded ideas about surveillance and citizens' rights; they show the social construction of what is deemed necessary and proportionate and illustrate the values that people attach to freedom of communication. Moreover, official sources also these categories as a form of defence:

> '…it is absurd to compare any aspect of this Bill to the practice in non-democratic countries' (Home Secretary Theresa May, CDB Written Evidence, p.255).

Social order is produced by such practices of consensus-building and constructing meaning. It follows that forms of social control designed to maintain social order (surveillance and regulation) should adhere to these conceptions of the type of social order we wish to preserve. Respondents' comparisons between the CDB and authoritarian regimes elsewhere alert us therefore to a paradox at the heart of the state response to the risks of crime and terrorism; the removal of the freedoms and liberties that they profess to protect. This 'state of exception' (Agamben 2005) – normalising exceptional powers and enactment of 'emergency' legislation – is characteristic of the UK and US rhetoric on national security post-9/11. As Lyon (2007) observes, this situation extends to routine surveillance (such as monitoring of communications data) as well as specific counter-terrorism powers (such as extended detention)[166]. Resistance to regulation and increased surveillance in this context is thus a process of competing for the right to define how social order should be protected.

[166] Indeed, since this analysis was conducted Parliament has passed – despite much criticism (see Powles 2014) – broadly similar powers to those in the CDB as emergency legislation in the form of the Data Retention and Investigatory Powers (DRIP) Act.

6.5.3 MEDIATED SPACE

Surveillance is rarely a relationship between two parties – the ideal type of 'watcher and watched'. The literature in this area has long acknowledged this, most notably with the concept of the surveillant assemblage (Haggerty and Ericson 2000) that alerts us to the plurality of modern surveillance. Among others, Haggerty (2006) has suggested that surveillance practices should no longer be conceived of in panoptic terms[167] as they have dispersed beyond a state-centric, control-based model into inter-personal interactions via new technologies (webcams, IRC, social media) and into transactions between individuals and a variety of organisations. While state-centricity remains a powerful influence in the context of this chapter, also evident are the multiplicity of actors with a stake in current debates around regulation of digital surveillance. Specifically, there is a tenuous relationship between states and CSPs. Citizens, meanwhile, are caught in the middle.

Online spaces are not only constituted of state regulatory jurisdictions. Just as significantly, online spaces are the territory of private organisations; for example CSP networks, social media websites and search engine facilities. These domains are strictly regulated in their own way and subject to extensive (but typically consensual[168]) monitoring and for that reason have been referred to as 'walled gardens' (Berners-Lee 2010). In the context of the CDB, mediation of surveillance is particularly visible as there is a tacit acknowledgement on the part of governments that private corporations and their services are a valuable source of information.

> '…I had a chat with the guy at the Home Office who I think drafted the draft Bill and he was saying "well you know, in effect all we're asking for is the same kind of level of information that already exists in private companies like Google and places like that" so my answer then is actually, maybe, there is a debate to be had about how much information the likes of Google are allowed to keep.' (Trefor Davies – CTO, Timico)

From these remarks, the tension between states and CSPs is evidently connected to other concerns regarding data practices of the latter. Recent media and academic outpourings on 'big data' are indicative of these and have found resonance with pre-

[167] See the discussion in Chapter Three.

[168] In the form of Terms of Service and Privacy Agreements. However, these are frequently the source of contention as service providers often introduce new features that impact upon privacy expectations of their users.

existing concerns regarding the socially regressive possibilities and sorting effects of 'dataveillance' technology (Clarke 1988; Gandy 1993; Lyon 2003b). What emerges is that artificially-imposed jurisdictions in 'borderless' cyberspace present a barrier to the state's efforts at trans-national mediated surveillance. Two related lessons follow from this. First, regulating cyberspace within national jurisdictions (*intra-regulation*) is less problematic – although by no means straightforward – than attempting to cross virtual jurisdictions (*extra-regulation*). This is due to other legal obligations placed on corporations. Second, there is increased blurring between regulation offline and online, which again plays out in form of tension between the state and the private sector.

Lessig's (1999) work is instructional at this point. Contrasting 'East Coast Code' (law and regulation) with 'West Coast Code' (computer coding of programmers and engineers), Lessig shows how the former (i.e. the government) has increasingly attempted to control the latter (cyberspace). Importantly, this has become easier as West Coast Code has increasingly become the domain of corporations (think Google, Facebook or BT) who can be regulated much easier than earlier programmers and software writers. Corporations do have a (commercial) interest in regulation – indeed they regulate themselves to a degree. However, the trend Lessig identifies remains true today and has been demonstrated by the data here: 'the West, partially, resists' (1999: 53).

Lessig's story of 'East meets West' (1999: 53) resembles the theme of this chapter. When East meets West in the context of digital surveillance, tensions become particularly apparent. In part this is due to the increasingly politicised nature of private data and cyberspace. CSPs have obligations to customers and other commercial actors that must be balanced with the need to comply with law enforcement and state regulation. Regardless, CSPs have slowly been transformed into surveillance instruments for the state. While a large amount of what they do for their own gain is worrying in the context of civil liberties and privacy, CSPs and other corporations do – as the data show – resist to some extent. Yet, the incremental control of West Coast Code by the East is clear. Again, we need only to look at the Snowden revelations to see that the true nature of mediated surveillance

– sculpting the private sector into a system of mass surveillance – is far deeper, longer and more intensive than previously thought.

6.6 FUTURE-PROOFING AND FUNCTION CREEP

A general concern with the draft Bill, evidenced in both the written and oral evidence and vocalised in fieldwork interviews, was that Part One of the Bill was too broad, the powers it granted and subsequently the types of data that might be collected too wide ranging. As the breadth of extracts below illustrate, this pervasive issue was taken up by all categories of respondents. The dilemma at the heart of this speaks to this chapter as a whole; how to adequately respond and adapt to continual technological development. There were, then, two pathways that might be followed. Home Office officials and law enforcement bodies favoured the path of keeping the scope of CDB wide so as to anticipate further advances in communications technology – 'future-proofing' the Bill:

> 'The fundamental reason why we are nervous about limiting Clause 1 is future-proofing…I genuinely believe that no sooner will you get this legislation through than something else will come up, given the pace of change in the communications industry, which will create another gap…' (Charles Farr (Director General of the Office for Security and Counter-Terrorism) – *Official*, CDB Oral Evidence, p.346)

> '…we need…to make sure the legislation is framed so that it maintains that capability for the months and years ahead.' (Sir Peter Fahy (Chief Constable Greater Manchester Police) - *Official*, CDB Oral Evidence, p.376)

Opponents on the other hand advocated a narrower, limited scope to tackle only the *current* capability gap and to require some form of Parliamentary approval for any future addition to the powers that would be enacted:

> 'I think this Bill is future-proof, but in the worst possible way…the Home Secretary seeks to have the power to her and her successors, in the words of the Bill, to do anything they like once the universal surveillance engine is connected up to the entire national internet. So, for that reason, it is additionally terrifying…I do not think you can put in place a good future-proof Bill, but you could put in a transparent, thoughtful, representative system of reviewing how you adapt access to intercept and communications data as the technology changes.' (Duncan Campbell – *Media*, CDB Oral Evidence, p.315)

Reflecting the earlier discussion of the data dichotomy, it is plausible that as technologies continue to develop, it will become even harder to separate the two forms of data. Evidence has already been presented that this is a technical hurdle at

present, let alone in 10 years' time. There is a danger that wide ranging Order-making powers could result in content (or likewise revealing data) being captured at a later stage. This is yet another example of the tendency of a failure of control to produce successively more intensive forms of control (Innes 2003). In response to this concern, the Home Secretary felt 'that would be a different discussion that would need to be had' (CDB Oral Evidence, p.402). Evidently not persuaded, the Joint Committee recommended in their final report that concerns over the breadth of Clause One were hardly surprising and that it be narrowed, rather than enacted with a promise of being used, at present, to a limited extent.

This brings us to the issue of 'function creep', which can be conceived of in three ways. The first has already been noted; over time the parameters of what is classed as content data may be altered. Dr Paul Bernal, in his written submission (p.59), describes two more: the *purposes* to which the data is put and *access* to data. The former describes the temptation to use the data for additional and perhaps less serious criminal investigations than the primary categories outlined in the Bill: terrorism, organised crime and child pornography. The consequence would be an expanded net of social control (Cohen 1985). The latter describes a concern that has also been directed at RIPA, that a wide array of additional agencies and organisations may access the data for their own purposes; in Cohen's terms, wider and different nets of control (1985: 44).

In the case of RIPA, many local councils have come under fire for using investigatory powers for minor incidents – fly tipping for instance – which were not felt justified (see Norton-Taylor and Roberts 2009). Pete Bradwell of the ORG and the CTO of Timico address this concern:

> '…they've done nothing to address the problems they have, existing problems with RIPA…that access in our opinion is far too easy and that's a problem already we think especially when you consider the oversight regime in our opinion is too, isn't strong enough…' (Pete Bradwell, ORG)

> '…you'll note that already local government bodies are wanting the scope of this Act or Bill to extend to them and again the concern is that they will use it for all sorts of things that the Bill wasn't originally intended to be used for. Who knows what happens when a new political environment comes in and they say "hey, we've got all these tools at our disposal, let's use it to good purpose."' (Trefor Davies – CTO, Timico)

Four public bodies were designated access to communications data: the police, SOCA, HMRC and the intelligence services. Additional organisations requiring access were obliged to submit their justification in writing to the Home Office. The Home Secretary remarked that she anticipated the Financial Services Authority and the UK Border Agency being granted access and 'others that we are still looking at' (p.409), suggesting therefore that function creep in respect of access to data was already in evidence.

Data, in this context and others, have intrinsic value; they are a resource to be exploited. This is patently true for the private sector, particularly in the recent context of the advent of 'big data'. Moreover, 'Google envy' is characteristic of public bodies and government as a whole – and the approach of the CDB – as the previous section argued. There are a wide variety of uses to which data can be put – the bill outlines ten ambiguously broad[169] purposes for which data may be obtained – and thus it can be expected that a federated database of communications data would be a compelling resource for many organisations and institutions. As one individual/non-expert respondent to the consultation observed,

> 'Any assurance that "we won't allow that in the rules" is not worth the paper it would be published on. Once the data is on file, the uses of it will creep outwards step by step, and each step looks small to the government that allows it. Within ten years use of that data would be widespread, and vested interests would be too big to let it be given up.' (J. R. S. Kistruck – *Individual/Non-Expert*, CDB Written Evidence, p.336)

This has echoes of earlier remarks[170] and shows both a more general concern with function creep and a specific issue with what happens to data once it is collected. Added to this, while the description of the data to be collected was typically that which CSPs 'had no business interest' to retain, it is similarly plausible that at some stage in the future, they *would* develop a business interest in these data. It is unclear what the effect of this would be, given that the data would be held in privately-owned databases. This, along with all of the factors outlined in respect of

[169] For national security, for preventing or detecting crime or preventing disorder, in relation financial misconduct under section 123 or 129 of the Financial Services and Markets Act 2000 (civil penalties for market abuse), in the interests of the economic well-being of the UK, in the interests of public safety, for protecting public health, for tax reasons, for emergency health reasons, to assist investigations into alleged miscarriages of justice and to identify people who are incapacitated or dead, in order to identify them, their relatives, people connected with them, or to understand what has happened to them.
[170] See data from Martin Ammann and Liberty in section 6.4.1.

future proofing and function creep, all raise the question of data security and the oversight regime.

6.7 OVERSIGHT AND SECURITY

The proposed safeguards at all stages of the data collection, authorisation and retention regime and the formal oversight mechanisms received intense scrutiny throughout the consultation. Like many other aspects of the CDB these systems were drawn in large part from those already in place under RIPA but – as was the case with the definition of communications data – this approach was not perceived as wholly adequate for the new technological environment. Focusing lastly on safeguards and oversight permits an examination of the concepts of necessity and proportionality, which have since become a unifying banner for advocacy groups and concerned organisations and individuals. It is here that the contributions of the 'Independent Authorities' category are mostly heard.

6.7.1 NECESSARY AND PROPORTIONATE

Two independent commissioners – the Information Commissioner's Office (ICO) and the Interception of Communications Commissioner (IoCC) – have responsibilities with regards to protection of and access to data in the UK. The IoCC does not play a role in authorising requests for data; responsibility for assessing and authorising access to data resides with the Single Point of Contact (SPoC) and the Designated Senior Officer[171] within an organisation. It is for the SPoC to assess, in the first instance, whether an application satisfies the tests for necessity and proportionality.

For one privacy advocate, Caspar Bowden, the opacity of the tests for necessity and proportionality was concerning. In his written evidence, he observed that 'under the UK regime, almost all jurisprudence about interception and communications data takes place within the cranium of the IoCC, and almost nowhere else' (p.100).

[171] SPoCs are responsible for assessing the application for communications data and, if satisfactory, passing this to the DSO for authorisation. If the application is granted, the SPoC submits the request, obtains the data from the CSP and passes them to the investigatory team. Within the police force, SPoCs must be of a certain rank or higher; Inspector for subscriber data and Superintendent for service user and traffic data. In other public authorities the equivalent rank must be held, which can sometimes be the reason for procedural errors, i.e., the proper rank for authorisation can be misunderstood. Serious instances of wilful and fraudulent attempts to obtain communications data are criminalised under various Acts.

Citing the IoCC, Mr Bowden highlighted that necessity entails making the link 'between the crime/offence…the suspect, victim or witness; and the phone/communications address'[172]. Proportionality meanwhile rests upon 'the benefit the data will give the investigation', the relevance of the time period requested, whether less intrusive methods are possible and why any collateral intrusion into individuals' privacy is justified. The problem is that this does not provide contextual examples of what is and is not necessary and proportionate:

> 'How many people's data can be accessed to investigate what types of crime, what happens to that data subsequently, especially if something unexpected is found? Can a request be widened if nothing is found initially? Is anything done systematically to detect attempts at fishing expeditions? What is the policy on disclosure of communications data access to defense counsel? There is no published policy on any of these matters.' (Caspar Bowden – *Advocacy/Non-Profit*, CDB Written Evidence, p.101)

Elsewhere in the evidence, this issue was returned to:

> '…it is still not clear to me what criteria SPOCs use to determine what is necessary and proportionate. Indeed, it is not clear what criteria the Interception Commissioner uses, despite his evidence…in his evidence, said he does not have any difficulty deciding which is which, and I suggest this means that all SPOCs are somehow operating with some sort of magical sense of pre-established harmony, which I find rather hard to believe. I would like to know concretely what is considered necessary and proportionate.' (Caspar Bowden – *Advocacy/Non-Profit*, CDB Oral Evidence, p.372)

For the Executive Director of Privacy International, SPoCs – while valued for their training and skills – were not sufficiently independent arbiters of necessity and proportionality. Instead a warrant system was favoured, his reason for this echoing the discussion in section 6.4.

> 'One opportunity for this Committee is to start having a debate about why is it we protect communications content to such a degree but not highly invasive data-minable communications data and why are they any different? I believe once we start having that debate, we will start asking why is it we require a warrant for content but not for communications? (Dr Hosein – *Advocacy/Non-Profit*, CDB Oral Evidence, p.372)

For both Dr Hosein and Mr Bowden, the independence required to satisfactorily oversee the authorisation process resided with magistrates – echoing the earlier

[172] Necessity also relies upon demonstrating the use of the data fits with one of the purposes listed in footnote 150.

remarks of Brown (2010)[173] – although there was concern that they lacked the specific training needed.

6.7.2 VULNERABILITY

Aside from formal oversight mechanisms, the other pertinent issue here is the vulnerability of data. Vulnerability covers a broad spectrum of risks from technical weaknesses to human error including database security, hacking, commercial pressures to monetise data (alluded to above), and theft and data loss. Due to the high profile and newsworthiness of hacker groups such as Anonymous and the loss of confidential public records by public authorities, it is unsurprising that these vulnerabilities were picked out by a large number of respondents – particularly individuals/non-experts. The CTO of Timico, too, voiced his concern about these potential pitfalls.

> 'OK, so you put this big system in place…and you're gathering information, lots of diverse information about everything, about a person's online activity and keeping it somewhere which you are saying is very secure and which will be very carefully managed and access to it will be very carefully monitored etc., but since we've started talking about the Draft Comms Data Bill, I've started asking taxi drivers how often they find laptops left in the back of their cabs and out of the last taxi drivers I've asked, two have said "never, although I find a lot of phones" and three of them said they'd had eight laptops left, one had five laptops over a period of four to five years…so you have all this evidence about laptops stolen from GCHQ, laptops lost by civil servants, you know you hear about them in the news periodically about someone's left their entire national health records on a train or something like that and, you know, that will happen and on top of that once this system is in place it will become a target for hackers wanting to show that they can actually access this information and just like we had 6.5 million LinkedIn passwords published on a website in Russia, it will happen.'

The logical counterbalance to the problems highlighted in this extract is not to collect and retain communications data on this scale. Certainly this was the foundation of many of the critiques of the Bill. It was the same criticism levelled at the proposals for the IMP in 2009 in respect of a centralised government database, which can perhaps help explain the shift to a distributed/federated database model in 2012. This could be read as an attempt to give ownership of the vulnerability 'problem' to CSPs, thus both deflecting concern about privileged access to communications data and trying to ensure that data were held by those with the

[173] See section 6.4.3

technical capacities to do securely (and cheaply). However, as Dr Paul Bernal rightly pointed out (CDB Written Evidence, p.58), even sophisticated computing systems are vulnerable to attack; in 2011, Sony's online gaming platform the PlayStation Network was hacked, resulting in the disclosure of millions of users' passwords and credit card numbers[174].

While a distributed, federated database circumvents the problem of having all data accessible in one place, security as a result does not logically follow. This approach simply means there are multiple access points that are vulnerable to attack and more opportunities for human error in data handling across differently operated systems. Moreover, it does nothing to counter fears of data loss once they are passed to public authorities.

To an extent, these are problems that will have to be tolerated. Data exist and no security system is infallible. The variable factor, however, is the *extent* to which data exist and this was the crux of the debate surrounding the CDB. The Bill was described as a step-change in surveillance practice; not only one in which the mediation of surveillance was formalised to a greater extent but one that moved away from a 'traditional' model of targeted surveillance towards one of blanket surveillance – retention of data 'just in case'. Caspar Bowden described this as the dichotomy between data preservation and data retention and while this is an apt description of trends in communications surveillance, it has wider resonance for society.

> '…because of exponentially falling data storage costs, in the long run two contrasting states of society can be envisaged. Subject to exceptions, the default must be either that individuals determine whether and when their history is recorded, or data will exist about everyone all the time. At some point in the future, most people *will* understand the reality of "dataveillance" and the loss of associated freedoms.' (Caspar Bowden – *Advocacy/Non-Profit*, CDB Written Evidence, p.86, *emphasis* in original)

[174] See Halliday (2013).

6.8 SURVEILLANCE AND RESISTANCE PART 2: LESSONS FROM REGULATION

6.8.1 UNCERTAINTY AND AMBIGUITY

The question of how to 'do security' online is a troubling one for government. Evidently there is a pressing need. The Internet presents a bewildering array of opportunities for criminals to communicate and carry out their activities. However, we have seen that need is only one side of the coin. It is counterbalanced by proportionality and by most accounts the CDB represented a disproportionate extension of digital surveillance capabilities. Government perceived the necessity of keeping pace with technological change, to bridge a capability gap that emerged as the development of communication technology outstripped that of surveillance capacities. However, the findings here show that uncertainty plagues this field. What are the risks presented by technological developments in communication? What data are needed? Who has – or should have – the power and responsibility to conduct this surveillance? What are the impacts of surveillance on subjects? How will data be kept safe and by whom? The ethos behind the CDB was very much 'more data is better' but there appeared a corresponding lack of acknowledgment of what this drive towards blanket surveillance and data retention would entail and what impact it would have on individual citizens.

The Internet domain is an ambiguous one in this context; the threat posed can be misunderstood (or even unknown in the case of 'future-proofing' the Bill against as yet non-existent dangers) and attempts to implement security measures such as expansive capacities for data retention can produce unintended effects. These effects can include the sort of resistance to surveillance legislation demonstrated in this chapter or the circumvention of measures put in place, which produces a repetitive cycle of action and reaction (Marx 2009; Innes and Levi 2012). This argument is picked up by Harvey Molotch (2012). Analysing several 'sites of ambiguous danger' Molotch contends that top-down security should be avoided and in its place flexibility and responsibility given to those 'on the ground' who are better suited to understanding and responding to the reality of risk environments. Turning

to the case of the government's attempted Bill, however, there is a case for both sides of this argument.

First, the government did not plan to solely wield the powers of the Bill. The discussion comes back to this momentarily but the mediation of surveillance – empowering CSPs to collect and retain communications data – is a step towards allowing those who are best placed to do the job of security. Zittrain (2003) calls CSPs natural 'points of control' on the Internet. Mediation of this sort is, therefore, instrumental and more than a little shrewd, but it can help avoid the criticisms of top-down, heavy-handed, centralised methods of control that Molotch (2012) outlines. Moreover, the desire to future-proof the Bill is reminiscent of Molotch's suggestion that security measures should 'leverage redesign' (2012: 218-19). That is, they should serve multiple purposes and focus on wider, long-term goals.

The second side to the argument countermands this. The reality is that CSPs would not have been given any flexibility, being compelled to collect and retain whatever data the government instructed. As Molotch predicts – and as the findings are testament to – the implementation of the powers in the CDB would ignore many side-effects; the revelation of personal information from communication data, the obfuscation of existing regulation, the vulnerability of data and the infringement of civil liberties. Doing this runs contrary to what Molotch describes as the 'default to decency'; when presented with a risky situation or environment to regulate, the approach should be that which preserves the rights of individuals and groups. Contrary to this, Clark (2014) notes how states are resorting to deception to persuade the public of the need for mass surveillance. This is the paradox alluded to previously. Security is about protecting freedoms and liberties. If these goals can be better met by *not* implementing a surveillance regime like the CDB, surely that is the right solution. It is a question of necessity and proportionality.

6.8.2 MEDIATED SURVEILLANCE

The 'central plank' of the CDB was a collaborative relationship between government and CSPs, both in the UK and overseas. Elements of this have surfaced throughout the discussion. 'Mediation' emerges as the mechanism by which the government attempted to implement a digital surveillance regime in pursuit of a wider crime

prevention and security agenda. There is already excellent work done on the topic of mediated surveillance by Bright and Agustina (2013). Their three hypotheses of mediated surveillance state that 1) it occurs in situations where institutions have incomplete power or information, 2) a significant degree of coercion is required to mediate surveillance, and 3) mediation has significant consequences for the effectiveness with which surveillance is carried out, including the opportunity for circumvention by the surveilled (2013: 123). The findings presented here are consistent with at least the first two of these hypotheses. The first is shown by the identified 'capability gap' and the tacit acknowledgement that CSPs are in the best position as 'points of control' to remedy this. The second is evidenced by the fact that the Bill mandated CSPs to retain CD – there would have been little scope for negotiation[175].

> 'I think we really do have to recognise the step change here, from a position where companies keep information for their own commercial purposes to a situation where we are effectively contracting out responsibility for keeping records on the entire population for future law enforcement purposes.' (Rachel Robinson – *Advocacy/Non-Profit*, CDB Oral Evidence, p.91)

It is likely the third hypothesis would play out, although that is of course only conjecture. However, given the frequent argument that criminals would find a way to bypass the measures, we can presume this would be the case. We can also look at mediation more broadly. While CSPs are the locus of mediation, other individuals and authorities are implicated in the process; SPoCs, DSOs and the IoCC.

Mediation can be understood as a problem-solving exercise in surveillance. It provides some of the answers to the uncertainty faced by government and is simultaneously a means of allaying fears. The abandonment of the centralised database, for example, is suggestive of this. However, mediation presents its own challenges when we factor in jurisdictionality. It does not seem to be the case that devolving responsibility or co-opting the riches of the private sector is a panacea. Third-party data remains elusive – at least in the way the UK government envisaged.

As suggested above, mediation is also closely tied to theoretical work on assemblages. In the context of this case study we have on the one hand a multiplicity of organisations, institutions and individuals engaged in the activity of

[175] By passing DRIP in 2014, this is essentially what Parliament achieved.

surveilling one another (usually in unequal measure). On the other hand we have a multi-actor network that is engaged in resisting surveillance (see Martin *et al.* 2009 and Chapter Five), the possibilities for which are enlarged by the very process of mediation (Bright and Agustina 2013: 132). All of these actors help to constitute a surveillance assemblage. As well as *permitting* the rhizomatic operation of surveillance systems across society, this assemblage is continually engaged in the process of *negotiating* surveillance in new environments. Recent contributions to the wider literature on risk regulation are instructive here. Hutter and Lloyd-Bostock (2013) for example discuss how an array of interest groups becomes involved in defining risk expectations and shaping regulatory responses. Two extracts from this discussion resonate with this case study. They note that 'the central justification of regulation is that it controls undesirable risk and it is embedded in socio-cultural and political risk environments which are in the business of managing feelings of vulnerability and *demands for security*' (2013: 398, *emphasis added*). Risk, growing from an inadequate surveillance capability in the midst of technological change, was the justification of the CDB. However the proposals in the Bill had the unintended effect that 'regulation came to be framed as itself a source of risk' (Hutter and Lloyd-Bostock 2013: 400). A final lesson from the authors is picked up in the next chapter; that such a flurry of regulatory activity emerges at times of crisis.

6.8.3 CONCLUSION

This chapter has shown a specific instance of the interaction between digital surveillance and resistance. The setting for this has been the regulatory arena. Consequently, the nature of the resistance seen is not of the 'technological fix' variety (Dupont 2008; see also Marx 2003) – the deliberate evasion or neutralisation of a specific digital surveillance technology. Rather it is a collective process of constructing counter-arguments to the proposed regulation of surveillance and attempts to have resistance codified in law[176]. Sometimes this is through cooperation between individuals and groups and other times as a result of individual

[176] This is a process (and an opportunity) that has continued since the fieldwork was conducted. The Investigatory Powers Bill (2015) underwent a similar process of consultation and, given it appears to be progressing towards enactment, represents a milestone for codification of some the principles being advocated by privacy campaigners – however small the government's concession on these may ultimately be.

efforts. Particularly in the case of individual/non-expert respondents and advocacy groups, this was an instance of putting 'information politics' (Bennett 2008) into practice. The chapter has also shown a key feature of digital surveillance in the information society; that it is framed by complex regulatory practice, a necessity given the favoured approach of 'mediating' surveillance. Regulation and digital surveillance are increasingly intertwined and consequently regulation generates specific effects of resistance that impact the nature of surveillance.

The case study of the CDB contributes to guiding narrative of the thesis. In particular, it provides a great amount of detail as to *why* individuals and groups choose to resist digital surveillance (research question two). These include: the 'intrusion fallacy' (that communications data can be just as revealing as content); problems relating to the jurisdiction in which data are collected and transmitted (in particular with overseas/third-party data); the potential for function creep inherent in surveillance legislation, and; inadequate oversight and security mechanisms. The chapter has also fleshed out the relationship between digital surveillance and resistance (research question one) by illustrating a specific instance of this relationship. Last, there are implications for understanding contemporary social control (research question three) that are informed by the focus on both regulation and surveillance. Centralising and decentralising impulses discussed earlier are one important theme here and this is returned to in Chapter Eight.

Regulation and surveillance are modes of social control that are intrinsically connected. In combination they dictate much of the national surveillance experience, whether this surveillance is political or economic. Despite this, there is typically little opportunity for nodes beyond the public and private sector to participate formally in the process of shaping the regulation that governs how they are surveilled. The consultation on the CDB accommodated this and, from a research perspective, offered valuable insights into the types of issues that were negotiated and contested between the various groups involved.

Acknowledging the wealth of data held by private CSPs, the 'central plank' of the CDB was collaboration between government and these organisations. From the data, this relationship appeared to be a tense one. Although some CSPs supported the rationale behind the CDB and some of its proposals, the issue of allowing the law

enforcement to request third-party data was rejected unanimously on both technical and jurisdictional grounds.

Being alert to the changing nature of the public-private relationship is also necessary for developing an understanding of contemporary social control. Cohen (1985) discusses various characteristics associated with privatisation of control. He observes that 'huge areas of public life previously under state control are now in the hands of private corporations' (1985: 67). This remains applicable in the information society. A broader debate the CDB thus speaks to in the context of this thesis is one of ownership and control of the virtual spaces of the Internet. The CDB is only one example yet it continues a trend[177] of increasing regulatory activity by the state that attempts to responsibilise (see Stenning 2000), private corporations to create, maintain and enforce social order online.

All of this helps to clarify the nature of resistance at the level of regulation. In the previous chapter, the constitution of the advocacy community online revealed the potential for the geographically dispersed community to quickly respond to real world 'surveillance events'. The CDB was one such event and the consultation revealed the participation of several prominent nodes from the network of privacy advocates. Alongside these, many others emerged who partook in negotiating what, in the context of digital surveillance, is necessary and proportionate. This shows the broader constitution of the network of governing nodes that contribute to the framing of surveillance issues. The categorisation of respondents outlined at the start of the chapter helps to indicate how each of these groups constructed their responses around certain themes. Some categories primarily addressed specific issues, while others spoke more broadly to an array of concerns. Drawing out these patterns reinforces the multi-actor character of resistance (Martin *et al.* 2009) and counter-resistance at the level of regulation[178].

Much of this chapter has demonstrated the truth in the assertion that 'the law has failed to keep pace with the ever more sophisticated surveillance techniques available…' (Akdeniz *et al.* 2001: 19). The government would argue slightly

[177] For instance, see Chapter Three and also the earlier discussion in this chapter of Lessig's (1999) contributions on 'East Coast' versus 'West Coast' code.
[178] See Appendix H for a summary of these positions.

differently; that the law has failed to keep pace with risks posed by new technology. The underlying assumption is the same: effective regulation is the favoured way to manage the various risks posed by technology. The trend, as Vogel (2012) has argued, is that regulation in Europe has become increasingly precautionary. In the context of regulating digital surveillance, measures are justified on the basis of protection from known and unknown threats arising from a new communication environment. Blanket surveillance, as opposed to court-sanctioned, targeted surveillance (Brown 2010) indicates this preference for precaution. However, the context of digital surveillance challenges Vogel's (2012) claim that while precaution characterises European regulation the US has shifted towards evidence-based approaches. Pursuing an agenda against terrorism on each side of the Atlantic, *both* the UK and US governments have sought to pre-emptively harvest and retain enormous quantities of Internet traffic data for subsequent analysis by intelligence agencies. Yet, these developments problematise the study of regulation because the activities of the intelligence agencies have been, for the most part, *un*regulated or at the very least, subject to little oversight and accountability.

Regulation (of digital surveillance) is highly relevant facet of social control. This case study showed an attempt at regulating digital surveillance that was reflective of neither the contemporary technological environment, nor people's concerns about communications data. The rapidly changing and diverse nature of digital communications means that such attempts to regulate the environment for the purposes of crime prevention are lacking in precision and are resultantly resisted for the dangers such ill-conceived attempts represent. Running counter to the 'default to decency' (Molotch 2012) like this will likely engender more resistance in future.

This produces a new regulatory dilemma. Surveillance infrastructures must be regulated according to the same principle that regulation like the CDB attempted to fulfil in the first place; protection of the public against threats to civil liberties. The current 'state of exception' (Agamben 2005) has resulted in the need to regulate against the types of protective measures that were designed in the first place. Trust and public consent are vital; the social order we are trying to preserve should not be undermined by the very surveillance and regulation that aims to protect it.

.. .- ... -.- -.-- --- ..- --- ..-. - .... . .--. .- ... - - --- .-.. . .- ...- . ..- ... .- .-.. --- -. . .-.-.-

CHAPTER SEVEN

NEWS AND NEW MEDIA: THE LEGACY OF THE CYPHERPUNKS

7.1 INTRODUCTION

This is the final substantive empirical chapter of the thesis. It examines the symbolic and communicative aspects of the relationship between digital surveillance and resistance. To do this, the chapter focuses on two instances of 'resistive surveillance': new media platform WikiLeaks and the later revelations about mass surveillance from Edward Snowden. The WikiLeaks case illuminates one element of the surveillance/resistance relationship – how resistance to digital surveillance (i.e. resistive surveillance) capitalises on the potential inherent in the socio-technical medium of the Internet. This constitutes the first half of the chapter and is informed by qualitative data from the interview with Daniel (a co-founder of WikiLeaks) supplemented by secondary data from interviews and documentaries about Julian Assange and WikiLeaks.

The WikiLeaks case, in combination with the case of Snowden, also shows how resistive surveillance is met with counter-resistance efforts. These efforts are represented in the second half of the chapter by analysis of reporting in the news media. To make sense of the series of claims and counter-claims made about surveillance and resistive surveillance the concept of moral panic is used as an analytical framework. Doing so allows for a discussion concerning the construction of social problems and moral panics in the context of surveillance and resistive surveillance. In closing, the chapter takes a broader look at the implications of this recent history of public discourse around digital surveillance for understanding the role of the media in the relationship between digital surveillance and resistance.

7.1.1 ON SOCIAL PROBLEMS AND MORAL PANIC

The closely related issues of social problems and moral panics share a foundation in social constructionism. This approach focuses on the ways different groups attempt to define certain acts, practices or issues as problematic for society and in need of a response. However, defining a problem is far from straightforward. It brings social actors into conflict with one another, as each try to impose their version of events as the 'true' account, whether that it is 'the problem has been caused by the failings of this group', 'there is no problem', 'there is a problem, but it is not the way it has been portrayed' or ' the problem is not as bad as it seems and can be justified' (Cohen 2002: xli). Moral panics, characterised by the exaggeration of a threat to the social order, are an example a very specific form of societal reaction to the construction of a problem. This occurs most often with the assistance of mass media reporting:

> 'The student of moral enterprise cannot but pay particular attention to the role of the mass media in defining and shaping social problems.' (Cohen 1972: 16)

Constructing a problem does not require the existence of a moral panic. Moral panic, on the other hand, is an example of the construction of a social problem but to label it a 'panic' is to draw attention to the disproportionate reaction it receives. Related to this are questions of why this issue has been reported in the way it has, whose purposes the panic appears to favour and why some (trivial) issues generate such a response while other (catastrophic) issues do not. Moral panics are 'condensed political struggles' and exploring them 'allows us to identify and conceptualise the lines of power in any society' (Cohen 2002: xliv). Key to swaying people's perception of a problem, then, is control over information and this chapter illustrates two aspects of this: news media reporting, and the ability to access and make public confidential information.

These issues resonate with a study of surveillance and resistance. In fact, much of what this thesis has shown so far could be incorporated into a study of, if not moral panic, then certainly the construction of social problems. The Communications Data Bill is a good example of this. The oral and written evidence quite obviously illustrate claims and counter-claims regarding the necessity and proportionality of digital surveillance. But resistance to surveillance in its widest terms also

exemplifies the efforts to which individuals and groups go to construct surveillance practices as dangerous, or as a risk to personal privacy and civil liberties. 'Information politics', the favoured strategy employed by the privacy advocates from Chapter Five, is further evidence of on-going claims-making about such risks.

Risk and moral panic share some of the same conceptual ground. Risk (incorporating both information about objective threats and the ways to respond to them) has colonised some of the sociological space once occupied by moral panic (Cohen 2002). It has produced a reflexive and more technical way of identifying problems and how to deal with them; however, statements about risk can still devolve into moral judgements, for instance regarding the integrity of 'experts' or the proportionality of the proposed solutions (Cohen 2002: xxx-xxxi). Surveillance, for instance, is promoted as a technological solution to the insecurities arising from increased crime rates or the risk of terror attacks (Ceyhan 2008). However, when surveillance extends to the indiscriminate bulk collection of digitised personal data, moral judgements arise regarding invasion of privacy, trust in those who collect and retain the data and the transparency of regulation that permits such practices. Some of this will sound familiar. These themes continue in this chapter, where we see repeated instances of surveillance practices being forcibly opened to scrutiny to construct them as problematic and risky. The counter-claims are evidenced too: that revealing confidential information about the state and about surveillance systems increases the risks they are intended to protect. WikiLeaks, Julian Assange and Edward Snowden were vilified and celebrated in equal measure. The events described in this chapter from 2007 are thus an effective backdrop to explore the shifting relationship between digital surveillance and resistance.

The framework of moral panic and social problems, then, guides the analysis of the empirical data. However, the chapter is not so much concerned with proclaiming the existence (or not) of a moral panic about digital or resistive surveillance. Instead, it uses some of the lessons of this framework to illuminate the presentation of troubling individuals and groups in the news media, the patterns of reporting on these over time, and the consequences of these for public consciousness and concern about digital surveillance. In that respect, this chapter picks up an important point from Chapter Five regarding the presence of news media in online

networks of privacy advocates and their ability to retain their power by occupying *online* spaces as well as 'offline'.

Cohen (1972) emphasised how he paid correspondingly less attention to the 'folk devils' than to the social reaction that followed. This chapter aims for more balance. Using the qualitative data it first describes and characterises WikiLeaks to 'set the scene' for what follows. Not only does this highlight why WikiLeaks were susceptible to negative constructions in the news media, it also shows how they were capable of their actions – and consequently, why they were the target of counter-resistance. The second half of the chapter charts the changes in patterns and tone of reporting on WikiLeaks and Edward Snowden in news media reporting to illustrate the competing claims-making about digital surveillance and resistive surveillance.

7.2 WIKILEAKS

Whistleblowing is a long-standing form of resistance; the circumventing of control measures to bring confidential information of perceived interest into the public domain (Conway 1977; Vandekerckhove 2006). In 2010, however, it found new currency with the emergence of a novel, online media platform: WikiLeaks (Greenberg 2012; Brevini *et al.* 2013). Built on a foundation of sophisticated encryption, WikiLeaks was able to encourage whistleblowers to reveal sensitive information. Exploiting the architecture of the Internet, they could consequently publish it without fear of reprisal. WikiLeaks actively sought evidence of censorship for 'while it is something to condemn, it is always an optimistic signal, it is always an opportunity, because censorship reveals the fear of reform by knowledge' (Julian Assange, *WikiLeaks: Secrets and Lies*).

WikiLeaks is associated most prominently with a series of leaked military and diplomatic communications. A brief history of WikiLeaks is presented below. However, before this a caveat is added to put the organisation into context. A large amount of WikiLeaks' publications were not the result of leaked information. WikiLeaks identifies itself as an investigative, journalistic, not-for-profit media organisation. To that end it publishes information that it believes is in the public interest but this is not, therefore, solely reliant upon whistleblowers. While the

whistleblowing aspect of WikiLeaks is important, the story presented here necessarily focuses on publications that were also the result of investigative efforts on the part of WikiLeaks and its ad hoc collaborators.

WikiLeaks (and more recent instances of whistleblowing) is helpful for developing our understanding of the relationship between surveillance and resistance. On the face of it there are obvious reasons why this could be: some of WikiLeaks' publications and all of those released by Edward Snowden pertain to various aspects of the surveillance complex. But this analysis aims to provide a more comprehensive account, drawing on the work of Cohen (1972) and also the concepts outlined in Chapter Three – sousveillance and the synopticon, broadly captured under the term resistive surveillance. Resistive surveillance, then, points to the ways that digital technologies are used to surveill those in authority and make their actions, and by extension surveillance practices, more visible to the surveilled.

7.2.1 A WHISTLE-STOP TOUR OF WIKILEAKS AND WHISTLE-BLOWING

WikiLeaks emerged in the public sphere slowly. The data below show that throughout the three-year period from 2007 to 2009, reports of WikiLeaks in UK publications were low-level and sporadic. Published leaks varied in style: political corruption in Kenya ('The Kroll Report'), financial malpractice by Swiss bank Julius Baer, the contents of US state governor Sarah Palin's emails and operational handbooks and documents from the Church of Scientology. In 2010, WikiLeaks arrived fully on the media stage. *Collateral Murder*[179] – video footage shot from an Apache helicopter in Iraq that showed the death of a number of civilians and two Reuters journalists – was released in April, followed by the publication of the *Afghan War Diary*[180] in July; 91,000 classified US military reports. Media impact increased further in October with the subsequent publication of the *Iraq War Logs*[181], at the time the largest release of classified military information (391,832 reports), followed by the *Cablegate*[182] incident in December; 251,287[183] US diplomatic cables, detailing correspondence between 274 US embassies and the State Department from 1966 to

[179] http://www.collateralmurder.com/
[180] https://wikileaks.org/wiki/Afghan_War_Diary,_2004-2010
[181] https://www.wikileaks.org/irq/
[182] https://wikileaks.org/cablegate.html
[183] According to WikiLeaks (2013), 15,652 of these cables were classified as 'secret'.

2010. The 'Arab Spring' events of 2011 were partly attributed to the corruption revealed by the release of the diplomatic cables (see Walker 2011).

Subsequent leaks did not generate the same level of media impact in the UK. April 2011 saw the publication of files relating to detainees at Guantanamo Bay and in September of that year attention returned to the diplomatic cables; WikiLeaks released the full archive of the cables without redactions that had been used to protect sources when the cables were initially released via media partners in 2010. At the end of 2011 and in early 2012 WikiLeaks released a series of related documents entitled *The Spy Files*[184] and the *Global Intelligence Files*[185]. The former detailed the international trade in surveillance technologies and saw WikiLeaks partner with several organisations including Privacy International. The latter consisted of over five million emails from US intelligence contractor Stratfor. These emails had been hacked by Anonymous and were used by WikiLeaks to demonstrate the 'inner workings…web of informers, pay-off structure, payment laundering techniques and psychological methods' (WikiLeaks 2014) of an intelligence firm that WikiLeaks alleged were employed by the US government to discredit their organisation (see Ball 2012) – just one instance of counter-resistance.

As the analysis below outlines, throughout 2012 the attention directed at WikiLeaks was a product of Editor-in-Chief Julian Assange's legal battle against extradition to Sweden from the UK. The failure of this culminated in his taking residency inside the Ecuadorian Embassy in London in June 2012 (where he was subsequently granted asylum) and where he remains to date, nearly four years later. In the interim, WikiLeaks have retained an offline and online (including social media) presence but any published leaks have failed to generate the type of impact seen in 2010. With the publication of Edward Snowden's revelations in June 2013, WikiLeaks enjoyed some renewed media attention (despite not being involved in publication). However this remained at a lower level than that seen in 2010. Likewise, Edward Snowden, the National Security Agency (NSA) and the Government Communications Headquarters (GCHQ) have all fuelled more media speculation in the intervening 18 months than WikiLeaks.

[184] https://www.wikileaks.org/the-spyfiles.html
[185] https://wikileaks.org/gifiles/

In sum it is worth noting a few key points. WikiLeaks use sophisticated encryption methods to protect the anonymity of their sources and they have never publicly revealed the identity of any whistleblowers. They have presented themselves throughout as an investigative journalistic platform committed to motives of press freedom and democracy, transparency and accountability in government. Over time, there has been a noticeable shift from a very 'broad brush' approach to a much more anti-US agenda in published information. Lastly, WikiLeaks have never been successfully subjected to censorship or termination of service.

7.2.2 TECHNOLOGY, JURISDICTION AND RESILIENCE

There are both social and technological aspects of the WikiLeaks phenomenon. These help to describe the operability of WikiLeaks and also reintroduce the centralisation/decentralisation concept from the previous chapter. The technological foundations of WikiLeaks are a logical starting point for analysis. Cryptography and code have always been the heart of the subversive culture of hackers, activists and cypherpunks. Greenberg (2012) tells the story of this culture as it grew throughout the last few decades and, importantly, the role of advances in encryption as a driving force behind online anti-authoritarian activism – resulting most recently in WikiLeaks. The keystone of WikiLeaks' capabilities was encryption designed to protect the anonymity of whistleblowers and thereby encourage them to leak information that might otherwise remain private. It is this that is largely responsible for the impact WikiLeaks had. For Daniel, this was part of his motivation for the project, as he said in interview:

> '…you have whistleblowers that are speaking out but there are not enough of these people so the idea was how do you, how do you, maximise this potential, how do you get the most out of it? And as such WikiLeaks was set out to provide an avenue on the Internet that is, that has a much lower barrier than anything else…classical ways that whistleblowers can use have quite a high barrier that one has to overcome and WikiLeaks' idea was to provide a barrier that was very low, that with three clicks you're done you know and the anonymity is part of the concept you don't have to worry about that and the question was if that was provided can we maximise the potential we have for whistleblowers, can we encourage more people? And that was at least for me, what this was always about – finding out if there was a potential and if so, tap into this potential.' (Daniel Domscheit-Berg)

By facilitating the ease with which whistleblowers could submit information and allaying fears of identification, WikiLeaks harnessed the potential of the distributed architecture of the Internet (see Galloway 2004[186]). Thus enabled, WikiLeaks acted as both sword and shield in respect of privacy; by leveraging confidential information they could undermine institutional secrecy while at the same time protecting the privacy of its sources. On another level there is a broader message here: online technology can be actively used to *not* surveill people (i.e. whistleblowers). It was not the case that WikiLeaks protected the identity of *known* sources. Rather, the cryptographic mechanisms ensured they *could not know* who the sources were. There is an interesting parallel in that respect with a Foucauldian reading of surveillance, namely that the initial (resistive) surveillance agent (the whistleblower) remains hidden from sight. This adds a different quality to resistive surveillance than 'information politics' seen earlier where resistance comes from known sources.

Coupled with this, there were techno-legal mechanisms employed by WikiLeaks that help to explain its resilience. As Julian Assange described in a TED interview in 2010:

> 'we use this state-of-the-art encryption to bounce stuff around the Internet, to hide trails, pass it through legal jurisdictions like Sweden and Belgium to enact those legal protections.'

WikiLeaks located servers around the world to facilitate this global transfer of information. This took advantage of the legal protections that passing virtual information through a jurisdiction invokes. Jurisdictionality, as the previous chapter indicated, is an important component in understanding contemporary digital surveillance and resistance. This also permitted WikiLeaks to host 'mirror' (duplicate) websites. Should one website be targeted by an injunction (as it was in February 2008 following the Julius Baer incident), the service can still be accessed via the Internet as traffic is routed to another of the duplicates hosted elsewhere. Combined, these technological and techno-legal aspects were the operational foundation of WikiLeaks. They illustrate why WikiLeaks is an exemplar of resistance in the digital environment and the potential of digital technology to generate new

[186] That is to say, they exploited the way in which is the Internet is regulated or coded (Lessig 1999) in order for it to operate effectively for subversive purposes.

and resilient forms of resistance. The point was made in Chapter Three that counter-resistance can only for a short time debilitate such efforts.

On an organisational level, WikiLeaks made use of a decentralised network form to great effect; centralising the organisation would have made counter-resistance a much easier prospect. With WikiLeaks, we are presented with a form of resistance that has arisen out of a specific set of technical (as well as social and cultural) circumstances. Decentralisation is not necessarily the way online resistance *has* to happen; but it is the way that is most effective within the architecture of the Internet as it currently stands[187]. As Lessig (1999: 30) says, 'the possible architectures of cyberspace are many.' It stands to reason that the possible architectures of resistance are equally numerous.

Despite the preference for – and the necessity of – a decentralised model in technical terms, centralisation was still required by WikiLeaks to some extent. Setting WikiLeaks up as the 'gold standard' of whistleblowing and source protection was a logical precursor to centralisation of information. WikiLeaks had to remain in control of all information received or their guarantee of protection for whistleblowers would be undermined. However, this is where a tension emerged. WikiLeaks' mission statement – 'we open governments' – was constructed in the pursuit of transparency and accountability and as this brief history of WikiLeaks depicts, this expanded to many corporate institutions and organisations. WikiLeaks' strict control of leaked information, while somewhat necessary, ran counter to this. By attempting to restrict mainstream media access to this information, and using their own privileged access to release un-redacted material, tensions grew between WikiLeaks and their media partners. The technical aspect of control over information thereby begins to overlap with social and organisational aspects of WikiLeaks.

Much of what has been said here overlaps with the centralising/decentralising dyad introduced in Chapter Six. The two themes discussed there (Internet architecture and information/services) are also evidenced here. A third theme emerged from what Daniel had to say about centralisation and decentralisation as organisational

[187] Recall the discussion in Chapter Five regarding the mobilising potential of a flexible, distributed network of advocacy groups.

principles; specifically that decentralising information flows is a preferable strategy. Daniel saw decentralisation as the preferred means of communicating leaked information, i.e., in opposition to the way in which WikiLeaks operated. Daniel's vision for an organisation of this kind was that it should strive for neutrality, acting as an intermediary between whistleblowers and a variety of actors – such as news media, advocacy groups and NGOs – who could use the information for different purposes and reach a broader audience.

> 'I think it's a question of how centralised this whole network is. In this chain of how information flows you know, somewhere there is information and then on the other end very far away there are these people that actually should care about the information. Now let's say the information, I don't know, is a 180-page military document, then all these people cannot have access to that because even if they would read it they probably wouldn't understand it, they'd be bored as hell after five pages and they wouldn't look it into it any further, they wouldn't understand the language the acronyms and all of that. So you need somebody mediating in between.'

The mediator (WikiLeaks) would be an interpreter. However, despite Daniel's claim, it would likely be difficult to absolve the organisation of a central role in this regard as interpretation, translation and subsequently highlighting important features of the information are crucial functions. Clarifying his position, he noted:

> 'The more decentralised you do that and the more layers you are adding I think the better it is, because first of all you're spreading it better…second it is not only particular organisations that is in control of the whole interpretation flow. You know if it's just one organisation that has access to it and that can publish it and interpret it and all of that then they can make a lot of politics of this but in a more decentralised model it keeps everybody honest because everybody is just this smaller player in the whole picture.' (Daniel)

Daniel's argument[188] is the same as that proposed in Chapter Five where resistance was portrayed as a networked, mainly collaborative project. Information flows within this network were dynamic, changing over time and in response to real-world events. While certain actors were shown to be prominent, there was no central hub through which information had to be relayed in order to reach an audience. This model is different from that enacted by WikiLeaks. WikiLeaks did collaborate with other organisations but these relationships were tenuous and fraught, and the

[188] As an aside, while Daniel's critique of centralisation of this type is entirely valid, his personal position in this debate should be acknowledged. His departure from WikiLeaks was an acrimonious one and therefore a degree of discontent with its operation is to be expected.

tendency towards centralisation was evident in a number of ways. Whether this proved to be an obstacle will be discussed later.

7.2.3 RATIONALE

The rationale behind WikiLeaks is complex and debated, particularly as the goals of the organisation became entwined with the status and profile of Assange. The original motivation behind WikiLeaks still perseveres in some form: forcing transparency on closed institutions and demanding accountability from government. Daniel's remarks above showed his motivation for joining WikiLeaks: lowering the barrier to whistleblowing, making it simple and reassuring. During another interview, Eric King of Privacy International echoed this sentiment; he felt that 'nurturing that community is really important.' However, this original USP – providing a safe and secure avenue for whistleblowers – was somewhat undermined in the aftermath of the prosecution and sentencing of Chelsea ing[189] in the US in 2013. In hindsight, Daniel had reservations. He explained that he felt some of what WikiLeaks engaged in was not working towards the broader agenda of transparency and accountability:

> 'I don't believe in abolishing secrecy completely, this is not what, this is too easy and the world is more complicated than this and this is a bit what the agenda has become today so it's more like a campaign platform against secrecy rather than a support platform for whistleblowers. Today I'm wondering a little bit about whether this has been the case right from the beginning and whether the whole whistleblower thing was just very easy to sell and this was why it had been promoted.'

Daniel distinguished between three types of activities WikiLeaks has carried out, each of which appear to show different rationales for publishing information: *whistleblowing*, *anti-secrecy* and what he later referred to as '*lobbying for awareness*'. Anti-secrecy, as his remarks indicate, was on the whole not considered a worthwhile pursuit and did not serve the public interest. Lobbying for awareness, as a subset of anti-secrecy (and tied more to WikiLeaks' role as an investigative journalistic platform), was more valuable and it is at this point we can turn to the matter of digital surveillance.

[189] A US soldier, PFC Bradley Manning was prosecuted for leaking confidential military and diplomatic communications to WikiLeaks, accessed while stationed in Iraq. In 2013, Manning announced she had experienced gender dysphoria for several years and that her new identity was Chelsea Manning.

It is possible to debate, ad infinitum, what WikiLeaks hoped to achieve with each of their publications. What we are interested in here is the ability of the case of WikiLeaks to shed light on our understanding of new media and resistance to surveillance. *The Spy Files* open the door to this discussion. Speaking to the Bureau of Investigative Journalism (with whom WikiLeaks and Privacy International collaborated), Assange described the motivation behind the release of information pertaining to the global surveillance-industrial complex. Over 90 companies are subject to scrutiny in the publications, which consist of prospectuses, presentations and pricelists for mass surveillance products, among other documents.

> 'There is little left of democratic life that is not surveilled. But it is not being surveilled equally, it is not the public that is surveilling big corporations, secretive government agencies and the rest of the public, rather there is a disproportionate flow of information from us, from the public, into organisations that are already very powerful. And that permits the elite, the surveillance elite, the national security elite of a country to lift off from its people, to disconnect from its people, to predict its people. Now that's a dangerous situation and what we're dealing with here is not merely the surveillance elite of one country operating alone but rather an international surveillance elite, transnational companies selling these [mass surveillance] products all over the world and intelligence agencies swapping data that they collect with each other, that's a worrying situation for Western democracy.'(Julian Assange [video transcript] in Chatterjee 2011).

These remarks indicate why WikiLeaks targeted the international surveillance industry, with the familiar political-economic surveillance dyad emerging once again. There are notions of equality and democracy that are in line with WikiLeaks' original motivations. Assange also suggested that *The Spy Files* release may place pressure on governments to create better export regulation 'so that Western companies can't sell mass surveillance equipment to regimes that abuse human rights' (in Chatterjee 2011). Rather than exposing corruption this appears to be a more measured attempt at opening a discussion about the extent of political and economic surveillance and the need to regulate the surveillance industry.

Assange's claim that life is 'not being surveilled equally' implies the need to level the playing field. WikiLeaks' strategy of 'opening up' was designed to redress the imbalance in the flow of information from the public to powerful public and private entities. This exemplifies 'resistive surveillance' in that it captures elements of both sousveillance (Mann *et al.* 2003) – using technological means to invert the panoptic gaze and observe those in authority – and the synopticon (Mathiesen 1997) –

illustrating the role of (news) media in making the actions of the elite more visible. In the case of the latter it is more apt to consider Doyle's (2011) reconfiguration of the synopticon to account for its resistive potential rather than its ability to maintain the surveillance status quo.

7.2.4 ORGANISATION AND 'DICTATORSHIP OF ACTION'

Finally, there are useful observations regarding the social organisational aspects of WikiLeaks. The organisational forms of technological activist groups have been explored by Milan (2013). She notes that within such groups there is a characteristic horizontality and decentralisation in organisational structure. This may include multiple or alternating leaders or a collective 'all in' approach. Others 'give the right to centrality and uniqueness of the individual' (2013: 93). There can be consensus-building but frequently individuals decide on a course for action by themselves and are allowed to pursue this on a basis of 'inferred consensus' resulting from a shared set of values amongst activists. Milan refers to this as 'dictatorship of action' (2013: 93-4).

The organisational culture of WikiLeaks appears to depart from this model. Many critical accounts from former staff and media partners paint a picture of Julian Assange as controlling and willing to privilege his own interests above those of the principles of WikiLeaks (see Domscheit-Berg 2011; Leigh and Harding 2011; Beckett and Ball 2012; Ball 2013). Assange himself is a former hacker, however, those beliefs in decentralised organisation characteristic of activist/hacker culture (Milan 2013) did not appear, entirely, to be carried into WikiLeaks. On the contrary, as WikiLeaks achieved recognition, Assange became the figurehead of the organisation. The management of WikiLeaks was, perhaps, less 'dictatorship of action' and more 'dictatorship'. At other times, he is described as the 'charismatic leader' (Brooke 2011: 41). Although a trait that undoubtedly helped WikiLeaks to forge its path, this adds further support to the argument that the organisation ran according to Assange's rules and not the principles of participation, democracy and horizontality – particularly during its most prominent phase.

> 'Julian brought with him a rather strange quality; he carried himself as though he were a cult leader. We started making jokes very early on about people around Julian drinking the Kool-Aid…all this made you feel as though you were

> dealing with someone who wasn't quite from the same planet as the rest of us.' (David Leigh, *WikiLeaks: Secrets and Lies*)

None of this is designed to pass judgement on these issues. They are important in sociological terms to the extent that they inform our understanding of why a group such as WikiLeaks faltered in the long term. Resistance of this kind depends not only on powerful technological foundations but also organisational characteristics that do not destabilise the potential for resistance that exists. Daniel described how he felt WikiLeaks should have adapted in this situation:

> '…when this whole thing in 2010 started to go in a really strange direction I said the only thing that needs to happen is that it burns. It needs to burn down to the ground and cease to exist. And then the phoenix can rise from the ashes as something new. WikiLeaks is not in a position to really make a difference. There have been so many mistakes that have happened; so many people have been scared away, so many people that have been made angry by how things have been published, by mistakes that have been made, all of that. I don't think this is sustainable anymore.'

Daniel believed the concept of WikiLeaks was sound but organisational factors undermined its potential. This theme, along with the relations between WikiLeaks and its collaborators indicate two points to take forward. First, despite their technological sophistication, news media partners were still vital to the impact WikiLeaks could generate. This is reinforced by the patterns of reporting seen with the Snowden revelations. Consequently, it is important to appreciate the position of both traditional and new media platforms in contemporary surveillance relationships. This is a point that echoes from Chapter Five, where we saw the 'egocentric' tendencies of WikiLeaks on social media and the online presence of traditional news media. Second, we can relate perceptions of WikiLeaks and Assange to the broader issues of social problems and moral panics. For claims-makers, *trust* and *credibility* is vital if arguments are to be maintained. Loss of credibility also helps the agenda of creating folk devils out of whistleblowers.

7.3 TIMELINE OF THE NEW DIGITAL ANARCHISTS

Media analysis covering a period of four years shows the pattern of reporting on a variety of issues related to WikiLeaks and surveillance. Initially, this analysis was focused only on the prominence of WikiLeaks in UK publications (primarily the news media) and the relative discussion of surveillance and privacy. In the aftermath of

the revelations from Edward Snowden in 2013, the focus was extended to show the impact of these events in comparison to the reporting of WikiLeaks[190]. Figure 9 shows clear points over the four-year period where the volume of media reports of these themes increased significantly. The major fluctuations of interest concerned WikiLeaks and Assange in 2010 through to 2011 and Snowden in 2013. Also of importance are the patterns in late 2011 and early 2012 for surveillance and privacy; while they are less pronounced than those of WikiLeaks, Assange and Snowden, they still indicate the impact of particular moments in the recent history of surveillance.

From an analytical perspective the following discussion highlights the importance of considering 'crisis moments' in the on-going process of the construction of surveillance as a problem. Privacy advocates, as Bennett (2008: 225) notes, are often perceived as waiting for a 'privacy apocalypse', a major violation that will be the final straw that motivates the wider public to mobilise and confront unjustifiable intrusion into our private lives. Opinions from three interview participants were mixed on this issue:

> 'Yes, a lot of these sparks you can see. You see with ACTA[191] for example, the only spark it required was a really well-made YouTube video and that is what made the people understand what is happening that made my parents able to understand it and to suddenly have an opinion on a topic they've before that thought was completely irrelevant. And the same for SOPA[192] and PIPA[193] and the same for the German censorship law that they wanted to introduce…if you give people a tangible introduction to this topic, something they can relate to, then they can become politicised.' (Daniel)

> 'There are triggers all the time…It's in the media and it's there for a couple of weeks and everybody's shocked and like 'oh my god' the consequences that such a tiny mistake can have and you know the novelty wears off and people do it again…' (Anne-Marie Oostveen)

> '…whilst I think privacy is a genuine concern for society very few people instantly die because of a privacy violation, you know it does happen, but I think it's not something, there's sort of a deep-seated psychological where we're not, we're obviously not built to deal with this kind of issue, we're not programmed to deal with this kind of issue it's far away and abstract…' (Joss Wright)

---

[190] See Chapter Four.

[191] The Anti-Counterfeiting Trade Agreement, a multilateral policy that generated uproar amongst the Internet community for its potential to undermine net freedoms and the transfer of vital intellectual property (including medicine) across borders.

[192] Stop Online Piracy Act (US). Shelved: opponents argued this would open the door to unjustified and blanket online censorship.

[193] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property (PROTECT IP) Act (US). Shelved due to concerns over Internet freedom of speech, innovation and integrity.

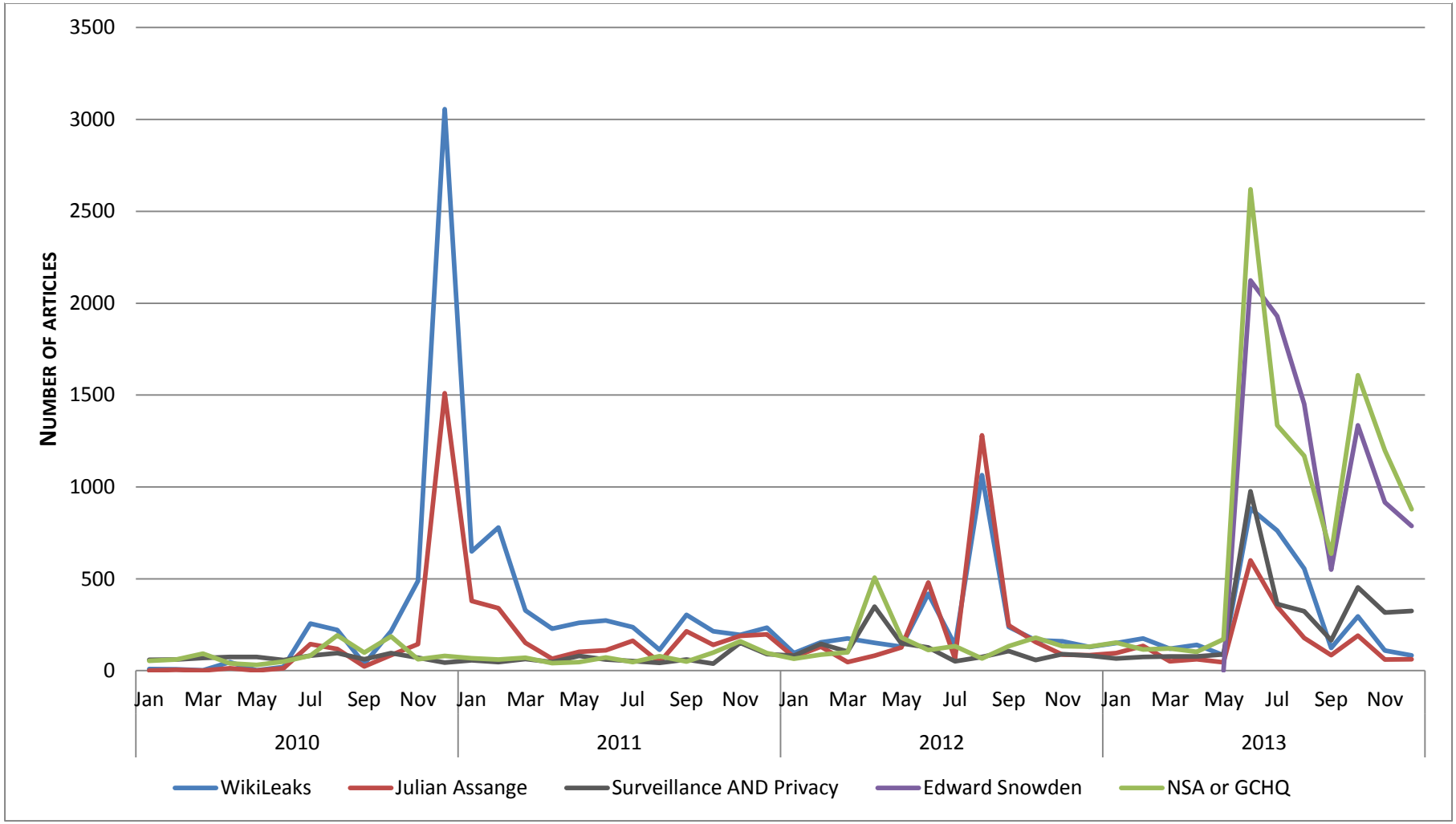
These excerpts raise two issues: the transience of surveillance/privacy stories in the news and the relevance and translatability of these for the public. The questions about digital surveillance are plain. Is it a social problem? Has it, or will it ever, generate a public outcry? As sociologists we should also bear in mind these questions carry their own moral judgement that (excessive) digital surveillance is a bad thing. The counter-argument is a familiar one: if you have nothing to hide, you have nothing to fear. This rhetoric exists to nullify any claims about the dangers of surveillance and can be combined with attempts to de-legitimise those claiming otherwise.

7.3.1 IMPACTS, INVENTORIES AND REACTION

The findings begin to point to an answer to the questions above. To begin with, the main period of interest in the WikiLeaks case is from mid-2010 through to the end of 2011. This period covers the bulk of significant publications/leaks as well as the time when WikiLeaks was most often in the news, as seen in Figure 9. The publications relating to digital surveillance practices appeared in late 2011 and actually garnered very little coverage, both in comparison to earlier leaks and to the later revelations by Snowden. Only seven articles in December 2011 mention 'Spy Files' and thirteen mention both 'WikiLeaks' and 'surveillance'. Of these, seven were the Spy Files reports and three were irrelevant. The tone was also entirely neutral; in the case of the Spy Files, the short articles[194] quoted Assange at the launch event with little elaboration on the rationale or consequences of the leaks. Only one of the thirteen articles – 'www.friend or foe?' (Kelly 2011) – engaged in debate about the liberating or repressive possibilities of the Web. WikiLeaks and surveillance are mentioned only once here and even then, not in relation to one another.

[194] Typically under 200 words.

FIGURE 9: THEMATIC REPORTING IN UK PUBLICATIONS 2010-2013



While this evidences little specific connection between WikiLeaks and resistance to digital surveillance, the relevance of WikiLeaks for this analysis lies elsewhere. To put these findings into context, then, we need to look at the earlier trajectory of WikiLeaks in the news media.

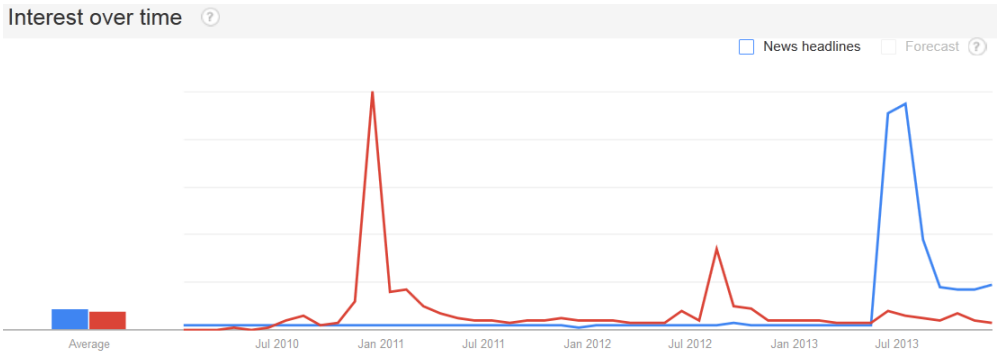
Cohen's (1972) exposition of the patterns of moral panics was based on observations from natural disaster research. He outlined a process of warning, impact, inventory and reaction to describe a typical sequence of events that make up a deviant incident: its antecedents, the occurrence of the incident, the reporting of these behaviours in the news media and the social reaction to them. The reaction phase was most critical, for it was here where attitudes towards the subject of the panic were shaped and crystallised into a broader perception of the 'problem'. Through cycles of amplification in the new media, subsequent reactions to otherwise minor transgressions were disproportionate and served to further demonise those engaged in the initial deviant behaviour. We do not need to apply this model to the letter. Indeed, later authors have critiqued the specifics of what Cohen proposed (see Goode and Ben-Yehuda 1994; McRobbie and Thornton 1995; Jewkes 2004; Altheide 2009) and Cohen himself revised his elaboration of the concept of moral panic in subsequent editions of *Folk Devils* (1980, 1987, 2002). Aspects of these revisions will be revisited later. Nevertheless, the model helps to draw out some of the key elements of the WikiLeaks case.

There are clear 'spikes' in the pattern of reporting on WikiLeaks and Julian Assange in Figure 9. Where they begin to converge indicates that, over time, reports of WikiLeaks became conflated with those of Assange; conversely articles in 2010 and early 2011 mentioned WikiLeaks more without reference to Assange, indicating more focus being paid to the organisation and the publications they had released. There was arguably a 'novelty' factor at play as well, which is one explanation for the gradually decreasing volume of news coverage over the period. The leaking of enormous quantities of confidential information in the *War Diaries* and *Cablegate* was hitherto unseen. In interview, Daniel alluded to the fact that WikiLeaks' earlier publications were reported not so much for their content but for the fact that something had leaked. In his opinion, this was 'wasting a lot of the information that could actually make a difference.' In the UK context this is understandable, as the

War Diaries and *Cablegate* had direct relevance to the UK and US government. Pre-2010, the publications were not so pertinent. Naturally the content of these leaks was of interest to the news media, but the perceived public appetite for these would have to be great to sustain such reporting over a longer period of time. Relatedly, another argument for the much less significant impact of *The Spy Files* in December 2011 and January 2012 is the issue of 'translatability' discussed below.

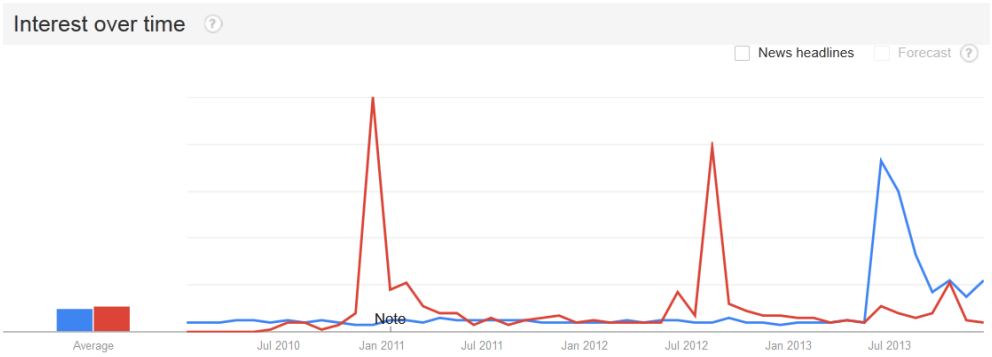
Figures 10 and 11 below validate the findings of the frequency analysis in Figure 9. They indicate worldwide and UK 'interest' (signified by volume of Google searches) in Assange (and Snowden[195]) across the same four-year period[196]. The patterns are almost identical to those in Figure 9. In addition, they provide a little nuance; interest in Assange was more pronounced in the UK in mid-2012 (when Assange took refuge in the Ecuadorian Embassy), while conversely, Snowden generated greater interest worldwide than in relative terms in the UK.

FIGURE 10: GOOGLE TRENDS RESULTS: WORLDWIDE INTEREST IN ASSANGE AND SNOWDEN 2010-2013 (WEB SEARCHES)



[195] Discussed in more detail later (section 7.3.2).
[196] The red and blue lines represent Assange and Snowden respectively.

FIGURE 11: GOOGLE TRENDS RESULTS: UK INTEREST IN ASSANGE AND SNOWDEN 2010-2013 (WEB SEARCHES)



The news media evidenced mixed responses during late 2010 (the inventory in Cohen's model). Some reports framed WikiLeaks or Assange as dangerous, some cast them in a more positive light and others appeared to leave it to the reader to decide, as these headlines illustrate:

- 'Who put WikiLeaks on the moral high ground? Secrecy causes damage but so can disclosure. Julian Assange has no right to decide which makes the greater evil' (*The Times*, 29th July 2010)
- 'WikiLeaks may already have blood on its hands over Afghan revelations' (*The Times*, 30th July 2010)
- 'Why WikiLeaks must be protected' (*New Statesman*, 23rd August 2010)
- 'Hail to the whistleblowers' (*The Guardian*, 23rd June 2010)
- 'Paranoid. Anarchic. Is WikiLeaker boss a force for good or chaos?' (*Daily Mail*, 27th July 2010)
- 'WikiLeaker crusade or ego trip?' (*Daily Telegraph*, 31st July 2010)

This division of opinion, which characterised the majority of news reports collected, signals the competing claims being made about what the social problem actually was. On the one hand the 'inventory' in response to the 'impact' of each batch of leaks was to praise the efforts of WikiLeaks and problematise the lack of transparency and accountability within government. On the other, it was to question the justification of WikiLeaks' actions, illustrate the damage they could cause and vilify the character of Assange.

Other reports indicate the broader reaction that began to take place as the two sides to this process of social construction exchanged blows:

- 'WikiLeaks booted off Amazon servers' (*V3.com*, 1st December 2010)
- 'Amazon faces boycott for dropping WikiLeaks' (*New Media Age Online*, 1st December 2010)
- 'How the net hit back at attempts to shut website' (*The Guardian*, 8th December 2010)
- 'WikiLeaks fans crash credit card websites' (*The Sun*, 9th December 2010)
- 'More attacks in WikiLeaks cyber war' (*South Wales Argus*, 10th December 2010)
- 'Hackers in web wars to protect leaks site' (*The Express*, 9th December 2010)

Reports such as these indicate the broader ramifications of WikiLeaks. Beyond the conflict between WikiLeaks and governments around the world, a range of other entities and actors were directly or indirectly involved in the process of claims-making, through supporting, or not, the actions of WikiLeaks. This enriches our understanding of what 'resistive surveillance' entails in the context of new media. Although WikiLeaks developed their own technological strategies and resources, they were also reliant upon others, for instance to host servers, or process donations. This is a consequence of networked forms of organisation and thus is a vital dynamic to add to the analysis as these other actors can facilitate or debilitate attempts at resistance. Furthermore, as some of the reports cited indicate, one element of the social reaction following the media inventories at the time was to generate more support for WikiLeaks. This adds little support to the idea of there being a panic about WikiLeaks and its detrimental implications for security and control.

Following this the pattern of reporting changed. No period generated the same volume of reports as those in December 2010. A series of *Guardian* articles in early 2011 entitled 'After WikiLeaks…' signalled the perception that WikiLeaks had already had its day. Arguably the most significant event in the WikiLeaks timeline was Assange's arrest (also in December 2010) over allegations of sexual assault. The lengthy process of bail, house arrest, hearings and appeals that followed consumed the majority of news reports concerning WikiLeaks and Assange throughout 2011

and into 2012. The spikes in 2012 correlate with Assange's final appeal hearing and subsequent refuge in the Ecuadorian Embassy.

To return to the start of this discussion, the question of why *The Spy Files* did not generate the impact previously seen can therefore be explained primarily by their position in the broader, turbulent history of WikiLeaks and Assange. Two other factors are worth briefly considering. First, these documents were not leaked. They were the product of an investigative journalistic effort by WikiLeaks and its collaborators (including Privacy International). Consequently, the novel character of leaked information was missing. Second is the issue of translatability of the material. This fundamental issue is one that concerns all forms of resistance against surveillance: how to make people care when there are myriad other social problems competing for their attention? When this question arose with Daniel, he suggested that the lack of reaction in the UK to releases like *The Spy Files* is a product of the extent to which surveillance is accepted:

> 'I think you [the UK] are much further down the lane than everybody else, you see you just look around for all these cameras you know, that would be completely impossible over here you'd have people rioting in the streets if that would happen…That just shows to what extent people have kind of accepted that, you know, they're, I don't know, I think the UK is the leading example of that in the world so your threshold for outrage is much higher that you have to reach in order actually for people to care. You've already accepted it.'

This synopsis of the key elements of the reporting of WikiLeaks bears out *some* of the characteristics of moral panic. Goode and Ben-Yehuda (1994) suggest a moral panic is typified by concern, hostility, consensus, disproportionality and volatility. Assessing WikiLeaks against these criteria involves a little subjectivity[197]. However, we can see clear evidence of concern, hostility and volatility (the latter in the rapidly fluctuating volume of reports). Consensus was not achieved; the news media appeared split along traditional ideological lines. Disproportionality, a key element of moral panic, is also trickier to claim given the unique nature of WikiLeaks and the information they brought to the public domain. On balance, the existence of a panic regarding WikiLeaks may be an overstatement, a key reason being that the events did not seem to be perceived as indicative of wider moral decline. However, we should not discount the broader implications for constructing social problems, in

[197] Indeed, a critique of the concept of moral panic is that defining which issues are 'moral' is subjective and arbitrary (Critcher 2016).

particular, the insights into how resistive surveillance and counter-resistance can be understood as claims-making activities that assert particular values.

WikiLeaks alerted the public to a new state of affairs wherein the activities of governments and private companies could be made visible. We might suggest this shifted the contours of morality in such a way that the rhetoric of secrecy in the name of providing security was challenged. Spector and Kitsuse (1987) note that claims-making has an implicitly moral dimension. Claims are normative in that they assert 'conditions *ought not* to exist; something *ought* to be done to improve conditions' (1987: 86, *emphasis* in original). In this case, governments ought not to have privacy from citizens and confidential information in the public interest ought to be revealed; surveillance practices ought to respect the right to privacy and there ought to be greater regulation of this industry. On the other hand, activists ought not to endanger security by publishing confidential information and these acts ought to be criminalised and punished by the law.

So far, the analysis has been based on the relatively short time frame that WikiLeaks were in the public eye. A final suggestion is that it may be of greater help for understanding digital surveillance and resistance to place these events in a broader historical context. This would recognise contemporary resistive surveillance as a product of the development of the information society alongside the evolution of moral concerns about (perceived) subversive use of technology. It would also allow us to explain the greater significance for debates about digital surveillance in the context of Snowden.

This history would date back to the early days of the Internet and incorporate the hacker culture of the 1980s and the steady growth of cryptography as alluded to above (Greenberg 2012). It would also accommodate significant moments of public anxiety regarding digital issues: the Stop Online Piracy Act, PROTECT Intellectual Property Act, Anti-Counterfeiting Trade Agreement, turn-of-the-millennium P2P services such as Napster and WinMX, the Regulation of Investigatory Powers Act, the Communications Data Bill; the list is a long one. Cohen's (1972) modelling would be difficult to adapt to this perspective. It would be hard to connect these disparate 'moments' into a single story of warning, impact, inventory and reaction, and again the question of which side of the conflict a panic may exist about is unclear. There is

concern about subversive use of technology in society *and* about political and economic control through surveillance and regulation of surveillance. Where moral panic is not applicable, then, the process of social construction of digital surveillance and resistive surveillance can still provide useful insights.

7.3.2 SNOWDEN AND SURVEILLANCE

We have seen that for several reasons there was little evidence of a connection between WikiLeaks and reporting on surveillance, even where leaked material pertained to the surveillance industry. In 2010, only 14 articles mentioned WikiLeaks, surveillance and privacy together and of these, only a handful did so relevantly. The most relevant article was by Heather Brooke, who later authored *The Revolution Will be Digitised*, an exploration of, among other things, the phenomenon of WikiLeaks. In her article she notes that 'The powerful have long spied on citizens (surveillance) as a means of control, now citizens are turning their collected eyes back upon the powerful (sousveillance)' (Brooke 2010). From Figure 9 we also see that there was little variation in volume of reporting on surveillance and privacy from 2010 to mid-2013. The one spike in April 2012, the analysis revealed, coincides with the announcement of the Draft Communications Data Bill. As briefly mentioned in Chapter Six, the media dubbed the CDB 'the Snooper's Charter', conveying a sense of the nature of reporting on the Bill. Capturing the negative aspects of the Bill with such symbolism may also have helped overcome the issue of translatability. This instance notwithstanding, for a more sustained media inventory on surveillance we need to examine the impact of Snowden.

In June 2013, *The Guardian* published the first in a prolonged series detailing the surveillance practices of the NSA and GCHQ. Perhaps the most significant of Snowden's early revelations was the existence of two intercept programs – PRISM and Tempora[198]. PRISM targeted foreign nationals outside of the US allowing content and communications data to be collected 'direct from the servers' of nine US service providers[199] (see Gellman and Poitras 2013). Tempora, meanwhile, tapped submarine fibre-optic cables making landfall in the UK and stored large

[198] Operated by the NSA and GCHQ respectively.
[199] Microsoft, Yahoo!, Google, Apple, Facebook, AOL, Skype, YouTube and PalTalk.

quantities of content and communications data, including '600 million "telephone events" each day' (MacAskill *et al.* 2013). The details of the two programs share a common thread: the relationship – willing or not – between state intelligence agencies and corporate telecommunications service providers. Moreover, many of the data gathered and analysed under these two programs are shared between the NSA and GCHQ and – as later publications would reveal – with other intelligence agencies.

The impact of these leaks had clear consequences on the reporting of surveillance and privacy in the UK. The average monthly frequency of reports on surveillance and privacy in 2013 approximately tripled to 276 articles. As Figure 9 illustrates, this increase was not the distorted product of a one or two month impact; the frequency was consistently higher than previously seen. Reports mentioning the NSA or GCHQ followed a similar pattern. *The Guardian* unsurprisingly dominated headlines from June and thus the tone of reports was critical of the political and economic entities involved, and aimed to stimulate debate about privacy and proportionality:

- 'Our privacy is not a luxury: Don't fall for the narrative if you've nothing to hide, you needn't worry. Democracy is at risk' (7th June)
- 'Did we really all check 'agree' to this government snooping?' (12th June)
- 'How can this level of state surveillance be legal?' (19th June)

Other news outlets followed similar lines of thought:

- 'Facebook and Google deny knowledge of top secret government spying initiative PRISM' (*Mail Online*, 8th June)
- 'Spies strip us all bare' (*Daily Mail*, 30th June)
- 'A case of the thief crying, Stop! Thief!' (*China Daily European Edition*, 19th June)

The last of these most clearly speaks to a moral dilemma regarding the ethics of data collection. The language of theft relates to ownership, which naturally begs the question of who the rightful owners of digital data are? In contrast to the largely critical reports at the time, some (conservative) newspapers opposed the 'presumption of guilt' placed on the intelligence agencies:

- ‘We’ve made it so easy for the data snoopers; the PRISM furore is not just about civil liberties. Think how willingly we trade personal information for convenience’ (*The Times*, 10th June)
- ‘Snooping Big Bruv helps keep us safe’ (*The Sun*, 16th June)

The Sun article expanded this argument, while at the same time implying the justification for digital surveillance:

> ‘We're crazy about telling everyone what we're up to, so why the mass indignation about the fact there might be someone listening? If you're not doing anything wrong, why worry? Unless you're discussing the latest bomb-making techniques…searching for illegal images on Google, does it matter who sees your search history (embarrassing as it might be)? Not really. Not if it keeps you a little bit safer from prospective paedophiles, terrorists or murderers. As Obama said, "we can't have 100 per cent security and 100 per cent privacy". He's right.’

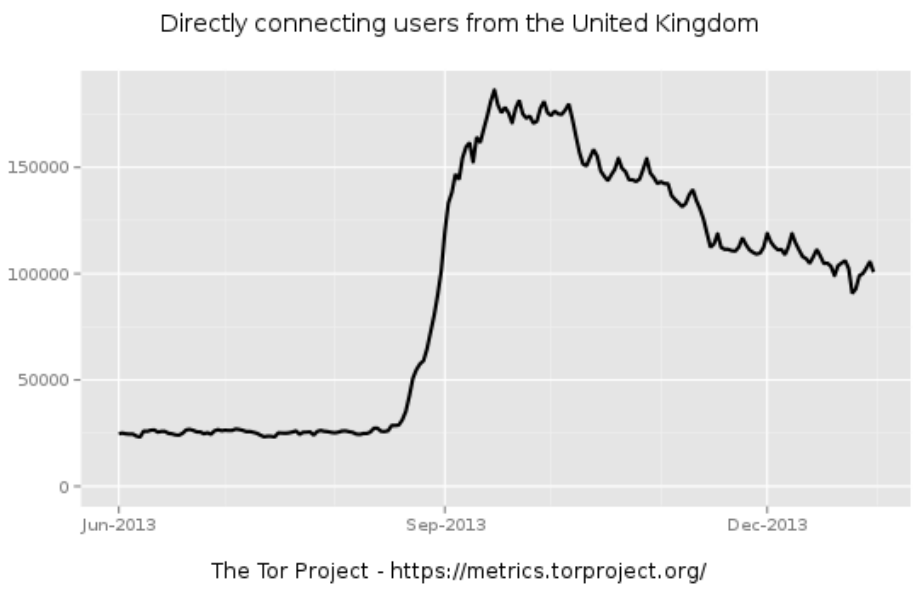
Aside from reporting details of political and economic surveillance, other agendas were pursued in the news media. One was raising awareness of the means by which the public could protect themselves. These individualised mechanisms of resistance that previously experienced little uptake in the public domain were vitalised in the news media. One *Independent* article introduced:

- ‘The Tor system: Welcome to the dark Internet where you can search in secret’ (9th June 2013)

Figure 12[200] supports the claim that such reports helped raise awareness of these techniques of resistance; the number of users of Tor in the UK rose dramatically in August and September 2013 from around 25,000 to 175,000.

[200] Statistics drawn from Tor Metrics: https://metrics.torproject.org/users.html?graph=userstats-relay-country&start=2013-06-01&end=2013-12-31&country=gb&events=off#userstats-relay-country

FIGURE 12: TOR USERS IN THE UK POST-SNOWDEN



However, there were also indications of the counter-resistance strategies employed by the intelligence agencies:

- 'NSA and GCHQ target Tor network that protects anonymity of web users' (*The Guardian*, 4th October 2013)

As well as drawing the public's attention to these efforts, the practices illuminated in this article evidence digital counter-resistance. Such attempts to nullify the benefits of Tor impacts not only on those engaged in illicit activity on the 'Dark Web' but also privacy advocates, journalists and members of the public who use the technology out of a desire to preserve the *value* of privacy.

The most important narrative, however, alongside the leaked material itself was that concerned with Snowden. There were two key aspects to this for the purposes of this discussion: the involvement of WikiLeaks and debate of the legality and value of his actions. Regarding the former, Assange voiced support for Snowden:

- 'Support NSA whistleblower Edward Snowden, says Julian Assange' (*The Guardian*, 22nd June)
- 'Whistleblower Edward Snowden 'has left Hong Kong for Russia' with help from WikiLeaks one day after US charges him with spying' (*Mail Online*, 23rd June)

While WikiLeaks undoubtedly supported Snowden, some critics equated WikiLeaks' efforts with an attempt to regain the spotlight (see Leetaru 2013). While for some this will have elevated his credibility – WikiLeaks have not emerged from their time in the spotlight completely discredited – for competing claims-makers this would have provided an opportunity to equate Snowden with the wider problem of undermining national security.

The attention directed at Snowden himself was, therefore, predictable. Calls for his return to the US to stand trial were reported alongside praise for his actions. The phrases 'on the run', 'traitor' and 'America's most wanted man' are frequently seen in early reports, reinforcing the official statements of the US government that Snowden's actions were illegal and threatened national security. These were strongly counter-balanced by more positive accounts:

- 'Edward Snowden is a modern American hero; this was a precious public service' (*The Independent*, 11th June)
- 'Snowden deserves our thanks for revealing world of surveillance' (*Irish Examiner*, 18th June)
- 'Edward Snowden: History will be kind to him' (*The Guardian*, 26th June)

There was, therefore, some similarity to the ambivalent way WikiLeaks and Assange (in earlier reports) were presented. However, to date at least, Snowden appears to have avoided much of the negative attention that accompanied Assange. The fact that he appears to remain a credible source is doubtless a contributing factor to the continued dialogue surrounding political and economic digital surveillance[201].

The extent to which the UK public are accepting of surveillance, as Daniel claimed, was challenged in 2013. Where WikiLeaks' publications (and other 'surveillance events') failed to generate an increased public consciousness of surveillance and privacy through media exposure, the Snowden revelations succeeded. In one (obvious) respect this is to be expected; the Snowden revelations were primarily concerned with digital surveillance practices. Compared to WikiLeaks, whose publications focused only sporadically on the surveillance complex, Snowden was bound to generate a greater social reaction. Moreover, the timeline of reporting on

[201] For instance in the on-going discussions and campaign surrounding the Investigatory Powers Bill (2015).

Snowden indicates the value of a *sustained* process of claims-making about one subject. Whereas WikiLeaks published documents relating to a broad array of institutions and practices, Snowden's revelations all contributed to the same issue of digital surveillance. In this case, resistive surveillance is at its most effective. To persuade people that something 'ought to be done', the problem needs to be sustained, which means the claims need to be sustained. In turn this means the issues have to be able to be translated to the public effectively. This is a hurdle for much resistance to surveillance, particularly in the face of counter-claims in the news that we should not be concerned if we have nothing to hide (as above). The symbolic nature of resistive surveillance is thus an important consideration.

7.4 SURVEILLANCE AND RESISTANCE PART THREE: THE SOCIAL PROBLEM OF DIGITAL SURVEILLANCE AND RESISTANCE

7.4.1 THE SYMBOLIC POLITICS OF SURVEILLANCE: CONDENSATION SYMBOLS AND CRISES

This chapter began with a question about the extent to which WikiLeaks and the more recent Snowden revelations can inform our understanding of digital surveillance and resistance. The analysis has aimed to provide a foundation to move beyond a simplistic response based on 'what we now know about digital surveillance practices' thanks to the efforts of WikiLeaks and Snowden. The recent history of the contest over control of information and digital surveillance in the news media is marked by events (impacts) and their aftermath (inventories). The reaction phase of interest to Cohen has been addressed so far in respect of the creation of a public consciousness about surveillance and privacy, which was evidenced most prominently in the wake of the Snowden revelations. Another element of this reaction is the effect of WikiLeaks and Snowden on the symbolic nature of the politics of surveillance. Rather than isolated instances, then, the reaction phase can be considered as an on-going and cumulative process, supplemented by each new encounter between digital surveillance, resistance and counter-resistance.

Surveillance is never neutral. It implies a power dynamic: the power to 'watch over' someone or something. Resistive surveillance re-appropriates this power, using

technological mechanisms and distribution of information through media channels to subject political and economic entities to surveillance. Surveillance is, therefore, also increasingly political. As surveillance becomes increasingly contested, so do the ways in which the 'problem' is constructed. An important aspect to this is symbolism.

Edelman (1964) notes how 'condensation symbols…evoke the emotions associated with the situation. They condense into one symbolic event, sign, or act, patriotic pride, anxieties, remembrances of past glories or humiliations, promises of future greatness: some of these or all of them' (1964: 6). Graber, meanwhile, defines such a symbol as 'a name, word, phrase, or maxim which stirs vivid impressions involving the listener's most basic values' (1976: 289). A condensation symbol is useful, therefore, for achieving political ends; it can engender support by offering reassurance or by constructing a threat to be protected against. If we are so inclined we can see symbols everywhere. 'Practically every political act that is controversial or regarded as really important is bound to serve in part as a condensation symbol', Edelman suggests (1964: 7). Thus 'surveillance' is a condensation symbol – but we can look in finer detail at the issue of digital surveillance and resistance to gain a better understanding of the relevance of this.

Symbols appear frequently in the news. Indeed, Edelman argues that the public 'wants symbols and not news' (1964: 8). He also notes we can attach emotion and become involved in a reported political act more readily when it is remote to our everyday experience – particularly when it is presented as some form of crisis or controversy. The findings of this thesis provide support for this idea. The insights into diplomatic communications, military practices and the activities of the intelligence services certainly fulfilled the 'remoteness' aspect of condensation symbols Edelman highlights; their presentation in the news media, the 'crisis' aspect. From 2010-2013, WikiLeaks, Assange and Snowden all acted as condensation symbols in both Edelman (1964) and Graber's (1976) terms. They became symbolic of the power of an individual to overturn political and economic control over information, and of the ability of the Internet to put a degree of control back into the hands of citizens. They have also become symbols of governments' desires to punish those who challenge their legitimacy or 'right' to secrecy. Resistive

surveillance has helped to reshape the political landscape of digital surveillance by making visible what was previously invisible.

WikiLeaks and Snowden helped condense a set of attitudes, experiences and fears into a highly visible contest between activists, states and corporations. Symbols of this conflict abound, for instance 'civil liberties', 'privacy', 'security', 'freedom' and, naturally, 'surveillance' or 'surveillance society'. WikiLeaks and Snowden fed into this existing and growing concern with personal digitised data. However, all these symbols exhibit duality; they themselves are contested as each participant to the conflict attempts to construct them in order to achieve and justify their own political ends. In the case of 'surveillance', government rhetoric frames the term as vital for safeguarding civil liberties and freedom. As a condensation symbol, it is designed to reassure. Advocacy groups, on the other hand, talk about surveillance as invasive and eroding civil liberties. WikiLeaks, Assange and Snowden underwent a similar process of social construction. Snowden's single sustained narrative, despite its illegal foundations, and his adherence to his values arguably helped cement his position as a folk hero. In contrast, the personification (as a mode of symbolisation) of what WikiLeaks stood for in the personage of Assange undermined the aims and reputation of the organisation. In this respect, symbolisation needs to be treated carefully. As Shirky (2011) observed 'The press has covered him as dutifully as any movie star, while paying too little attention to what his invention means about the wider world.'

Condensation symbols, therefore, illustrate the importance of significant 'moments' in the trajectory of the digital surveillance/resistance relationship. Key events and crises can be appropriated and re-appropriated. They can convey a sense of the problem to be resolved and to engender support or attachment. Surveillance is thus a contested symbol, employed as both a rhetorical and practical tool for reassurance and – particularly over the last few years – as a symbolic device, illustrating the threat posed to the private lives of citizens. In tandem with resistive surveillance, which brings with an element of the 'underdog', these have shifted the landscape of digital surveillance.

7.4.2 MORAL PANICS AS CULTURAL POLITICS

To talk of a 'moral panic about surveillance' is arguably a misnomer if taken in its original sense. Panics have typically been understood as directed at marginalised sections of the population, and generated by a conservative, traditionalist elite. Surveillance does not fit that bill; it is enacted by those *in power*. To label concern about it as a panic would invert the concept. However, Cohen's (2002) later comments do address 'good' and 'bad' moral panics and their respective use by different ends of the political ideological spectrum. The evidence in this chapter shows claims were made for both of these ends.

Panics are also characterised by disproportionate reaction and, while it is a subjective judgement to make, surveillance *is* potentially detrimental to social groups so any public anxiety about surveillance is, arguably, justified. The converse – a panic about whistleblowing and the damage it could do – is more typical of a panic generated by conservative forces. However, technologically-augmented strategies of resistance have proven too mobile, too resilient, to be targeted and subjected to a sustained attack. In conflicts such as those seen in this chapter, both sides defend their actions by 'implicatory denial' (Cohen 2002: xli): 'what happened was not really bad and can be justified.' Particularly post-Snowden, the on-going public debate about digital surveillance suggests that such denial has been less effective on the part of the elite (political and economic entities).

The analysis has been couched in a broader language of social problems, rather than attempting to declare with certainty if a panic exists, and about what. However, conceptually, the question of morality is still important in the context of contemporary surveillance. One reason for this is the connection between panic and risk. Moral panics are associated with periods of rapid social change. The pace of change of information and communication technologies, as Chapter Two described, has been rapid indeed. It is for this reason that reforms to legislation of the kind in Chapter Six are proposed, because ICTs develop faster than law can keep pace. This is equally true of digital surveillance and the appropriate degree of protection for privacy the law can offer. The pace of change is therefore associated with risk and the need to implement controls that minimise such risks. This raises

difficult questions: what level of risk and what sorts of risks are we prepared to tolerate? How much surveillance will we accept for the benefit of our security? Does whistleblowing pose a greater threat than mass surveillance? Privacy and security are abstract concepts. They cannot be measured objectively and thus the question is one of political morality. A related issue, however, is whether because something *can* be done, it *should* be done. Just because information can be distributed without restriction, does that mean it should? That is a moral dilemma, not only restricted to the realm of political morality. Bear in mind as well the point from Chapter Two – the characteristics of the information society cannot be distilled only to technology. There are social and cultural forces at work as well and we can see the intersection of all of these in the case of WikiLeaks and Snowden.

Recall Cohen's earlier point about conceptualising lines of power. Here is the value in Cohen's model for understanding the effect of WikiLeaks. To theorise moral panics, Cohen (1972: 198) says we need to acknowledge that power differentials at a societal level mean some groups are vulnerable to attacks (that is, constituted as deviant or worthy of panic). WikiLeaks redrew these lines of power and helped recast the boundaries of what can fall within moral concerns. Indeed, this is what resistive surveillance more broadly achieves. Altheide (2009) for instance suggests that terrorism is 'off-limits' as a panic in the news media. It is an issue that cannot be subjected to point and counter-point. Likewise, until WikiLeaks, the various mechanisms of the state and, after Snowden, of political and economic surveillance, were uncontested as 'problems' for two reasons: because they were there to protect security and, more simply, because the information was not there to inform any debate. That the actions of governments are now more visible is a result of a shift in the lines of power in society brought about by (digital) resistive surveillance.

> 'The manipulation of appropriate symbols – the process which sustains moral campaigns, panics and crusades – is made much easier when the object of attack is both *highly visible* and *structurally weak*' (Cohen 1972: 198, *emphasis* added).

Perhaps there are panics still to come, either about the extent of political and economic surveillance or about the inability of the Internet to be controlled for the purposes of safety and security. Meanwhile, the 'cultural politics' as Cohen (2002) described it of the information society – panic, risk, social problems, and more

specifically of digital surveillance and resistance – will continue to play out online and offline.

7.4.3 CONCLUSION

This chapter completes the exploration of different sites of nodal governance. Broadly speaking, it has been concerned with 'the media', both the news media and 'new media' platforms like WikiLeaks. The importance of the news media was signalled in Chapter Five and this chapter has shown why this is. Digital surveillance and resistance involve the public above all else. Therefore, how these issues are communicated and constructed in the public domain is vital for understanding the broader nature of control in the information society. Cohen (2002) tells us that people's perceptions are difficult to shift. Posing the question of why digital surveillance may or may not be taken 'seriously' is therefore of central importance. The chapter has also reiterated the *socio-technical* nature of resistance/resistive surveillance and returned to the idea of 'visibility' introduced in Chapter Three.

The broader message to take from this chapter is not actually about the content of leaked material concerning surveillance practices. The message is about the potential of resistive surveillance. WikiLeaks, we have seen, did arguably little to foster a dialogue about digital surveillance and several reasons have been proposed as to why that is. Snowden has achieved much more in that respect. The impact is still being felt today. The Investigatory Powers Bill working its way through the Houses of Parliament has been influenced greatly by the increased awareness that now exists regarding the extent of surveillance capabilities of intelligence agencies and the lack of regulation of their activities that exists. Regardless of this, we should not discard the activities of WikiLeaks as they set the tone for the way in which political and economic entities can be subject to surveillance by citizens as a result of the dissemination of information across online and traditional news media channels.

WikiLeaks perhaps exemplifies more clearly the technological potential of the Internet that underpins this. They were empowered by sophisticated encryption and manipulation of global information flows through various jurisdictions. These allowed an older form of resistance – whistleblowing – to find new currency via a

novel media platform. The same technology allows individual Internet users (and organisations) to protect their anonymity and security online. That WikiLeaks have resisted all attempts to remove their online presence adds to this. Whilst Snowden was a much more 'traditional' whistleblower in that sense, he still made use of encrypted communication technology to communicate his intent at the outset and the documents that were later revealed. Both cases, then, illustrate and support the argument of this chapter; that resistance to digital surveillance (in this case resistive surveillance) is resilient and socio-technical. It also signifies – and as Doyle (2011) suggested, complicates – the relationship between media and surveillance. The recent history this chapter has covered challenges Mathiesen's (1997) original view of the synopticon as one that reinforces panoptic surveillance. Our concept of media in this context needs to be much broader. To be certain, there are patterns of reaction in the news media that aim to counteract resistive surveillance, as we have seen in the attempts to make folk devils out of WikiLeaks, Assange and Snowden, but these are opposed, if not outweighed, by the potential that exists for media platforms to challenge digital surveillance.

Drawing on Cohen's (1972) model of moral panic has allowed for a systematic appraisal of the construction of surveillance issues on an individual, organisational and symbolic level. Charting the reaction alerts us to the construction of the subversive potential of the Internet, digital surveillance and resistance to this as simultaneously positive and negative. The news media is the place in which these contests are played out. Moments such as those explored in this chapter allow us a glimpse of what Becker has called a 'moral enterprise…the creation of a new fragment of the moral constitution of society' (1963: 145) or Gusfield (1963) refers to as a 'symbolic crusade'. Despite continued obstructions and counter-resistance along the way, three years on from Edward Snowden this crusade continues.

-.-- --- ..- .- .-. . -. --- - .-- . .-.. -.-. --- -- . .- -- --- -. --. ..- ... .-.-.-

CHAPTER EIGHT

EMERGING THEMES FROM THE SITES OF SURVEILLANCE AND RESISTANCE

8.1 INTRODUCTION

New technologies and the uses to which they are put always bring with them uncertainty and risk, but also potential (Beck 1992). This thesis has presented a picture of the communicative, interactional environment of the Internet as a constantly evolving technology that has given rise to an active, vociferous and complex set of inter-relationships between varieties of actors. The history of the Internet is one of both competition and cooperation (Fuchs 2008), as the uncertainties, risks and possibilities it has persistently introduced have been argued for and against, co-opted and capitalised upon. This trend has continued in recent times; specifically, the virtual environment is increasingly manipulated to maximise the visibility of Internet users. The dynamics of digital surveillance and resistance, explored in three key sites, have provided the context in which the contemporary form of social control is produced. Commonalities and patterns have begun to emerge and it is the purpose of this chapter to draw these out.

The narrative guiding the analysis up to this point has two chief characteristics. Firstly, it has been framed by a theory of nodal governance that has helped to draw different entities with a stake in the relationship between digital surveillance and resistance into the analysis at different stages. Secondly it has progressively become more focused. IIt began in Chapter Five with an exploration of a online community of resistance and the patterns of organisation within this. It then examined, in Chapter Six, a specific instance of resistance where this community and other nodes negotiated the regulation of digital surveillance. Finally, in Chapter Seven, it scrutinised one organisation and one individual that have been at the heart of much recent debate around surveillance and the potential afforded by the Internet to invert surveillance relationships. Organising the analysis in this way has helped to

draw out different features of the relationship between digital surveillance and resistance. While these are distinct from one another – to a degree – they combine to produce an overarching picture of some of the contemporary characteristics of social control. Consequently, this chapter develops three main themes: nodal governance, regulation and visibility. These each fit broadly with the concepts deployed in Chapters Five, Six and Seven but they do not simply restate the issues. There are additional insights that allow us to consider the various and related features of control in the information society. The groundwork is laid for the discussion in Chapter Nine of the specificities of what is termed *socio-technical* control.

8.2 NODAL GOVERNANCE: COMPETITION AND COOPERATION

The thesis began with the contention that networked communication technologies such as the Internet – and the broader networked organisation of global society (Castells 2007, 2008, 2009) – force us to reconsider the operation of social control. Specifically, surveillance and resistance need re-investigating and reconceptualising in a digital society that has changed significantly the way in which they operate. Top-down, one-directional, state-centric conceptions of surveillance based on the historical analysis of the 'panopticon' (Foucault 1977) are untenable in contemporary society. So too are modernist concepts of resistance that pit a powerless subject against a powerful agent of control. The relationship between the two is instead much more fluid and intricate, which mirrors the networked character of the information society. With this in mind the theory of nodal governance was employed to reflected this approach to understanding surveillance, resistance and control and to structure the thesis accordingly. Namely, cases were selected that highlighted the broad range of social actors and entities where surveillance and resistance takes place and, thus, where control is negotiated and shaped.

In criminological discourse nodal governance has been used to describe the ways in which a diverse set of actors interact as providers of security (Wood and Shearing 2007: 34). Security in this context includes digital surveillance, and maps on to Haggerty and Ericson's (2000) concept of the 'surveillant assemblage': a society-wide horizontal network of public and private entities that within and between them

function to create the surveillance apparatus of society. The aim of Chapter Five was to demonstrate how these complementary ideas could be expanded to take account of resistance as well as surveillance. Nodal governance refers not only to those practices that seek to enact surveillance or other forms of security and control but to all manner of positive action that aims to guide a social system. Thus, in the same way as governance of security amongst public and private entities has been described (see Johnston and Shearing 2003; Shearing and Wood 2003; Burris *et al.* 2005; Wood and Shearing 2007), resistance is networked and fluid. Online, within the advocacy community united by broadly-framed libertarian goals, there is jostling for position at the same time as there is cooperation in the form of coalitions, or 'superstructural' nodes. To add to this, resistance is also undertaken by some of those entities that seek to provide security (political surveillance) or carry out other economic surveillance (illustrated in Chapter Six).

The analysis of the data in Chapter Five using the theory of nodal governance contributed to the narrative of the thesis, therefore, by illuminating the social organisation of resistance. Drawing on insights from previous research on nodal governance and networked communities, several characteristics of the online network of 'privacy advocates' were highlighted. These included: mentalities, resources, technologies and institutions (Burris *et al.* 2005); stability and density (Introna and Gibbons 2009) and responsiveness to the real time events. Chapter Five demonstrated these digital workings of nodal governance empirically through visualisation of online networks of resistance.

At its core, then, nodal governance implies a constant shifting of relationships between various entities, characterised by both competition and cooperation between networks of actors (Fuchs 2008). These can define the relationship between any two actors. Wood and Shearing (2007) also refer to these ideas in their discussion of nodal governance. Nodes are not necessarily joined to one another in permanent, stable networks, even when they are pursuing the same goals. For instance, the networks revealed in Chapter Five, while containing a breadth of advocacy groups with similar mentalities, were flexible and changed over time. Relationships change depending on circumstance. Martin *et al.* (2009) identified these themes in similar circumstances. They suggest that a 'multi-actor

framework' is necessary to understand the relationships and processes that occur in response to specific surveillance developments. Importantly, these frameworks are context-dependent. Thus, for Martin *et al.* (2009) the set of competitive and cooperative interactions that emerged in response to the Identity Cards Act 2006 was unique, just as were the interactions that were seen in this research in response to the Communications Data Bill. The information society has allowed for these patterns of organisation to flourish (Castells 2000 in Burris *et al.* 2005: 37). This is an important point, as it restates why it is crucial to focus research efforts in this area on the information society and why networks in particular are of analytical interest.

Civil society, in its broad sense, is a node for governance as are the state and private sector. These nodes, however, also encapsulate a large number of other nodes. Nodal governance thus operates at different organisational levels. The relationships between the constituent nodes of the 'privacy advocate' sub-sector of civil society were visualised in Chapter Five. There was evidence that some of these nodes were more connected in the hyperlink environment of the Web than others – and were thus possibly more 'important' for the network – which further develops the sense of constant competition and cooperation in governance processes. A new insight theorised from the data was the existence of 'bridging nodes'. This important role was made visible through the visualisation of hyperlink networks and deepens our understanding of the operation of nodal governance.

With respect to cooperation, aside from the connectivity via hyperlinks, there was further evidence of this in the existence of groups such as the European Digital Rights Initiative (EDRi) and Don't Spy On Us. Such groups could be considered 'superstructural nodes' (Burris *et al.* 2005) insofar as they demonstrate a willingness to coordinate resources and technologies within the community to increase the impact the various groups can have in resisting surveillance. Similarly, the privacy advocate community could also be considered a superstructural node but in perhaps a looser organisational sense as issues of geography and mission of groups becomes more dispersed and diverse. Just as the relationship between digital surveillance and resistance is dynamic, so too is resistance a fluid process. There are elements of the online social organisation of resistance that are stable over time, but there are also shifts in the contours of this community and different organisational levels

where resistance happens. These online patterns were evidenced and expanded upon in Chapter Six, where a broader array of governing nodes were seen interacting; some advocating greater surveillance (the government), some resisting this (civil society and individual citizens) and others fulfilling both functions (CSPs and some experts).

Wood and Shearing (2007: 34) also suggest that the nodal governance perspective does not presume a decline in state authority or power (resulting from the diffusion of governing roles to various other locales). On the contrary, they argue, it represents a pervasive expansion of such power as diverse entities begin to function as auspices of security (Shearing and Stenning 1981, 1983, 1985; Cohen 1985, Garland 2001). This research supports this claim, to an extent. The government is prominent in the networks and interactions that have been explored, and through practices of surveillance and regulation they have sought to consolidate that position. However, their authority has been challenged on a number of fronts. Rather than a decline in state power, then, what we are witnessing is a concurrent escalation of the *resisting power* (Sharp *et al.* 2000) of other nodes. These patterns are the result of the empowering capacity of Internet communication and organisation.

Wood and Shearing acknowledge this process when they say that other actors 'may work with states but they can also coordinate nodes to resist and contest state governance' (2003: 28). This is a theme that was apparent within and between the three research sites and can be thought of as a competitive process of accumulating, deploying and mobilising various forms of 'capital' (Bourdieu 1986, in Dupont 2003, 2006) – economic, social, cultural, political, and technological. Private sector online service providers are particularly important in this respect. While their motivations are primarily profit-driven (economic surveillance), government and law enforcement increasingly define them as important providers of security – what Wood and Shearing (2007: 29) call a blurring of 'governing mentalities'. These findings are similar to those of Dupont (2003, 2006) who claims that public policing bodies mobilise capital in order to maintain a degree of hegemony in the provision of security. They are similar in that the government, by mandating CSPs to retain more data, sought to rectify a 'capability gap' in the ability of law enforcement to

provide security for citizens. The way in which government attempts to mobilise this capital in the corporate domain is through regulation like the Communications Data Bill[202] (CDB). They differ, however, insofar as, by outsourcing or 'mediating' (Bright and Agustina 2013) control functions such as surveillance to the private sector, they acknowledge their shortfalls. The public sector cannot reclaim this means of providing security – it *must* be carried out by other nodes. In the other research sites, too, competition for capital occurred in different forms. Social capital is important for the advocacy community (and indeed is a cornerstone of social movement theory that was touched upon in Chapter Five). Cultural capital could be identified in similar terms and also in the efforts of WikiLeaks, Edward Snowden and the news media to create a symbolic sense both of the Internet as an empowering tool, and surveillance of this space as fundamentally repressive. Technological capital is a new addition to the list outlined by Dupont (2003) but is vital to understanding *online* governance; WikiLeaks is a good example of how technological capital can be mobilised in the pursuit of specific goals. Likewise, returning to CSPs, the reason that government identifies these nodes as valuable is for their technological capital – their ownership of the means to capture citizens' transactional data.

In respect of the theoretical positions outlined in Chapter Three, nodal governance here does not replace or supersede social control. We need to be aware of both; control is a product of relationships and motivations within a broader *socio-technical* system of governance. While the argument presented in Chapter Three, that there has been a shift in patterns of control – namely towards co-opting and responsibilising private auspices of security (i.e. towards a governing mentality) – is accurate, social control is not a defunct concept. Rather, the socio-technical system of governance that has been described here is particularly productive of a new character of social control. The Internet has amplified the potential for control but also the potential for resistance. In Chapter Three, nodal governance was described as a 'post-social' outlook on control (Johnston and Shearing 2003; Shearing and Wood 2003; Wood and Shearing 2007). That is, the 'social', as both a target and location for control, has been replaced by various locales and sites of governance

[202] And, more recently, the Investigatory Powers Bill (2015).

(nodes). This research challenges that perspective. The degree of interaction between nodes (changeable though it is) does suggest that the social is still a valuable theoretical construct. Taken together, the sites identified in this thesis, for instance, encapsulate much of what could be fairly described as 'the social'. They do exist as distinct locales with differing motivations, priorities and targets for governing. Yet they are connected to, and influence, one another (through competition or cooperation) to the extent that governance, and subsequently control, occurs at a societal level. These trends are facilitated by the networked, communicative technology of the Internet. The Internet also creates new *spaces* for governance and control, within which these nodes compete and cooperate with one another. The concept of space and place is highly relevant for studying surveillance and control. Indeed, it connects to Foucault's (1977) initial elaboration of surveillance within certain institutions. However, although the data here have pointed towards these issues, this is a theoretical debate that would require diiferently focused research to fully explore[203]. While this might seem to suggest a deconstruction of the social once again – a division of society into distinct, virtual locales – the globally networked nature of these spaces instead re-emphasises the societal level of governance and control. It is for all these reasons that the contemporary character of governance and control can be described as 'socio-technical'. This concept is explored in greater detail in the concluding chapter in response to the third research question of the thesis.

The concept of nodal governance has enriched the theoretical arguments of the thesis. In equal measure, the thesis has added to contemporary debates about nodal governance by illustrating empirically the specificities of how it plays out in the information society. Traditionally, discussions of governance and social control have placed the state at the centre of these processes, particularly in terms of security and crime prevention. Both the nodal perspective on governance and the context of the information society problematise this perspective. The primacy of the state is challenged by the private sector that owns the channels of communication and has its own interest in the data that are generated within them. The socio-technical system of governance encapsulates all the interactions and relations that

[203] See Chapter Nine (section 9.4.1).

construct the Internet as an economic domain as well as a social, cultural and spatial one. While governance, in these terms, is descriptive of the operation of power across society and illustrates the various rationalities for managing and influencing populations, social control, by comparison, occurs within this system and between the actors who constitute it.

8.3 REGULATION: CONTROLLING BEHAVIOUR AND SHAPING THE WEB

The focus in Chapter Six on regulation of surveillance both narrowed the focus of the research (by examining a particular context where surveillance and resistance intersected) and expanded upon some of the insights from Chapter Five (by illustrating the broader network of social entities involved in advocating surveillance and enacting resistance). The aim of Chapter Six was to demonstrate how legal frameworks have sought to regulate surveillance in the information society and how these have subsequently generated effects of resistance. Underpinning the analysis was the contention that regulation and surveillance intersect as modes of social control. The relevance of focusing on regulation alongside surveillance (to inform a discussion of social control) stems from two sources: theoretical and empirical research[204] that has examined the 'regulation of cyberspace' in various ways (from which this thesis takes a great deal of inspiration), and the precedent for incorporating this concept into studies of surveillance. In Chapter Three, for instance, it was shown that Foucault's (1977) elaboration of discipline was essentially concerned with *regulating* behaviour through constant surveillance. In Chapter Two, Lessig's (1999) 'architectures of identification' illustrated how regulating the digital environment can allow for specific forms of surveillance to exist. Less has been said in the literature about the specificities of regulation of the surveillance industry or techniques of surveillance, although the extensive body work around this subject (e.g. Ayres and Braithwaite 1992; Gunningham and Grabosky 1998) does indicate the value of considering how regulation functions alongside surveillance in the contemporary information society.

[204] See Chapter Two.

Regulation is 'concerned with technical modifications of procedure' (Innes 2014: 149) – how things should or can be done – rather than a concern with outcome. Rehearsing a theme for Chapter Nine, regulation in this context can be considered either as 'social' (i.e. legislation that compels certain behaviour) or 'technological' (i.e. the ability of technology to dictate the kinds of behaviour that are possible online). This is behaviour that, to use Cohen's (1985) approach, may be perceived as deviant or problematic, but it may also be behaviour of online consumers, for instance, whose preferences are targeted on the basis of algorithmic surveillance techniques. Online, this is particularly applicable. Galloway (2004) describes 'protocol' as a technological system of control that defines the limits of possibility for online action; nothing can be done outside of the limits of the protocological system. Even resistance has to operate within the boundaries of action that protocol makes possible. Given that all interaction and organisation on the Internet can only occur because it is made possible by technological processes, regulation is a pertinent form of control that requires attention in the context of a study of digital surveillance, resistance and social control.

These aspects of how regulation intersects with surveillance began to emerge from the data in Chapter Six (in the context of regulating those who carry out surveillance) and also in Chapter Seven (where the regulation of cyberspace or 'code' was what allowed for WikiLeaks' unique brand of resistance). Regulating the way in which the digital environment can be accessed for the purposes of security is an enormously challenging process, as the CDB was testament to and as subsequent legislation has also shown[205]. The CDB aimed to codify the tenuous relationship between the state and CSPs in the private sector. This 'mediation' (Bright and Agustina 2013) of surveillance is not a new phenomenon, but the characteristics of surveillance in the information society complicate the process. Specifically, regulation in this area must fit within a global surveillant assemblage (Haggerty and Ericson 2000) and not only within the boundaries of the nation state in which it is enacted. Resistance to these newly regulated forms of surveillance, as a consequence, is amplified as this opens it up to a much broader set of actors who simultaneously work to codify their interests in law.

[205] For example, the Investigatory Powers Bill (2015): https://www.gov.uk/government/collections/investigatory-powers-bill

The lessons learned in Chapter Six about regulation, therefore, were not confined to highlighting the position of private sector CSPs in the dynamic of surveillance and resistance. While an important finding in itself, researching the regulatory domain in the context of digital surveillance also illuminated the role of other categories of actors in shaping a debate about necessary and proportionate surveillance. These findings highlighted that the state no longer enjoys a monopoly on defining what is risky or problematic when it comes to crime and security and the necessary mechanisms to regulate these risks. Drawing on the theme of Chapter Five, a large number of nodes aligned against the state during the consultation on the CDB, in both formal and informal collaboration. Agamben's (2005) 'state of exception' – the paradoxical tendency to undermine civil liberties in an effort to protect them – was a useful tool for understanding this situation. Regulating the digital surveillance apparatus of the UK is not only a question of how to provide security for citizens, because in the information society the methods for doing this impact on the daily lives and interactions of people online at an increasingly granular level. As before, then, regulation of digital surveillance speaks to the character of the information society in that everyone has a stake in this debate, not only the regulator and regulated.

8.3.1 CENTRALISATION AND DECENTRALISATION

A sub-theme connected to the concept of regulation that has emerged at various junctures is that of centralisation and decentralisation. Chapter Two described how architecture of the Internet is decentralised/distributed and that it is this which allows it to operate as it does. This characteristic is at the basis of many libertarian claims that the Internet democratises communication and is a powerful tool for free speech. However, in contrast to this, there have been concerns voiced in the findings that there are increasing tendencies towards centralisation – of architecture and subsequently of information and services – that undermine and challenge the potential of Internet communication to be free from control. The possible alternative architectures of cyberspace are many (Lessig 1999). Some would allow for greater control (perhaps through commonplace surveillance) while others would allow for more freedom – to exchange ideas and property, or to interact free from surveillance perhaps. *Both* of these are the product of a regulated Internet – or

regulated 'code'. This point is important. Regulation of cyberspace is not inherently damaging but there are forms of regulation that could allow for greater surveillance, greater control and less freedom online. This is what Lessig (1999) terms 'architectures of identification'. By changing the nature of the Internet (centralising information and services for example) and thus the types of behaviour that can occur (regulation), it is made more susceptible to ubiquitous surveillance.

It is a limitation of this thesis that it has not found specific instances where the technological architecture of the Internet has been regulated in such a way as to make surveillance more commonplace. Some indication of this was observed in the work of the Government Digital Service (GDS) who were changing the way in which online public services functioned. GDS were working closely with private sector businesses that held identifiable data on individuals, which could be used as a proxy for verifying the identity of prospective applicants for services. To an extent, this is representative of a trend towards an Internet that is regulated on the basis of identifiability. However, the arguments in Chapter Seven demonstrate how the antithesis is possible. That is, virtual networks can be regulated so as to ensure identities *cannot* be ascertained; WikiLeaks ensured that those who submitted leaked material could not be identified. This, of course, is not 'formal' regulation (i.e. 'social') but it is regulation of code (i.e. 'technological).

If we look to the case in Chapter Six, we see something similar in the regulation *of* surveillance. The CDB was less concerned with affecting change in the virtual environment, in order to make it more susceptible to surveillance, than it was with regulating how digital surveillance should be carried out in practice. This is a fine distinction but an important one. The CDB, and other legislation preceding it, exemplify where the conduct of surveillance is regulated[206]. Those subject to control in these cases include a wide variety of public and private bodies that collect data from citizens in one form or another. What we see in these cases is regulation ensuring compliance from public and private bodies, which in turn legitimises other forms of control (surveillance) and attempts to allay any public fears that may exist over the use of such powers – fears that were seen in the data in Chapter Six. Both

[206] The CDB and the Regulation of Investigatory Powers Act being two examples where the goal is control of deviant behaviour (crime prevention).

'social' and 'technological' forms of regulation then, are instances where its implementation affects the nature, purpose and extent of surveillance.

The regulation of surveillance can also be approached in terms of centralisation and decentralisation. Take the example of the failed Intercept Modernisation Programme (IMP) in 2009[207]. In this case, the conduct of communications data surveillance revolved around the establishment of a centralised database accessible to government and law enforcement. For critics of the IMP, this proposal was an insurmountable barrier. Furthermore, it illustrates that centralisation of data (specifically, data that can be very revealing[208]) is a major concern particularly, it would seem, when it is the government that holds such a repository. By contrast, and likely as a response to this, the CDB proposed a decentralised/federated model for storing data. This approach, of course, had the added benefit that responsibility for collecting and storing data securely would rest with the private sector. Regardless, the CDB was rejected on grounds more related to the fundamental opposition to the necessity and proportionality of extensive digital surveillance.

In the legislative context, neither centralised nor decentralised processes, it would appear, are a panacea for implementing acceptable regulation of surveillance. By contrast, participants in this research *did* advocate decentralisation of Internet architecture and information. We need to couple these observations with the fact that decentralisation is a defining trait of the organisation and operation of contemporary surveillance. Foucault's (1991) work on governmentality laid the groundwork in shifting away from the dominant conceptualisation of a single point of power towards one of dispersed and diffuse networks of power. Likewise, Haggerty and Ericson's (2000) surveillant assemblage, and Cohen's (1985) earlier work, are cases in point – as indeed is the preceding discussion of nodal governance. Theories of social control, then, suggest that decentralising tendencies characterise contemporary society. Those networks exist and find new energy online. At the same time, in technological terms, this tendency appears to be reversing – towards centralisation of services, as a result of the strong economic motives behind the

[207] See Chapter Two (section 2.4.4).
[208] See Chapter Six (section 6.4.2).

regulation of cyberspace. That is a particular product of control in the information society.

8.4 VISIBILITY: DIGITAL SURVEILLANCE, SOUSVEILLANCE AND THE SYNOPTICON

The final sub-narrative guiding the findings of the thesis was that of moral panic and the social construction of surveillance and resistance. This is a vital part of understanding social control, as it is through such processes that the desire for, or alleged necessity of, more or less control is created. The thesis began by introducing the concept of visibility as it applies to modern digital technology. This was followed by a description of current surveillance issues and trends in contemporary surveillance practices. Correspondingly, Chapter Seven returned to some of these themes, and continued the trend of the previous chapters of focusing in greater detail on specific scenes and actors in the surveillance/resistance relationship. The analysis centred in closely on one actor in particular – WikiLeaks. It elaborated, first, the mechanisms by which WikiLeaks operated, thus demonstrating the potential of digital communication to foster highly effective resistance. Second, it drew out the cyclical process of resistance and counter-resistance that characterised WikiLeaks' and Snowden's interactions with surveillance agents (i.e. various governments). The theory of moral panic (and, more broadly, social problems) helped to guide the exploration of how both surveillance and resistance (in this case 'resistive surveillance') were constructed as potentially problematic. Throughout this discussion it also became clear that the division between surveillance and resistance is conceptually blurred. 'Resistive surveillance' – incorporating sousveillance (Mann *et al.* 2003) and the synopticon (Mathiesen 1997) – shed light on the nature of this relationship. These insights are drawn out here under the umbrella of 'visibility', introduced in Chapter Three. This idea is speaks to the simultaneous ways in which people are made visible online (by surveillance) as well as how surveillance agents are made visible (by resistive surveillance).

In many ways, the world around us is more visible in its literal sense; through video footage made available through the medium of television and the Web, we can see more places and people than we are ever likely to 'in the flesh'. Visibility in the

context of surveillance, however, need not always be about vision (Marx 2002). Indeed, online, we are often not 'seen' by those who surveill us but, rather, our actions, interactions and transactions for all intents and purposes render us more 'visible' than ever before. Even relatively innocuous data, when combined and aggregated, have the potential to reveal (or at least infer) very sensitive information about us, as the data in Chapter Six demonstrated. All these kinds of information, many of which we volunteer ourselves for reward or convenience (Andrejevic 2007), generate knowledge about us as individuals, as members of various groups and communities and as a citizenry. This knowledge, the product of algorithmic calculations, is frequently used to predict and subsequently persuade, instruct and regulate us.

Of course, we are not only subject to 'economic' surveillance. The revelations from Edward Snowden uncovered the mass 'political' surveillance practices of intelligence agencies in the UK and US, where in one case, millions of Internet users were made *literally* more visible as a result of GCHQ intercepting webcam images of Yahoo users (see Ackerman and Ball 2014). It is difficult to theorise to what extent the mass surveillance apparatus of these agencies is linked to online control, given the obscurity that still surrounds the volume of data collected, how they are analysed, who sees them, how long they are kept and where. Despite it being 'invisible' in a similar way to economic surveillance, the data are (we have to assume, or at least we are reassured) not used to alter our behaviour or the virtual environment. It is used only to identify deviancy in the form of the most serious criminal activity and terrorism.

However, what is clear is that both political and economic surveillance are increasingly invisible and unintelligible; carried out largely automatically by computers employing sophisticated algorithms. Schneier (2014) notes that the NSA and GCHQ have used algorithmic surveillance as a defence of sorts for mass online surveillance, the defence being that the large majority of Internet users' data are never viewed by a human operator and, hence, are never actually 'collected'. In another example of regulation of surveillance a US Department of Defense procedural manual says:

> 'Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties…Data acquired by electronic means is "collected" only when it has been processed into intelligible form.' (Department of Defense 1982: 15)

The adequacy of this is questionable; in 1982 it was unlikely they foresaw contemporary technological capabilities. Nevertheless, we are told to trust that our data go no further than the computer receiving them. However, as the Snowden revelations have demonstrated, trust in the intelligence agencies has been somewhat undermined. While their activities have, over the last three years, become more visible than ever before, there remains a high degree of invisibility concerning digital surveillance processes and practices.

Meyrowitz (1985) and Mathiesen (1997) offer useful tools for interpreting the impacts of evolving electronic media on control. Meyrowitz (1985) suggests that electronic media have made different social situations more visible and thus have a liberating effect, breaking down barriers between different social groups. One example of this would be between authorities and citizens (surveillers and surveilled). Meyrowitz argues that the expansion of broadcast media renders public figures more visible, as a result of which their authority can be diminished. The trends Meyrowitz identified in the 1980s in large part remain true today – and have escalated – in the context of social media where many public figures, organisations and institutions have an active presence. The events revolving around WikiLeaks and Snowden have reinforced this trend – albeit a kind of 'forced' visibility placed on political and economic institutions through resistive surveillance. These actions comprise, in part, the inversion of surveillance – 'sousveillance' (Mann *et al.* 2003) – through digital means. What is common to both patterns is that powerful groups in society have less control over what is known about them as a consequence of the changing role of media in society (for which the Internet is the vehicle). Mathiesen (1997) comments on similar trends. For him the 'synopticon' inverted traditional panoptic relationships where instead the 'many watch the few'. Again, this is attributed to new media platforms. However, Mathiesen is pessimistic; the synopticon is not liberating but controlling and 'taken as a whole, things are much *worse* than Michel Foucault imagined' (1997: 231, emphasis in original). As Coleman (2013: 142) echoes, 'the many in society are increasingly encouraged to watch and admire the ways of the powerful few' as a means to keeping us in thrall to control.

Certainly, digital media possess synoptic tendencies insofar as they assist in promulgating the cult of celebrity and providing a means of enchantment and satisfaction; 'it is by satisfying the need for escape that people are made to acquiesce' (Mathiesen 1997: 230).

However, new 'synoptic' media (such as WikiLeaks) do not necessarily reinforce panoptic surveillance. In fact, the practices of 'resistive surveillance' in Chapter Seven show how the concept of the synopticon and sousveillance are somewhat blurred. Moreover, platforms such as social media have also ushered in a situation where the 'many watch the many'. This is a view shared by Doyle (2011) who critiques Mathiesen's argument on the basis that contemporary (online) media have expanded rapidly and further than Mathiesen's analysis is able to adequately account for. Furthermore, Doyle identifies a lack of space within Mathiesen's work for the potential for resistance inherent in new media. The work of this thesis is testament to that potential. Mathiesen's argument suggests that news media, by and large, support the status quo. However, we have seen in Chapter Seven that the new media ecosystem is significantly less stable than this would suggest and has a more complex relationship with surveillance. As Doyle notes, 'in various contexts, mass media conduct surveillance, engender public support for it, help resist surveillance or help the marginalised use surveillance itself as a tool of resistance' (2011: 290). WikiLeaks has, in part, contributed to our understanding of how media and surveillance are entwined. The WikiLeaks case exemplifies all the facets that Doyle lists, while also demonstrating how the 'many watching the few' is as much a form of resistance as it is control.

It is still the case that powerful private and public influences shape what we are presented with in the media, but there is a strong counter-current resulting from the democratising potential of digital technology (Meyrowitz 1985; Brin 1998). In addition, it is not only individuals who can take advantage of these opportunities for resistance through new media. In Chapter Five, the advocacy community connected in different ways through various media platforms. Traditional news media featured in the network, their presence online allowing them to retain some of their power. Twitter, meanwhile, appeared to be a central 'hub' where communication between these groups and with individuals took place at a frenetic rate. Of course, this is not

to discount the fact that such platforms, while instrumental for resistance, are central components in the digital surveillance complex. Doyle (2006: 206) reminds us to be aware that although such tools are democratising and can 'reshape social situations' they are the product of power relations, the likes of which we saw at play in Chapter Six.

Visibility is a valuable concept for understanding digital surveillance and resistance. This thesis has helped to illuminate the continuing transformations in how different social groups (including surveillers and surveilled) and technologies are visible and invisible in the online environment. In light of the findings of this thesis, Doyle (2011) is correct that Mathiesen's (1997) argument for the 'many watching the few' as the central pillar of social control needs re-evaluating. The Internet is a two-way medium capable of offering enormous potential for both surveillance and resistance. Furthermore, the contemporary digital environment should not generate a sense of pessimism regarding digital surveillance and control. Visibility is a precursor to control but it also encourages resistance.

-.-- --- ..- .... .- ...- . -. --- ... --- ...- . .-. . .. --. -. - -.-- .-- .... . .-. . .-- . --. .- - .... . .-. .-.-.-

CHAPTER NINE

CONCLUSION

9.1 THE SURVEILLANCE AND RESISTANCE DYNAMIC

This final chapter summarises the main findings of the thesis and relates these to the broader issues of digital surveillance and social control in the information society. The impact of a specific technological medium – the Internet – on social relations has been at the heart of this thesis. Consequently, the research is situated amidst a broad and varied literature concerned, at its widest, with the contours of the contemporary information or network society and the role of the Internet in society (Castells 1997, 1998, 1999; Fuchs 2008; Graham and Dutton 2014) and, at its most specific, with digital surveillance, resistance, privacy and activism (Marx 2002, 2003, 2009; Lyon 2001, 2003b; Bennett 2008; Dupont 2008; Milan 2013). The evolution of the Internet has rapidly enhanced the volume and speed with which information is transmitted around the world. At the same time, this has had clear consequences for the nature of surveillance in society as more information is generated, volunteered, captured and analysed. Mundane communications, such as telephone calls, all contain metadata that tells our service providers where we were, whom we talked to and when. Our Internet browsing histories are also able to be captured and can reveal a detailed picture of our habits and preferences. Opinions, arguments and all manner of other sentiments are shared in public, online domains such as Facebook and Twitter. Digital data about our personal histories are stored in multiple databases and, as well as containing individual-level information, these data can be aggregated and used to analyse and predict group and population-level behaviour.

Surveillance is carried out for a large number of reasons in both the public and private sectors and increasingly, the motivations of actors from these two realms overlap. Surveillance by the state ('political surveillance') is equated with security for citizens, while much of the ability of the state to fulfil this function rests on accessing data held by custodians in the private sector ('economic surveillance') who

control the digital spaces and channels through which social interactions and transactions take place. At the centre of this network of competition and cooperation are individuals and groups of citizens. Awareness of the myriad mechanisms of surveillance is by no means uniform and even when people are aware of surveillance, it is often accepted as routine or conferring some benefit. However, resistance to surveillance is a constant factor in this dynamic, its technologies and techniques evolving and adapting as new measures to counter risks from crime and terrorism are introduced. The story of this thesis, therefore, is that as much as the Internet has allowed for the growth of surveillance in society, so too has it presented opportunities for resisting surveillance. The relationship between surveillance and resistance is crucial for defining the relationship of technology to society (and vice-versa). Examining this relationship in detail, as this thesis has done, has provided new insights, mapping social order in the information society and how social control constitutes and is constituted by it.

9.2 RESEARCH QUESTIONS

In engaging with these issues, the following questions have guided this thesis:

1. How are digital surveillance and resistance related?
2. Why do individuals and groups who resist surveillance identify a need for doing so?
3. What are the implications of these patterns for our understanding of control in the information society?

The conceptual framework for answering these questions developed out of a theory of nodal governance. Much of what this thesis has contributed with respect to that framework was discussed in the preceding chapter; the significant changes in social organisation brought about by the constant evolution of the Internet (reiterated above) require us to view surveillance through a lens that attunes us to the networked nature of contemporary society, rather than one that emphasises top-down forms of organisation and control. The sites that provided the empirical data for the thesis were selected in line with this framework. They illuminated the multiplicity of social actors involved in the digital surveillance/resistance dynamic and the consequently negotiated, fluid and networked character of social control. It

is with this in mind that we can look at the responses to the overarching research questions.

9.2.1 THE RELATIONSHIP BETWEEN SURVEILLANCE AND RESISTANCE

The introductory discussion serves in part to answer the first research question concerning the relationship between digital surveillance and resistance. This relationship is in constant flux. This is a characteristic identified in earlier work in this area by Marx (2009), who proposed a cyclical model of 'neutralisation' (resistance), 'counter-neutralisation' and 'counter-counter-neutralisation' (and so on). In this respect the patterns that have been identified in this research suggest that the core of the relationship between *digital* surveillance and resistance is the same as that for surveillance and resistance in broader terms as discussed by Marx. However, the nature of the relationship between digital surveillance and resistance can be understood in a more nuanced way. Namely, the relationship enlists a much broader array of inter-connected social actors (identified as governing 'nodes' throughout). Localised instances of 'real world' surveillance may generate effects of resistance at the individual level, and if these render the surveillance technology redundant, measures can be taken to neutralise the resistance by adapting the surveillance technology or practice (and so the cycle begins). However, the context of digital surveillance and resistance is *global*. Surveillance online has a much greater reach and subsequent resistance is generated at the level of networks of individuals and organisations. Technological 'fixes' (Dupont 2008) such as encryption tools do still operate at the individual level but even these are the product of collaborative efforts between actors concerned with erosion of privacy in the digital world. These networks were evidenced in Chapter Five, their overlapping mentalities constituting the basis for the formation of online communities at different levels. They were also seen in operation in Chapter Six, where civil society organisations, individuals and private corporations joined in ad hoc collaborations (even if not intentionally) to resist regulation that would extend the UK surveillance apparatus.

There are three key (related) points to take from this, which have been signalled throughout this thesis. First, the Internet has greatly enhanced the potential for

both digital surveillance and resistance. Regarding the latter, the case of WikiLeaks is particularly enlightening. Second, digital surveillance and resistance are increasingly entwined in the information society. As well as being a product of overlapping roles and motivations, this is also due to the 'fabric' of cyberspace that contains, within it, the building blocks for both surveillance and resistance (Galloway 2004). Third, the relationship between digital surveillance and resistance is to be considered in global and networked terms, however locally the manifestation of this may be played out.

The relationship between digital surveillance and resistance is, therefore, a complex one. It is not the case that there are two opposing sides of the divide – one advocating surveillance that the other resists – who are locked in a perpetual cycle of action and reaction. Different actors at different times are both complicit in surveillance and resistance. CSPs, several of whom featured in Chapter Six, seem particularly key in that respect. At various points in the thesis it has been noted that these entities occupy a prominent place in the surveillance apparatus of the information society. However, this position also confers on them the ability to effectively resist surveillance developments such as new forms of regulation. Individual citizens or users of Internet/digital technologies are also crucially positioned. Collectively, as well as individually, we are the source of much of the data that are collected and analysed by surveillance technologies (Clarke 1998; Lyon 2003). However, there is little evidence of widespread objection to these practices. In part this may be due to a lack of awareness both of the systems and of their implications (see Albrechtslund 2008). It may also be affected by a conscious desire to supply information that confers some sort of reward or benefit. Nevertheless, the findings in Chapter Seven do begin to point towards a growing public consciousness of the role of governments as surveillance agents – if not private sector actors – that has been influenced by the efforts of organisations like WikiLeaks and whistleblowers like Edward Snowden. It is questionable that this amounts to a moral panic about surveillance but equally the chapter argued that an identifiable 'panic' is not the be all and end all of the public's ability to challenge digital surveillance practices.

In addition, another factor in this dynamic is that resistance and digital surveillance are not engaged in a wholesale conflict. What this means is that not all surveillance is resisted – only 'excessive' or 'disproportionate' surveillance. However, this raises the question of who gets to define surveillance in these terms. Undoubtedly, there is an element of moral entrepreneurship at play here. Again, the gratification that digital, economic surveillance can provide (Andrejevic 2007) needs to be acknowledged, as this may go some way towards explaining apathy towards increased surveillance. As the data in Chapter Six illustrated, civil society organisations, private sector enterprises and individuals do recognise there is a need for surveillance that protects citizens and provides security in a range of contexts. However, there is also a feeling that this must be in proportion to the threats and risks faced. The relationship between digital surveillance and resistance should be geared, therefore, towards finding stability, not dominance. Subsequent attempts by the UK government to implement surveillance legislation irrespective of the concerns of civil society, parliamentary committees and a host of other actors suggests, however, that this approach is not currently being taken. We can hypothesise how this situation may continue to develop. As engagement with online services continues to develop, and as surveillance practices evolve as a result, it would be expected that normative values regarding what is 'appropriate' would also shift; necessity and proportionality are not objective. Bringing the discussion of this research question back to where it began, aiming for equilibrium requires networked collaboration between varieties of social actors, while also dictating that there will inevitably be competition in different ways.

9.2.2 WHY RESIST DIGITAL SURVEILLANCE?

This discussion leads us on appropriately to the second research question concerning the motivations for resisting surveillance. The findings of this thesis have shown, in different contexts, why individuals and groups resist digital surveillance. Chapter Five showed that the community of privacy advocates is characterised by a diverse and overlapping set of mentalities. Privacy has been used in previous work as a unifying concept. Bennett (2008) suggested that the organisations constituting this community can be categorised based on their relation to privacy; for some it is a core issue ('privacy-centric'), while for others it is marginal. In the literature, privacy

has typically been inseparable from the practice of surveillance because it is the natural antithesis to the process of extracting, collecting and analysing personal information. However, it is also an amorphous concept (Huey 2010). It is subject to changing interpretations over time and place. What privacy means in one national context may not be the same in another. Indeed, this argument was made to explain the density in the online organisation of German and other European organisations who may share a very different social history of surveillance to their counterparts from other countries. This issue of history and collective memory is an important one as the implications may be broader than simply asking why surveillance is resisted. It may, for instance, impact the nature of policymaking on surveillance, potentially enabling surveillance practices more in line with the 'default to decency'[209] (Molotch 2012). Privacy, then, is an important and underlying rationale for resisting surveillance but we can delve in a little more detail into motivations for resistance. Chapters Six and Seven enabled this by examining specific instances where resistance occurred and the reasons why the digital surveillance in question was challenged.

The UK Communications Data Bill contained reforms that generated a great deal of resistance. Some challenges to the Bill were indeed based on the broad idea of an invasion of privacy. Others, however, were directed at more specific issues and these were grouped into themes in Chapter Six that illuminated the particularly troubling aspects of *digital* surveillance. Foremost among these was the (allegedly) incorrect claim that communications data were less sensitive than content data. The nature of digital interactions and transactions is such that even seemingly mundane information about browsing habits, or the when and where of a telephone call, when collated, can build up a detailed picture of a person's social and personal life. Again, this is a concern related to privacy but demonstrated in a concrete way. Concerns relating to jurisdiction were another key reason for resisting digital surveillance. The global nature of digital communications means that it was not considered appropriate (or indeed possible in some respects) to empower UK-based CSPs to collect and process data shared via overseas social networking websites or other service providers. Other reasons for resisting digital surveillance evident from

[209] See Chapter Six.

the consultation on the CDB included perceptions of function creep – the gradual expansion of digital surveillance capabilities – and a lack of effective oversight, which translates to a problem with the regulation of surveillance practices. Both of these two issues, while enhancing our understanding of why digital surveillance is resisted also speak to broader concerns with surveillance in society.

Chapter Seven's exploration of WikiLeaks, Edward Snowden and the public consciousness/media presentation of surveillance also shed light on reasons for resisting digital surveillance. Rather than focusing on a specific modality of digital surveillance (like the CDB), here the focus shifted to the nature of digital surveillance across society. Underpinning the actions of WikiLeaks[210] and Snowden were two related points. First,the claim that a global network of surveillance is overly intrusive and threatening to civil liberties. Second, the belief that there exists a lack of transparency and accountability as to how such surveillance is carried out. In this sense, the motivations for resisting digital surveillance are to inform public opinion and generate further resistance, for instance through moral panic or by influencing policy debates. While WikiLeaks and Snowden laid out in detail specific surveillance programmes, this form of resistance can be considered as a more broad-based strategy of catalysing public sentiment against unwarranted surveillance.

Particularly in the case of WikiLeaks, the mechanisms for 'resistive surveillance' were an inherent part of the operation of the organisation. WikiLeaks exploited the architecture of the Internet by encrypting and transmitting confidential information anonymously and evading attempts at counter-resistance such as court orders to prohibit access to the WikiLeaks website. In this sense, therefore, the analysis suggested that resistance to digital surveillance was carried out *because it could be* – because the social order of the information society allowed for it. The motivation for doing so was because it was a necessary part of the politics of surveillance in the information society. Consequently resistive surveillance was both the mechanism and motivation for resistance.

The reasons why individuals and groups who resist digital surveillance identify a need for doing so overlap in some ways with 'traditional' forms of surveillance – that

[210] In those contexts where they published information pertaining to surveillance.

is, with previous expositions of the motivations for resistance. Privacy is naturally a common feature that underpins much of the discussion here. Ultimately, surveillance (digital or otherwise) involves extracting or collecting personal information and therefore privacy is the logical counterpoint to this. However, we have seen specific ways in which this concern is played out in the information society. Changes to how we interact and conduct our daily lives through digital forms of communication have altered the ways in which privacy is experienced or considered. This is a process still in constant flux. Again, public awareness of surveillance is important to consider, as is the continued evolution of digital, networked technologies that impact how privacy operates on an individual and societal level. All of this adds further weight to the rationale for this thesis; that the information society has and will continue to generate new manifestations of the relationship between digital surveillance and resistance.

9.2.3 UNDERSTANDING SOCIAL CONTROL IN THE INFORMATION SOCIETY: A SOCIO-TECHNICAL APPROACH

The aim of this thesis has been to examine social control through the lens of surveillance and resistance, and to explore the extent to which it requires re-thinking in a contemporary society that is characterised by global connectivity, networks and information flows. This is no small task and the research has consequently sought to lay out for the reader the breadth of social domains where control is shaped (through practices of surveillance and resistance) but with a degree of focus dictated by a overall narrative. It has achieved this in two ways: through a design informed by a theory of nodal governance and through employing theoretical frameworks that appropriately describe the social processes we see being played out. The final stage of this discussion is to draw all of the previous insights together in response to the question of what the changes in and patterns of digital surveillance and resistance tells us about the nature of control in the information society.

Theoretically, social control is a complex subject, constituted of various influences and subject to much change over time. We saw this in Chapter Three, along with a description of the particular function of surveillance as a modality of control.

Chapter Eight demonstrated where surveillance and resistance intersect with other modalities of control (such as regulation) and also expanded on nodal governance and visibility, concepts that are difficult to separate from a study of surveillance and control in the information society. While each of these themes adds a different dimension to our understanding of the dynamic between surveillance and resistance and how this shapes the character of contemporary control, it should also be apparent that there are continuities tying these themes together. Specifically, that there are *sociological* and *technological* facets of the patterns that have been revealed. These are two sides of the same coin and it is the existence and character of the interplay/relationship between these elements that is the core finding of this thesis.

Control, then, is increasingly experienced as a *socio-technical* process, due to the permeation of networked technologies in our daily lives. This assertion is based on some of the prominent themes discussed in the previous chapter including centralisation/decentralisation, competition and cooperation and visibility. Our understanding of control needs to accommodate the conflicting tendencies for data to be corralled into numerous loci at the same time as the structure of the Internet allows for distributed organisation and communication. Regulation of the ways in which digital data are collected, retained and processed is, likewise, a vital influence on the nature of control. In addition to these factors, the increasingly granular ways in which we are made (and make ourselves) visible online, coupled with efforts to invert this visibility and expose surveillance agents using the Internet, add another dimension to how we understand control in the information society.

This implies two key ideas. First, it points towards control of people and populations within digital spaces, using digital technologies, and through surveillance of digital data. Second, it concerns control of the technologies that constitute the fabric of digital space and that are used in the practice of surveillance. These two denote distinct processes but they are nevertheless inseparable in the context of the information society. A final dimension to consider, of course, is resistance to both these social and technological aspects of control. Combined, these factors constitute what may be called *socio-technical control*.

To fully elaborate this concept, let us briefly take a step back. At the outset of the thesis, and in Chapter Three, the influence of Foucault's (1977) analysis of discipline on studies of surveillance was noted. So too was the incompatibility of the panoptic metaphor for the information society (see Deleuze 1992; Poster 1996; Bogard 2006; Latour 1998; Haggerty 2006). Specifically, Foucault's analysis suggested a state-centric, top-down model and it is this point which is particularly outmoded in contemporary society. Deleuze (1992) said as much in his critique of Foucault. Simply, it comes down to the emergence of the computer as the dominant machine on which society bases its mode of production. This is not to imply a Marxist reading of the situation. It is only highlighted to make clear the pervasiveness on a previously unseen scale of one form of technology and the obvious ramifications this will have (indeed, has had) on society. These arguments have been well rehearsed in this thesis; as networked computing power develops, it re-organises the relationships between people, organisations and states around the world. It is within these networks that control is negotiated and enacted. This is not to diminish the importance of the state in these relationships but it is to suggest they occupy a position within a horizontal, rhizomatic system (Haggerty and Ericsson 2000), not a hierarchical one. Additionally, this needs to be considered more broadly than a system of socio-technical control. This is one result of new forms of social organisation but it is situated within a wider system of socio-technical governance. The defining characteristics of this were laid out in Chapter Two and the logic of this argument was what drove the design of this research. This system of governance is, as Chapter Two described, mainly centred on economic imperatives and the 'information economy', although its other features should not be overlooked.

This broader system complicates our understanding of control because all of the interconnected ways in which economic, social, cultural and technological spheres are governed have some relation to the ability to control in both social and technological ways. Surveillance is necessarily central to how we need to look at control in the information society, simply because it is concerned with the multitude of ways in which information is harnessed and used to monitor and direct the actions of others. Such surveillance need not necessarily be guided by any ulterior motive. The fact is simply that these capabilities and patterns of surveillance have been made possible by technological evolution and they proliferate because they

confer benefits in many ways. How we understand 'benefits' of course *does* depend on the motivation of whoever is carrying out the surveillance. Increasingly granular knowledge of consumers is a benefit for commercial organisations. Instantaneous access to friends and family via social networking is a benefit for individual Internet users. Capturing communications data is a benefit for law enforcement and the state. The point is that in the entire multitude of arenas defined by the socio-technical system of governance, surveillance is enacted in one form or another, for one purpose or another and – from time to time – it is resisted in one way or another.

This is a qualitatively different situation to what has gone before in how we subsequently need to approach control in society. While the state remains an important auspice of control its position is just one within a much wider network of actors whose activities, whether they are oriented towards the control of crime and deviance or not, and as a response and counter-response to the actions of others, produce a complex and shifting web of control. Surveillance in one context can be 'repurposed' in another and thus it is not accurate to think of surveillance solely as a coercive means of controlling deviance. 'Socio-technical control' describes these contemporary patterns wherein control is a product of the multiple, overlapping motivations of a global set of actors connected through digital networks.

The architecture of the Internet itself appears as a useful metaphor for socio-technical control. It is 'distributed' in the sense that there are a large number of globally connected components (nodes) interacting through constantly shifting relationships, some more permanent than others. It is this that allows for resistance to forms of surveillance and control because digital technologies have the potential to 'level the playing field' in many respects. 'Distributed control', then, means to gain a sense of its rhizomatic character. On the other hand, socio-technical control can also be seen as 'decentred'. In this sense, different actors each have ownership over certain control functions and mechanisms of surveillance. Each has capabilities they can leverage and motivations and interests they pursue in competition or cooperation with others. From this perspective there is a degree of horizontality (cooperation) but also hierarchy (competition). Both distributed and decentred models are applicable in the information society. Both describe and are described

by the interaction between surveillance and resistance that this thesis has illustrated. Having said all this, what we have is actually equal parts metaphor and reality, for socio-technical control is enacted within the very digital networks that constitute the Internet.

9.3 CONTRIBUTIONS AND IMPLICATIONS

There are several key contributions this thesis makes to theory and method. There are also implications for policy and the continuing development of practices of digital surveillance. At several points, the thesis has noted that the pace of change of digital communication, the Internet user environment and techniques for monitoring and surveilling is incredibly rapid. Far too quick, in truth, for *research* to effectively keep pace. The close of this section, therefore, updates the social and technological context of the findings of the thesis.

9.3.1 CONCEPTS AND THE LITERATURE ON SURVEILLANCE AND CONTROL

The primary conceptual contribution of this research has largely been outlined in the preceding discussion. Developing an understanding of control that is attuned to both its social and technological features ('socio-technical control') as well as the implicit connection between thetwo is vital in the context of the information society. It was made clear at the start of the thesis that the characterisation of society as networked, and as productive of a social order that is based around information flows, requires us to re-think core concepts such as control. This thesis has begun to contribute to such a reorientation. In sum there are a few core themes to develop.

Centralised, state-centric and top-down notions of control are outmoded for an analysis of the information society. Even former developments in the literature on social control that indicated the growing prominence of private auspices of control (Cohen 1985; Shearing and Stenning 1981, 1983, 1985; Garland 2001) require updating for a society characterised by global, digital connectivity. States remain influential in the apparatus of socio-technical control but they are reliant upon cooperation from other actors. Control through regulation of digital surveillance is an increasingly difficult means of achieving this cooperation. There is some continuity with the literature that highlights the centrality of risk-based approaches

to control as surveillance technologies are key in this regard, however, we must also recognise that the continued expansion of digital communication technologies has, and will, bring with it new risks to be regulated. An interesting dimension that this thesis has highlighted is the paradoxical situation whereby the surveillance mechanisms developed and deployed in response to risks are themselves constructed as dangerous for citizens and for society.

Surveillance is increasingly sophisticated – that was known at the outset of this thesis. However, this research adds weight to the argument that control in the information society is characterised above all by technologies of surveillance. These are utilised by a breadth of social actors with differing motivations, but which are all connected to the emergence of information as a global commodity. The thesis contributes, then, to the body of work that advocates a 'post-panoptic' view of surveillance. Coercion, compliance and the control of deviancy are effects that are still pursued through surveillance by the state, but these go hand in hand with other rationales for surveillance in other sectors of society.

The other main conceptual contribution made by this thesis to the area of surveillance studies and social control is that resistance is an inherent and fundamental part of how control is shaped. This is especially true in the context of digital surveillance, owing to the potential for resistance that the Internet creates, through networked communication, organisation and technical 'fixes' (Dupont 2008). Digital surveillance cannot be explored without regard to those counter-measures designed to limit its spread and mitigate its effects. Increasingly, as surveillance practices pervade every social domain, we also need to give due regard to the changing nature of resistance. Resistance to surveillance in general is most commonly framed as 'privacy advocacy', while to digital surveillance in particular it is typically described by encryption or anonymisation tools. However, what this thesis has shown is that resistance takes many forms and there are many reasons why individuals and groups choose to resist. Surveillance and resistance are inseparable. As one develops, the other adapts, and this is a feature of that relationship that is only amplified by continued evolution of the information society.

9.3.2 METHODOLOGICAL INNOVATION

It is also worth revisiting the approach the thesis has taken to studying surveillance and resistance empirically and how this might inform future research in related areas. The thesis advocates a broader move that is required towards new methodological approaches in the social sciences. The development of new methods at the intersection of computer science and social science is naturally one part of this. Such innovation allows researchers to capitalise on the wealth of data that are produced in digital spaces. It also drives interdisciplinarity, enabling new insights into social data. This is a positive and necessary step forward for the social sciences. However, we might also look to a more general paradigm shift in the way in which research is structured in the context of our mobile, connected and digitally augmented society.

A defining characteristic of this research, then, has been its use of a diverse methodological toolkit. The decisions relating to the use of certain methods and their application to three distinct cases have been outlined for the reader. Early in the research process, it became clear that studying digital surveillance and resistance could not be confined to one instance where this relationship played out. Although the intention, at the very earliest stages, was to carry out an exploration of WikiLeaks as the basis for the thesis, it was evident that there was much more 'going on' that not only *could* be studied, but *should* be studied to develop a sound understanding of how surveillance and resistance interacted in the digital world. One example of this is a key contribution of the thesis to both theory and method. No previous research has sought to use legislation as a window onto resistance. However, as has been emphasised throughout, the opportunity the CDB presented and the novel insights it generated were invaluable for the research and for the broader impact of the thesis.

Collectively, the cases selected captured a set of inter-related processes that characterised much of the current nature of digital surveillance and resistance to surveillance. There is of course a good deal more that might have been observed. Social phenomena are not static. This is especially true for the context of this research; the landscape is rapidly changing and there are already shifts that have

occurred which necessitate further research beyond that presented[211]. Above all, however, the methodology employed avoids the kind of grand theorisation and abstracted empiricism that Mills (1959) felt inappropriate for contemporary sociology.

While the thesis has focused on social change in the context of the information society and the Internet, the fieldwork was not designed to examine empirically only online behaviour. The purpose of the research was to examine a range of social activity within that specific context. The methodology – both the multi-case design and the use of a varied methodological toolkit – reflected this aim; indeed it was required to meet it. The data that emerged from each of the three sites were diverse and unique to each particular case. In instances such as this, *integration* of data is a key issue. Data were integrated as part of a broader strategy to understand, as comprehensively as possible (within the restrictions of the research), how digital surveillance and resistance interacted as part of a system of social control. Fielding (2012) observes three key reasons for conducting mixed-method research and it is the final one of these – 'analytic density' – that applies particularly to the research design here. This rationale is not about gaining more reliable or valid findings (another reason for triangulation strategies) but is instead about 'getting a wider and deeper picture from all angles' (Shih 1998: 633). This approach, Fielding argues, must be animated by a guiding theory and for this thesis that theory was nodal governance. This was put in place at the start of the thesis. As the research progressed, the theoretical frame was validated by the interactions seen occurring between the various nodes involved. Equally, it allowed for fresh theoretical insight to be generated when the data were taken as a whole. The integration of data in these terms took place in the form of a narrative running through the thesis, which culminated in Chapter Eight where themes relating to the features of social control and surveillance were elaborated. Overall, the methodology was both a necessary and valuable way of studying these particular social phenomena. It is an approach that will be increasingly important for social science research that is situated in, and seeks to study, digital society in all its guises. The context of digital surveillance is wide ranging and complex, and thus to study

[211] See below – section 9.3.3.

one aspect in isolation would have been to the detriment of the research. Consequently, the thesis contributes to knowledge about the many ways in which digital surveillance and resistance interact to produce what we might identify as the state of surveillance in contemporary society.

9.3.3 THE SHAPE OF THE DIGITAL SURVEILLANCE SOCIETY

This thesis is positioned in proximity to a rapidly shifting policy landscape. A great deal has changed since the inception of the research. Indeed, the world had not heard of Edward Snowden when the research commenced. The state of surveillance had continued to change up until that point but from mid-2013 this landscape shifted immensely. The legislative arena has also seen a lot of changes and these have all been framed in light of the new knowledge that Snowden helped to bring to the public domain. As a consequence, there has been a persistent critical narrative within the policy realm regarding digital surveillance. Now more than ever, surveillance is a highly politicised subject and it is to be hoped that research in this area contributes to the growing consensus that surveillance matters in the everyday lives of ordinary people.

The patterns that this research identified in Chapter Six with regards to the regulation of surveillance technologies have been largely repeated during the time of writing this thesis. In November 2015, the government published the Draft Investigatory Powers Bill. In many ways, this Bill mirrored the Communications Data Bill, not least because it replicated the consultation process undertaken three years previously. Likewise a similar response was seen from civil society organisations, CSPs, and technical and legal experts. Regardless of this negative reaction, the Bill is currently in the House of Lords, following only minor amendments that do not address the multitude of privacy and oversight-related concerns voiced during the consultation. These concerns were also foreshadowed in the form of three independent reports in 2015 into surveillance capabilities in the UK (Anderson 2015; ISC 2015; RUSI 2015). This climate of public and policy concern surrounding digital surveillance illustrates the contemporaneity of this research. Surveillance studies as a field of inquiry has already established a good presence in this area. Incorporating wider issues by drawing on ideas from other disciplines, like this research has done,

there is an opportunity to develop a robust social scientific contribution to these debates as they rumble onwards.

In broader terms, there is also scope for this research to feed into an exploration of the role of 'digital civil society'. This has emerged as a prominent undercurrent in the research. There is good potential for some of the tools used in this research to be used to map other sub-sectors of civil society. Specifically, it would be valuable to examine their involvement in and shaping of public and policy discourses in online spaces. The story of this thesis has been how the evolution of the information society has impacted on one particular social process and those lessons could be easily translated to other issues as they arise. The potential for digital spaces and communication technologies to foster collective or 'connective' action (Bennet and Segerberg 2012) is enormous and social research should take care to keep pace with these developments.

9.4 CONCLUDING THOUGHTS

This thesis has provided an empirical study of digital surveillance and resistance to surveillance. Its contributions are both theoretical and empirical. They relate to developing a critical sociological and criminological understanding of social control in the information society and illustrating, through a multi-case approach, how relationships between surveillance and resistance play out in this context. It is a timely piece of research. As outlined above it touches on issues including the necessity and proportionality of Internet surveillance for crime prevention and national security, the right to privacy and the role of civil society in advocating this, the 'problem' of encrypted communication (insofar as it hinders government attempts to provide security) and protection for whistleblowers are just some of those at the centre of debates that continue to run back and forth. This closing section highlights some of the limitations of the research but also the promising directions in which it takes us.

9.4.1 LIMITATIONS AND FUTURE DIRECTIONS

It is always the case with any project that compromises will need to be made for the sake of progress. On reflection, there are always things we would have done

differently or spent more time on. This is part of the research journey and looking back on what has been achieved allows us to take our research forward to investigate new problems and capitalise on new opportunities. The first point worth highlighting is perhaps not so much a limitation but rather a challenge of researching surveillance and the Internet. Things move and change quickly. As a case in point, Snowden's revelations appeared at a point in the research when fieldwork had concluded. However, given the immense significance of these developments for the research, it was necessary to represent them in some way in the research. The final shape of Chapter Seven is the result of this. Following that, it was hard enough to keep up to date with the breaking stories on a personal level, let alone incorporate them into the thesis. A doctoral research project begun in 2013 would have enough material in the space of a few months to inform a thorough analysis of the changing nature of digital surveillance and control.

Similarly, while editing the findings chapter based on analysis of the CDB, new European legislation was introduced that changed the landscape of data retention. This was shortly followed by emergency legislation in the UK[212] contravening these measures and enacting – to an extent – some of the proposals from the rejected CDB. The pace of change is an on-going challenge that social researchers investigating digital society will have to tackle. Fortunately, it appears that new computational research tools are enhancing our capabilities in this respect.

A particular methodological limitation of the research is connected to the experience of using such tools, particularly *Issue Crawler*. While yielding helpful data and allowing some flexibility in their presentation, the tool itself required some leaps of faith. The software offers little explanation of how network metrics are calculated. As a novice in the field of social network analysis this required a lot of experimentation to ensure that results were interpreted correctly. Furthermore, in Chapter Four, the issue of hyperlink analysis using *Issue Crawler* was raised. Specifically, the question of whether we can attribute *meaning* to the practice of hyperlinking. This had to be inferred, to an extent, although the arguments made were satisfactory. On reflection, it would have added a valuable dimension to the

[212] Data Retention and Investigatory Powers Act (2015): https://www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014.

analysis if the resulting network diagrams were used as interview aids with members of the privacy advocacy groups. Seeking interpretations of these, based on their knowledge and experience of being involved in the community, would have provided more depth and rigour to the findings in that chapter.

A second related limitation concerns the interview component of the methodology. The intention was to conduct more interviews than was the end product. In part, this was due to several of the individuals contacted not being able to take part or contact with them drying up despite initial interest in the research. Among such potential participants were members of more advocacy groups based in the UK, a senior policy advisor at the Information Commissioner's Office and a member of the Icelandic parliament engaged in a programme aiming to establish a new foundation for free speech in the media[213]. The views of these individuals, and more, would have added a depth to the findings that, on occasion, would have helped to develop the insights presented. However, the opportunity afforded by the publication of the consultation on the CDB went a small way to remedying this shortfall. The consultation illuminated the voices of many people who would otherwise have been overlooked or (in the case of individual 'non-experts') or I would never had the fortune to encounter. It also goes without saying that, despite a great deal of determination and employing numerous tricks of the trade, it was disappointing not to meet with Julian Assange. It is to be hoped that future research might cause our paths to cross. Either that, or an application for asylum in Ecuador.

Finally, each of the case studies that constituted this thesis could have been the sole basis for a much more substantial piece of research, given the time to do so. In simple terms, network analyses could have continued for longer, all responses to the CDB, as well as subsequent legislation, could have been examined in finer detail, and leaked documents from WikiLeaks and Snowden could have been subjected to similar analysis. In addition, the issues the analysis highlighted in each case were valuable enough to warrant further inquiry. Aside from the time constraints, however, the approach taken was the most suitable for gaining a thorough appreciation of the complex dynamics of digital surveillance and resistance as they are played out in different contexts.

[213] The Icelandic Modern Media Institute: https://en.immi.is/.

Some of these limitations point naturally towards directions that future research might take. The affordances offered by the consultation process for the CDB were tremendous for social research. The fact that equal amounts of data are now available following the consultation on the Investigatory Powers Bill should allow for more rigorous analysis of the process of regulating surveillance. Relatedly, a promising avenue of inquiry not able to be followed in depth in this research was regulation of cyberspace or, in other words, regulation of the technology – 'code' (Lessig 1999) or 'protocol' (Galloway 2004) – that constitutes the architecture of the Internet. This is a crucial area to investigate as it is as much a part of 'socio-technical control' as forms of digital surveillance. Future research should seek to illuminate both regulation of behaviour (i.e. regulation of companies who provide online services) and also regulation of the infrastructure of the Internet. This thesis has been unable to examine the latter in detail but it is a crucial component in shaping how we experience the Internet and how it can be used for repressive and liberating purposes. Theoretically, this approach would also enable a fuller exposition of a theme that began to emerge in the course of the thesis but that did not make it through the final stage of editing. This concerns theories of space and place. The intersection between theories of social control and space is interesting and apposite, particularly as we begin to adapt the former to the digital world as this thesis has done. Cyberspace is a unique environment in which to study surveillance and control because, unlike in the physical world, the entire architecture and laws of the spaces people inhabit can be re-designed. As was stated in Chapter One, the digital world is increasingly designed to surveill.

Related to this proposal for a 'topology of control' in relation to the Internet, there is a pressing question that should guide future research: how does social control occur on the 'Dark Web'? There is a lack of social research into the Dark Web, those areas of the Internet only accessible using certain software such as Tor. Next to the World Wide Web, the 'Dark Web' is a space we know comparatively little about. We know it is a space where illicit activities are carried out: a burgeoning drugs trade, child pornography, and sales of illegal firearms. It is a place where alternative currencies such as 'BitCoin' are built. Subversive networks of hackers and activists gather on the Dark Web. Anonymous and LulzSec are two prominent examples of such groups but also included here are WikiLeaks who made use of the Dark Web to allow

whistleblowers to leak information without fear of surveillance. If we aim to fully understand the ways in which social control occurs in online environments, then we must explore those spaces where people actively and *successfully* seek to avoid it. Using ethnographic methods to immerse oneself in these spaces, while challenging in terms of researcher safety and ethics, suggest themselves as the most promising toolkit to explore these issues. Some questions that might begin to frame an exploration of this subversive cyberspace are as follows:

1. Why do people use the Dark Web? What are the 'perceived futures' of encrypted and 'hidden' social interaction?
2. How do government and law enforcement frame the 'problem' of Dark Web communication/interaction?
3. To what extent is formal and informal social control evident on the Dark Web and how do these differ from patterns of control on the World Wide Web?

A final direction for future research is concerned with methodology, for two reasons. There is enormous potential in the use of computational research methods for exploring social processes as they occur at the level of populations and in real-time. Chapter Five drew the reader's attention to the importance of social media as a forum for negotiating surveillance. Having experimented with the tools to explore interactions here in more detail but not developed this line of research in the thesis, it is easy to advocate a more detailed investigation of the communities and conversations that occur in these spaces; much like the hyperlink analysis, but on a more granular level. In this way, 'surveillance events' could be tracked as they unfold and their social impact analysed. The second reason for pursuing research using computational methods is to stimulate a debate across all disciplines of the social sciences regarding their associated ethical issues. The question of to what extent these tools constitute 'surveillance' is a pertinent one.

9.4.2 FINAL THOUGHTS

This thesis has examined the interplay of digital surveillance and resistance and developed our understanding of the contemporary character of social control. It has developed an innovative methodology to encompass a variety of social relations

related to digital surveillance and resistance. This has both added to existing knowledge – for instance of advocacy networks and the cultural politics of surveillance – as well as contributed new knowledge regarding how legislation can be a window onto resistance. Consequently, the thesis shows how organisation in, and governance of, online spaces occurs, both producing and resisting forms of control. The Internet represents, for some, the foundation of a progressive social order which is, consequently, to be protected from intrusive surveillance. Others say that it is necessary to enhance control online in order to preserve national security and protect the broader (economic) social order. The outcome is a complex web of relationships and entanglements of power wherein resistance, counter-resistance, negotiation and bargaining shape the nature of the Internet and social control.

In light of the findings of the thesis, what we now know is that control, in a society characterised by ubiquitous computing and digital interaction, must be understood as a socio-technical process. The Internet is a socio-technical system and as such there are social and technological forms of control. Surveillance proliferates in this domain, capturing immense amounts of data on an increasingly digital citizenry. Importantly, however, the dynamics and politics of surveillance play out in the 'real world' as well as online. While 'the digital' contains enormous potential for control in its own right, these patterns impact significantly on 'the physical'. This message is not a pessimistic one. Digital spaces *are* highly susceptible to surveillance and control; but the logic of this means that they are equally, if not more, capable of opening up new forms of organisation, order and resistance.

-.-- --- ..- .... .- ...- . -. --- ... --- ...- . .-. . .. --. -. - -.-- .-- .... . .-. . .-- . --. .- - .... . .-. .-.-.-

BIBLIOGRAPHY

Ackerman, S. and Ball, J., (2014), Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ, *The Guardian*, 28th February, available online at: http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo, accessed Mar 2014

Ackland, R. and Gibson, R., (2013), Hyperlinks and Networked Communication: A Comparative Study of Political Parties Online, *International Journal of Social Research Methodology*, 16 (3), 231-244

Agamben, G., (2005), *State of Exception*, Chicago, IL: Chicago University Press [translated by Kevin Attell]

Akdeniz, Y., Taylor, N. and Walker, C., (2001), BigBrother.gov.uk: State Surveillance in the Age of Information and Rights, *Criminal Law Review*, February, 73-90

Albrechtslund, A., (2008), Online Social Networking as Participatory Surveillance, *First Monday*, available online at: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949, accessed Dec 2014

Alexa Internet, (2013), *Top Sites*, available online at http://www.alexa.com/topsites, accessed Nov 2013

Altheide, D., (1996), *Qualitative Media Analysis*, Thousand Oaks, CA: SAGE Publications

Altheide, D., (2009), 'Moral Panic : From Sociological Concept to Public Discourse', *Crime, Media and Culture*, 5 (1), 79-99

Anderson, P., (2007), What is Web 2.0? Ideas, Technologies and Implications for Education, *JISC Technology and Standards Watch*, available online at http://www.jisc.ac.uk/media/documents/techwatch/tsw0701b.pdf, accessed Nov 2014

Anderson, D., (2015), *A Question of Trust: Report of the Investigatory Powers Review*, London: HMSO

Andrejevic, M., (2005), The Work of Watching One Another: Lateral Surveillance, Risk and Governance, *Surveillance and Society*, 2 (4), 479-497

Andrejevic, M., (2007), *iSpy: Surveillance and Power in the Interactive Era*, Lawrence, KS: University of Kansas Press

Armitage, R., (2002), *To CCTV or not to CCTV? A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime*, Community Safety Practice Briefing, London: NACRO

Arthur, C., (2013), What the New York Times Chinese hack tells about the layer cake of hacking, *The Guardian*, Friday 1st February, available online at: http://www.guardian.co.uk/technology/2013/jan/31/new-york-times-hacking-china-lessons, accessed May 2013

Associated Press, (2013), Edward Snowden says NSA surveillance programs 'hurt our country', *The Guardian*, Saturday 12th October, available online at: http://www.theguardian.com/world/2013/oct/12/edward-snowden-nsa-surveillance-wikileaks-videos, accessed Nov 2014

Ayres, I. and Braithwaite, J., (1992), *Responsive Regulation: Transcending the Deregulation Debate*, New York, NY: Oxford University Press

Ball, J., (2012), WikiLeaks releases first 200 of 5m Stratfor emails, *The Guardian*, Monday 27th February available at: http://www.theguardian.com/media/2012/feb/27/wikileaks-stratfor-emails-anonymous, Jun 2014

Ball, J., (2013a), Exclusive: Former WikiLeaks Employee James Ball Describes Working With Julian Assange, *The Daily Beast*, Thursday 30th May, available online at: http://www.thedailybeast.com/articles/2013/05/30/exclusive-former-wikileaks-employee-james-ball-describes-working-with-julian-assange.html, Jul 2014

Ball, J., Borger, J. and Greenwald, G., (2013), Revealed: How US and UK spy agencies defeat Internet privacy and security, *The Guardian*, Friday 6th September,

available online at http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, accessed Nov 2013

Barlow, J. P., (1996), *A Declaration of the Independence of Cyberspace*, available online at: https://projects.eff.org/~barlow/Declaration-Final.html, accessed May 2011

Bauman, Z. and Lyon, D., (2013), *Liquid Surveillance: A Conversation*, Cambridge: Polity Press

Bauman, Z., (2000), *Liquid Modernity*, Cambridge: Polity Press

BBC News, (2009), *UK 'most watched nation' by CCTV*, Tuesday 21st July, available online at: http://news.bbc.co.uk/1/hi/uk/8160757.stm, accessed Jun 2012

BBC News, (2013), *Bitcoin virtual currency reaches all-time high price*, Thursday 28th February, available online at: http://www.bbc.co.uk/news/technology-21601608, accessed May 2013

Beck, U., (1992), *Risk Society: Towards a New Modernity*, London: SAGE Publications

Beck, U., Giddens, A. and Lash, L., (1994), *Reflexive Modernisation: Politics, Tradition and Aesthetics in the Modern Social Order*, Cambridge: Polity Press

Becker, H., (1963), *Outsiders: Studies in the Sociology of Deviance*, New York, NY: The Free Press

Becker, H., (1967), Whose Side Are We On? *Social Problems*, 14 (3), 239-247

Becker, H., (2014), *What About Mozart? What About Murder?* Chicago, IL: University of Chicago Press

Beckett, C. and Ball, J., (2012), *WikiLeaks: News in the Networked Era*, Cambridge: Polity Press

Bell, D., (2009), Surveillance is Sexy, *Surveillance and Society*, 6 (3), 203-212

Beniger, J. R., (1986), *The Control Revolution: Technological and Economic Origins of the Information Society*, Cambridge, MA: Harvard University Press

Bennett, C., (2008), The Privacy Advocates: Resisting the Spread of Surveillance, Cambridge, MA: MIT Press

Bennett, W. L. and Segerberg, A., (2012), The Logic of Connective Action, *Information, Communication and Society*, 15 (5), 739-768

Bennett, W. L., (2012), The Personalization of Politics: Identity, Social Media and Changing Patterns of Participation, *The ANNALS of the American Academy of Political and Social Science*, 644, 20-39

Bentham, J., (1791), Panopticon, or the inspection house, & C., in E. McLaughlin and J. Muncie (eds.), (2013), *Criminological Perspectives: Essential Readings*, 3rd ed., London: SAGE

Berners-Lee, T., (2006), *developerWorks Interviews: Tim Berners-Lee* [interview by Scott Laningham], available online at http://www.ibm.com/developerworks/podcast/dwi/cm-int082206txt.html, accessed Nov 2013

Berners-Lee, T., (2010), Long Live the Web: A Call for Continued Open Standards and Neutrality, *Scientific American*, December 2010

Bogard, W., (2006), Surveillance assemblages and lines of flight, in Lyon, D. (ed.), *Theorizing Surveillance: The Panopticon and Beyond*, Cullompton: Willan

Bonger, W., (1969), *Criminality and Economic Conditions*, Boston, PA: Little, Brown and Co.

Booth, J., (2004), UK 'sleepwalking into Stasi state', *The Guardian*, Monday 16th August, available online at http://www.theguardian.com/uk/2004/aug/16/britishidentity.freedomofinformation, accessed Nov 2014

Bourdieu, P., (1986), The Forms of Capital, in Richardson, J. (ed.), *Handbook of Theory and Research for the Sociology of Education*, New York, NY: Greenwood

boyd, d. and Crawford, K., (2012), Critical Questions for Big Data: Provocations for a Cultural, Technological and Scholarly Phenomenon, *Information, Communication and Society*, 15 (5), 662-679

boyd, d., (2008), Putting Privacy Settings in the Context of Use (in Facebook and Elsewhere), *Apophenia*, available online at: http://www.zephoria.org/thoughts/archives/2008/10/ 22/putting_privacy.html, accessed Dec 2014

Brevini, B., Hintz, A. and McCurdy, P. (eds.), (2013), Beyond WikiLeaks: Implicaitons for the Future of Communications, Journalism and Society, Basingstoke: Palgrave Macmillan

Bright, J. and Agustina, J. R., (2013), Mediating Surveillance: The Developing Landscape of European Online Copyright Infringement, *Journal of Contemporary European Research*, 9 (1), 120-137

Brin, D., (1998), *The Transparent Society*, Reading, MA: Perseus Books

Brooke, H., (2010), WikiLeaks: The revolution has begun - and it will be digitised: The web is changing the way in which people relate to power, and politics will have no choice but to adapt too, *The Guardian*, Tuesday 30th November, available online at: http://www.theguardian.com/commentisfree/2010/nov/29/the-revolution-will-be-digitised, accessed May 2011

Brooke, H., (2011), *The Revolution Will Be Digitised: Dispatches from the Information War*, London: Random House

Brown, I. and Korff, D., (2009), Terrorism and the Proportionality of Internet Surveillance, *European Journal of Criminology*, 6 (2), 119

Brown, I., (2010), Communications Data Retention in an Evolving Internet, *International Journal of Law and Information Technology*, 19 (2), 95-109

Brown, I., (2010), *Future Internet Expert Workshop: Notes*, Future Internet Expert Workshop for the Towards a Future Internet (TAFI) Project, 15 March 2010, MIT, Boston

Bruns, A., Burgess, J., Highfield, T., Kirchhoff, L. and Nicolai, T., (2010), Mapping the Australian Networked Public Sphere, *Social Science Computer Review* [online], 21st September 2010

Bryman, A., (2004), *Social Research Methods*, 2nd ed., Oxford: Oxford University Press

Bryman, A., (2004a), Multi-Method Research, in M. S. Lewis-Beck, A. Bryman and T. Futing Liao, *The SAGE Encyclopedia of Social Science Research Methods*, Thousand Oaks, CA: SAGE Publications

Burgess, R. G., (1984), *In the Field: An Introduction to Social Research*, London: Allen & Unwin

Burnap, P., Rana, O., Avis, N. J., Williams, M. L., Housley, W., Edwards, A., Morgan, J. and Sloan, L., (2013), Detecting Tension in Online Communities with Computational Twitter Analysis, *Technological Forecasting and Social Change*

Burris, S., Drahos, P. and Shearing, C., (2005), Nodal Governance, *Australian Journal of Legal Philosophy*, 30, 30-58

Castells, M., (1996), *The Rise of the Network Society, The Information Age: Economy, Society and Culture*, Vol. 1, Oxford: Blackwell

Castells, M., (1997), *The Power of Identity*, *The Information Age: Economy, Society and Culture*, Vol. 2, Oxford: Blackwell

Castells, M., (1998), *The End of the Millennium, The Information Age: Economy, Society and Culture*, Vol. 3, Oxford: Blackwell

Ceyhan, A., (2008), Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics, *Surveillance and Society*, 5 (2), 102-123

Chatterjee, P., (2011), In Video – Surveillance Explained, *The Bureau of Investigative Journalism*, available online at: http://www.thebureauinvestigates.com/2011/12/01/in-video-surveillance-explained/, accessed Jun 2014

Chen, H., (2012), *Dark Web: Exploring and Data Mining the Dark Side of the Web*, New York, NY: Springer

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M. and Weimann, G., (2008), Uncovering the Dark Web: A Case Study of Jihad on the Web, *Journal of the Association for Information Science and Technology*, 59 (8), 1347-1359

Clark, L., (2014), UK privacy expert: For real reform we must demand 'surveillance minimisation, *Wired.co.uk*, available at: http://www.wired.co.uk/news/archive/2014-01/23/surveillance-minimisation, accessed Oct 2014

Clarke, R., (1988), Information Technology and Dataveillance, *Communications of the ACM*, 31(5), 498-512

Coffey, A. and Atkinson, P., (2004), Analysing Documentary Realities, in D., Silverman, (ed.), *Qualitative Research: Theory, Method and Practice*, London: SAGE Publications

Cohen, S. and Young, J., (1973), *The Manufacture of News: Deviance, Social Problems and the Mass Media*, London: Constable

Cohen, S., (1972), *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, Oxford: Blackwell

Cohen, S., (2002), *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*, (2nd ed.), Oxford: Blackwell

Cohen, S., (1985), *Visions of Social Control*, Cambridge: Polity Press

Cole, S. A., (2001), *Suspect Identities: A History of Fingerprinting and Criminal Identification*, Harvard, MA: Harvard University Press

Coleman, R., (2013), Imagining the City State: Synoptic Power and Urban Ordering, in K. Ball, and L. Snider, (eds.), *The Surveillance-Industrial Complex*, London: Routledge

Compaine, B. M. (ed.), (2001), *The Digital Divide: Facing a Crisis or Creating a Myth*, Cambridge and London: MIT Press

Conway, J., (1977), Protecting the Private Sector At-Will Employee Who 'Blows the Whistle': A Cause of Action Based Upon Determinants of Public Policy, Wisconsin Law Review, 77, 777-812

COSMOS, (2014), Ethics Resource Guide, *Collaborative Online Social Media Observatory*, available online at: http://www.cs.cf.ac.uk/cosmos/ethics-resource-guide/, accessed Dec 2014

Court of Justice of the European Union, (2014), C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, Press Release No. 54/14, Luxembourg

Cresswell, J. W., (2008), Mixed Methods Research, in L. M. Given, (ed.), *The SAGE Encyclopedia of Qualitative Research Methods*, Thousand Oaks, CA: SAGE Publications

Critical Art Ensemble, (2009), *Electronic Civil Disobedience*, New York, NY: Autonomedia, available online at http://www.critical-art.net/books/ecd/, accessed Nov 2013

Dahrendorf, R., (1959), *Class and Conflict in an Industrial Society*, London: Routledge and Kegan Paul

Dandeker, C., (1994), *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, Cambridge: Polity Press

Deleuze, G. and Guattari, F., (1987), *A Thousand Plateaus: Capitalism and Schizophrenia*, [translated by B. Massumi], London: Continuum

Deleuze, G., (1992), Postscript on the Societies of Control, *October*, 59 (Winter), 3-7

della Porta, D., (2008), Eventful Protest, Global Conflicts, *Distinktion, Scandinavian Journal of Social Theory*, 17, 27-56

Department of Defense, (1982), *Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons*, DoD 5240-1R, December

Doctorow, C., (2013), Internet copyright law has to have public support if it's going to work, *The Guardian – Technology Blog*, Thursday 31st January, available online

at: http://www.guardian.co.uk/technology/blog/2013/jan/31/internet-copyright-law, accessed May 2013

Dodge, M. and Kitchin, R., (2001), *Atlas of Cyberspace*, London: Pearson Education

Domscheit-Berg, D., (2011), *Inside WikiLeaks: My Time with Julian Assange at the World's Most Dangerous Website*, London: Random House

Doyle, A., (2006), An Alternative Current in Surveillance and Control: Broadcasting Surveillance Footage of Crimes, in K. Haggerty and R. V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, Toronto, ON: University of Toronto Press

Doyle, A., (2011), Revisiting the Synopticon: Reconsidering Mathiesen's 'The Viewer Society' in the Age of Web 2.0, *Theoretical Criminology*, 15 (3), 283-299

Dr-K, (2000), *A Complete H@ckers Handbook: Everything You Need to Know About Hacking in the Age of the Internet*, London: Carlton

Dupont, B., (2003), Public Entrepreneurs in the Field of Security: An Oral History of Australian Police Commissioners, paper presented at *In Search of Security: An International Conference on Policing and Security*, Montreal, QC: Law Commission of Canada

Dupont, B., (2006), Power Struggles in the Field of Security: Implications for Democratic Transformation, in J. Wood and B. Dupont (eds.), *Democracy, Society and the Governance of Security*, Cambridge: Cambridge University Press

Dupont, B., (2008), Hacking the Panopticon: Distributed Online Surveillance and Resistance, *Sociology of Crime, Law and Deviance*, 10, 259-280

Dutton, W. H., (2013), The Social Shaping of Digital Research, *International Journal of Social Research Methodology*, 16 (3), 177-195

Edelman, M., (1964), *The Symbolic Uses of Politics*, Urbana, IL: University of Illinois Press

Edwards, A., Housley, W., Williams, M. L., Sloan, L. and Williams, M. D., (2013), Digital Social Research, Social Media and the Sociological Imagination: Surrogacy,

Augmentation and Re-Orientation, *International Journal of Social Research Methodology*, 16 (3), 245-260

Ericson, R. V., Baranek, P. M. and Chan, J. B. L., (1989), *Negotiating Control: A Study of News Sources*, Toronto, ON: University of Toronto Press

Ericson, R. V., Baranek, P. M. and Chan, J. B. L., (1991), *Representing Order: Crime, Law and Justice in the News Media*, Toronto, ON: University of Toronto Press

Ess, C., (2002), *Ethical Decision Making and Internet Research: Recommendations from the AoIR Ethics Working Committee*, available online at: http://aoir.org/reports/ethics.pdf, accessed Dec 2014

European Commission, (2012), *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, 2012/0011 (COD), C7-0025/12, 25th January 2012 available online at: http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM%282012%290011_EN.pdf, accessed Nov 2013

Evans, A., Elford, J. and Wiggins, D., (2008), Using the Internet for Qualitative Research, in C. Willig and W. Stainton-Rogers, (eds.), *The SAGE Handbook of Qualitative Research in Psychology*, London: SAGE Publications

Facebook, (2013), Timeline*, Facebook Newsroom*, available online at http://newsroom.fb.com/Timeline, accessed Nov 2013

Feeley, M. and Simon, J., (1994), Actuarial Justice: The Emerging New Criminal Law, in D. Nelken (ed.), *The Futures of Criminology*, London: Sage

Ferrell, J. and Webdale, N., (1999), *Making Trouble: Cultural Constructions of Crime, Deviance and Control*, Hawthorne, NY: Aldine de Gruyter

Fielding, N., (2012), Triangulation and Mixed Methods Designs: Data Integration with New Research Technologies, *Journal of Mixed Methods Research*, 6(2), 124-136

Fielding, N. and Lee, R. M., (2008), Qualitative e-Social Science/Cyber Research, in R. M. Lee, N. Fielding and G. Blank, (eds.), *The SAGE Handbook of Online Research Methods*, London: SAGE Publications

Fischer, M., Lyon, S. and Zeitlyn, D., (2008), The Internet and the Future of Social Science Research, in R. M. Lee, N. Fielding and G. Blank, (eds.), *The SAGE Handbook of Online Research Methods*, London: SAGE Publications

Foucault, M., (1977), *Discipline and Punish: The Birth of the Prison*, New York, NY: Vintage Press

Foucault, M., (1991), Governmentality, in G. Burchell, C. Gordon and P. Miller (eds.), *The Foucault Effect: Studies in Governmentality*, Chicago, IL: Chicago University Press

Fuchs, C., (2008), *Internet and Society: Social Theory in the Information Age*, New York, NY: Routledge

Fuchs, C., (2013), "Castells and Jenkins…these approaches are terribly flawed": An Interview with Christian Fuchs, *Sociologija Media Blog* (Bilic, P.), available online at: http://fuchs.uti.at/959/, accessed Nov 2013

Galloway, A. R., (2004), *Protocol: How Control Exists After Decentralisation*, Cambridge, MA: MIT Press

Gandy, O. H., (1993), *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, CO: Westview Press

Garcia, A. C., Standlee, A. I., Bechkoff, J. and Cui, Y., (2009), Ethnographic Approaches to the Internet and Computer-Mediated Communication, *Journal of Contemporary Ethnography*, 38 (1), 52-84

Garland, D. (1985), *Punishment and Welfare: A History of Penal Strategies*, Aldershot: Gower

Garland, D., (2001), *The Culture of Control: Crime and Social Order in Contemporary Society*, Oxford: Oxford University Press

Gehl, R. W., (2014), Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network, *New Media and Society*, 1-17, [15th October, published online before print]

Gellman, B. and Poitras, L., (2013), U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program, *Washington Post*, Friday 7th June, available online at: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, accessed Jun 2013

Giddens, A., (1985), *A Contemporary Critique of Historical Materialism, Vol. 2: The Nation State and Violence*, Cambridge: Polity Press

Giddens, A., (1990), *The Consequences of Modernity*, Cambridge: Polity Press

Gill, M. and Spriggs, A., (2005), *Assessing the Impact of CCTV*, Home Office Research Study 292, London: Home Office Research, Development and Statistics Directorate

Gilliom, D., (2001), *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy*, Chicago, IL: University of Chicago Press

Goode, E. and Ben-Yehuda, N., (1994), *Moral Panics: The Social Construction of Deviance*, Oxford: Blackwell

Google, (2005), Vint Cerf speaks out on net neutrality, *Google Official Blog*, Tuesday 8th November, available online at http://googleblog.blogspot.co.uk/2005/11/vint-cerf-speaks-out-on-net-neutrality.html, accessed Nov 2013

Graber, D., (1976), *Verbal Behaviour and Politics*, Urbana, IL: University of Illinois Press

Graham, M. and Dutton, W. H. (eds.), (2014), *Society and the Internet: How Networks of Information and Communication are Changing our Lives*, Oxford: Oxford University Press

Greenberg, A., (2012), *This Machine Kills Secrets: How WikiLeakers, Cypherpunks and Hacktivists Aim to Free the World's Information*, New York, NY: Dutton

Greenwald, G. and MacAskill, E., (2013), NSA Prism program taps in to user data of Apple, Google and others, *The Guardian*, Friday 6th June, available online at: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, accessed Nov 2014

Greenwald, G., (2013a), NSA collecting phone records of millions of Verizon customers daily, *The Guardian*, Tuesday 6th June, available online at: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, accessed Nov 2014

Greenwald, G., (2013b), XKeyscore: NSA tool collects 'nearly everything on the Internet', *The Guardian*, Wednesday 31st July, available online at: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, accessed Nov 2014

Greenwald, G., MacAskill, E. and Poitras, L., (2013a), Edward Snowden: the whistleblower behind the NSA surveillance revelations, *The Guardian*, Tuesday 11th June, available online at: http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, accessed Nov 2014

Greenwald, G., MacAskill, E., Poitras, L., Ackerman, S. and Rushe, D., (2013b), Microsoft handed the NSA access to encrypted messages, *The Guardian*, Friday 12th July, available online at http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data, accessed Nov 2013

Gunningham, N. and Grabosky, P., (1998), *Smart Regulations: Designing Environmental Policy*, Oxford: Oxford University Press

Gusfield, J. R., (1963), *Symbolic Crusade: Status Politics and the American Temperance Movement*, Urbana, IL: University of Illinois Press

Haggerty, K. and Ericson, R. V., (2000), The Surveillant Assemblage, *The British Journal of Sociology*, 51 (4), 605-622

Haggerty, K., (2006), Tear Down the Walls: On Demolishing the Panopticon, in D. Lyon, (ed.), *Theorizing Surveillance*, Cullompton: Willan Publishing

Hall, E., (2000), *Internet Core Protocols: The Definitive Guide*, Sebastopol, CA: O'Reilly

Hall, S., Critchley, C., Jefferson, T., Clarke, J. and Roberts, B., (1978), *Policing the Crisis*, London: Macmillan

Halliday, J., (2013), Data watchdog fines Sony £250,000 over PlayStation ID hack, *The Guardian*, Thursday 24th January, available at: http://www.theguardian.com/technology/2013/jan/24/sony-fined-over-playstation-hack, accessed May 2014

Hammersley, M., (1996), The Relationship Between Qualitative and Quantitative Research: Paradigm Loyalty versus Methodological Eclecticism, in J. T. E. Richardson, (ed.), *Handbook of Research Methods for Psychology and the Social Sciences*, Leicester: BPS Books

Hammersley, M., (2004), Case Study, in M. S. Lewis-Beck, A. Bryman and T. Futing Liao, *The SAGE Encyclopedia of Social Science Research Methods*, pp.687-682, Thousand Oaks, CA: SAGE Publications

Hanna, P., (2012), Using Internet Technologies (such as Skype) as a Research Medium: A Research Note, *Qualitative Research*, 12 (2), 239-242

Hansard, (2014), *House of Commons Debate*, 2013-14, vol. 576 (127), col. 27WS

Hansen, D. L., Schneiderman, B. and Smith, M. A., (2011), *Analyzing Social Media Networks with NodeXL: Insights from a Connected World*, Burlington, PA: Morgan Kaufmann

Harris, J., (2015), Samsung under fire for recording smart TV voice recognition data, *Digital Spy*, Sunday 8th February, available online at: http://www.digitalspy.co.uk/tech/news/a627497/samsung-under-fire-for-recording-smart-tv-voice-recognition-data.html#~p4JMWqnUm0yeUe, accessed Feb 2015

Hewson, C. M. and Laurent, D., (2008), Research Design and Tools for Internet Research, in R. M. Lee, N. Fielding and G. Blank, (eds.), *The SAGE Handbook of Online Research Methods*, London: SAGE Publications

Hewson, C. M., Yule, P., Laurent, D. and Vogel, C. M., (2003), *Internet Research Methods: A Practical Guide for the Social and Behavioural Sciences*, London: SAGE Publications

Hine, C., (2000), *Virtual Ethnography*, London: SAGE Publications

Hine, C., (2005), *Virtual Methods: Issues in Social Research on the Internet*, London: Bloomsbury Academic

HM Government, (2011), *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, London: The Stationery Office

HM The Queen, (2012), *The Queen's Speech 2012 – Oral Statement to Parliament*, available online at: https://www.gov.uk/government/speeches/the-queen-s-speech-2012, accessed Apr 2014

Hollander, C. and Einwohner, R. L., (2004), Conceptualising Resistance, *Sociological Forum*, 19 (4), 533-554

Holt, A., (2010), Using Telephone for Narrative Interviewing: A Research Note, *Qualitative Research*, 10 (1), 113-121

Home Office, (1994), *CCTV: Looking Out for You*, London: Home Office

Home Office, (2012), *Press Release: Communications Data Bill published*, 14th June, available online at https://www.gov.uk/government/news/communications-data-bill-published--2, accessed Oct 2014

House of Commons, (2012), Great Britain Parliament, *Draft Communications Data Bill*, London: Stationery Office

Housley, W., Procter, R., Edwards, A., Burnap, P., Williams, M., Sloan, L., Rana, O., Morgan, J., Voss, A. and Greenhill, A., (2014), Big and Broad Social Data and the Sociological Imagination: A Collaborative Response, *Big Data and Society*, 1 [online], 1-15

Huey, L., (2010), A Social Movement for Privacy/Against Surveillance? Some Difficulties in Engendering Mass Resistance in a Land of Twitter and Tweets, *Case Western Reserve Journal of International Law*, 42 (3), 681-691

Hutter, B. M. and Lloyd-Bostock, S., (2013), Risk, Interest Groups and the Definition of Crisis: The Case of Volcanic Ash, *The British Journal of Sociology*, 64 (3), 383-404

Hutter, B., (1988), *The Reasonable Arm of the Law?* Oxford: Clarendon Press

Hutter, B., (1997), *Compliance, Regulation and Environment*, Oxford: Clarendon Press

InfoSecurity, (2013), *Snapchat's expired snaps are not deleted, just hidden*, Monday 13th May, available online at http://www.infosecurity-magazine.com/view/32350/snapchats-expired-snaps-are-not-deleted-just-hidden, accessed Nov 2013

Innes, M., (2003), *Understanding Social Control: Deviance, Crime and Social Order*, Maidenhead: Open University Press

Innes, M., (2014), *Signal Crimes: Social Reactions to Crime, Disorder and Control*, Oxford: Oxford University Press

Innes, M. and Levi, M., (2012), Terrorism and Counter-Terrorism, in Maguire, M., Morgan, R. and Reiner, R. (eds.), *The Oxford Handbook of Criminology*, Oxford: Oxford University Press

Instrom Security Consultants, (2014), *Review of CCTV Provision within the Dyfed-Powys Police Area*, Final Report on Behalf of the Dyfed-Powys Police and Crime Commissioner, Newport Pagnell: Instrom Ltd.

Intelligence and Security Committee, (2015), *Privacy and Security: A Modern Transparent Legal Framework*, London: HMSO

Introna, L. and Gibbons, A., (2009), Networks and Resistance: Investigating Online Advocacy Networks as a Modality for Resisting State Surveillance, *Surveillance and Society*, 6 (3), 233-258

Jewkes, Y., (2004), *Media and Crime*, London: Sage

Johnston, L. and Shearing, C., (2003), *Governing Security: Explorations in Policing and Justice*, London: Routledge

Joint Committee on the Draft Communications Data Bill, (2012), *Draft Communications Data Bill: Report, together with appendices and formal minutes*, London: The Stationery Office

Justice, (2011), *Freedom from Suspicion: Surveillance Reform for a Digital Age*, available online at: http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf, accessed Apr 2014

Kemple, T. and Huey, L., (2005), Observing the Observers: Researching Surveillance and Counter-Surveillance on 'Skid Row', *Surveillance and Society*, 3 (2/3), 139-157

Kennedy, J. B., (1926), When Woman is Boss: An Interview with Nikola Tesla, *Colliers*, January 30th, available online at: http://www.tfcbooks.com/tesla/1926-01-30.htm, accessed Dec 2014

King, N. and Horrocks, C., (2010), *Interviews in Qualitative Research*, London: SAGE Publications

Kirkup, J., (2008), Phones tapped at the rate of 1,000 a day, *The Telegraph*, Tuesday 29th January, available online at: http://www.telegraph.co.uk/news/uknews/1576937/Phones-tapped-at-the-rate-of-1000-a-day.html, accessed Apr 2014

Koskela, H., (2004), Webcams, TV shows and mobile phones: Empowering exhibitionism, *Surveillance and Society*, 2 (2/3), 199-215

Kozierok, C. M., (2005), *TCP/IP: A Comprehensive, Illustrated Internet Protocols Reference*, San Francisco, CA: No Starch Press

Latour, B., (1998), *Virtual Society: The Social Science of Electronic Technologies*, paper presented at the CRICT 10th Anniversary Conference, Brunel University

Layder, D., (1993), *New Strategies in Social Research*, Cambridge: Polity Press

Lee, J. H., (2013), Twitter in Pyongyang: how North Korea got the mobile Internet, *The Guardian*, Thursday 28th February, http://www.guardian.co.uk/technology/2013/feb/28/twitter-north-korea-mobile-internet, accessed May 2013

Lee, R. M., Fielding, N. and Blank, G., (2008), The Internet as a Research Medium: An Editorial Introduction to The SAGE Handbook of Online Research Methods, in R. M. Lee, N. Fielding and G. Blank, (eds.), *The SAGE Handbook of Online Research Methods*, London: SAGE Publications

Leetaru, K., (2013), King Snowden and the Fall of WikiLeaks, *Foreign Policy*, Tuesday 31st December, available online at: http://www.foreignpolicy.com/articles/2013/12/31/king_snowden_and_the_fall_of_wikileaks, Aug 2014

Leigh, D. and Harding, L., (2011), *WikiLeaks: Inside Julian Assange's War on Secrecy*, London: Guardian Books

Lessig, L., (1999), *Code and Other Laws of Cyberspace*, New York, NY: Basic Books

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

Lewis, K., (2008), *Tastes, Ties, and Time: Cumulative Codebook*, available online at: http://dvn.iq.harvard.edu/ dvn/dv/t3, accessed Dec 2014

Lewis, K., Kaufman, J., Gonzalez, M., Wimmer, A. and Christakis, N., (2008), Tastes, Ties, and Time: A New Social Network Dataset using Facebook.com, *Social Networks*, 30 (4), 330–342

Loader, B. (ed.), (1997), *The Governance of Cyberspace: Politics, Technology and Global Restructuring*, London: Routledge

Loseke, D., (2003), *Thinking About Social Problems*, 2nd ed., Hawthorne, NY: Aldine de Gruyter

Lyman, P. and Wakeford, N., (1999), Introduction: Going into the (Virtual) Field, *American Behavioural Scientist*, 43 (3), 359-376

Lyon, D., (1994), *The Electronic Eye: The Rise of the Surveillance Society*, Minneapolis, MN: University of Minnesota Press

Lyon, D., (2001), *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press

Lyon, D., (2002), Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix, *Surveillance and Society*, 1 (1), 1-7

Lyon, D., (2003a), Cyberspace, Surveillance and Control, in K. C. Ho, R. Kluver and K. C. C. Yang, (eds.), *Asia.com: Asia Encounters the Internet*, London: RoutledgeCurzon

Lyon, D., (2003b), Surveillance as Social Sorting: Computer Codes and Mobile Bodies, in D. Lyon (ed.), *Surveillance and Social Sorting: Privacy, Risk and Digital Discrimination*, London: Routledge

Lyon, D., (2006), *Theorizing Surveillance: The Panopticon and Beyond*, Cullompton: Willan

Lyon, D., (2007), Surveillance, Security and Social Sorting: Emerging Research Priorities, *International Criminal Justice Review*, 17 (3), 161-170

Lyon, D., (2014), Surveillance, Snowden and Big Data: Capacities, Consequences, Critique, *Big Data and Society*, 1 [online], 1-13

Lysloff, R. T. A., (2003), Musical Community on the Internet: An On-line Ethnography, *Cultural Anthropology*, 18 (2), 233-263

MacAskill, E., Borger, J., Hopkins, N., Davies, N. and Ball, J., (2013), GCHQ taps fibre-optic cables for secret access to world's communications, *The Guardian*, Friday 21st June, available online at: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, accessed Nov 2014

McRobbie, A. and Thornton, S., (1995), Rethinking 'Moral Panic' for Multi-Mediated Social Worlds, *British Journal of Sociology*, 46 (4), 559-574

Machlup, F., (1962), *The Production and Distribution of Knowledge in the United States*, Princeton, NJ: Princeton University Press

Mann, S., Nolan, J. and Wellman, B., (2003), Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments, *Surveillance and Society,* 1 (3), 331-355

Markham, A. and Buchanan, E. (2012), *Ethical Decision Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0)*, available online at: http://aoir.org/reports/ethics2.pdf, accessed Dec 2014

Martin, A. K., van Brakel, R. E. and Bernhard, D. J., (2009), Understanding Resistance to Digital Surveillance: Towards a Multi-Disciplinary, Multi-Actor Framework, *Surveillance and Society*, 6 (3), 213-232

Maruna, S. and Matravers, A., (2007), N=1: Criminology and the Person, *Theoretical Criminology*, 11 (4), 427-442

Marx, G. T., (1988), *Undercover: Police Surveillance in America*, Berkeley, CA: University of California Press

Marx, G. T., (2002), What's New About the 'New Surveillance'?: Classifying for Change and Continuity, *Surveillance and Society*, 1 (1), 9-29

Marx, G. T., (2003), A Tack in the Shoe: Neutralising and Resisting the New Surveillance, *Journal of Social Issues,* 59 (2), 369-390

Marx, G. T., (2009), A Tack in the Shoe and Taking off the Shoe: Neutralisation and Counter-Neutralisation Dynamics, *Surveillance and Society*, 6 (3), 294-306

Mathiesen, T., (1997), The Viewer Society: Michel Foucault's Panopticon Revisited, *Theoretical Criminology*, 1 (2), 215-234

May, T., (2011), *Social Research: Issues, Methods and Process*, 4th ed., Buckingham: Open University Press

McGinn, M. K., (2008), Secondary Data, in L. M. Given, (ed.), *The SAGE Encyclopedia of Qualitative Research Methods*, Thousand Oaks, CA: SAGE Publications

McLaughlin, E. and Muncie, J. (eds.), (2013), *Criminological Perspectives: Essential Readings*, 3rd ed., London: SAGE

McLuhan, M., (1964), *Understanding Media: The Extensions of Man*, New York, NY: McGraw-Hill

McPherson, M., Smith-Lovin, L. and Cook, J., (2001), Birds of a Feather: Homophily in Social Networks, *Annual Review of Sociology*, 27, 415-444

Meyrowitz, J., (1985), *No Sense of Place: The Impact of Electronic Media on Social Behaviour*, Oxford: Oxford University Press

Milan, S., (2013), *Social Movements and Their Technologies: Wiring Social Change*, London: Palgrave Macmillan

Mills, C. W., (1959)*, The Sociological Imagination*, Oxford: Oxford University Press

Molotch, H., (2012), *Against Security: How We Go Wrong at Airports, Subways and Other Sites of Ambiguous Danger*, Princeton, NJ: Princeton University Press

Murakami Wood, D., (2008), Towards Spatial Protocol: The Topologies of the Pervasive Surveillance Society, in A. Aurigi, and F. De Cindio, (eds.), *Augmented Urban Spaces*, Aldershot: Ashgate

Naughton, J., (2013), Why big data has made your privacy a thing of the past, *The Observer*, Sunday 6th October, available online at http://www.theguardian.com/technology/2013/oct/06/big-data-predictive-analytics-privacy, accessed Nov 2013

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), Privacy as Contextual Integrity, *Washington Law Review*, 79 (1), 119–157

Nissenbaum, H., (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford, CA: Stanford University Press

Noaks, L. and Wincup, E., (2004), *Criminological Research*, London: SAGE Publications

Norris, C. and Armstrong, G., (1999), *The Maximum Surveillance Society*, Oxford: Berg

Norris, C., (2003), From Personal to Digital: CCTV, the Panopticon and the Technological Mediation of Surveillance and Control, in D. Lyon (ed.), *Surveillance and Social Sorting: Privacy, Risk and Digital Discrimination*, London: Routledge

Norton-Taylor, R. and Roberts, T., (2009), Councils still breaking surveillance laws, *The Guardian*, Tuesday 21st July available at: http://www.theguardian.com/uk/2009/jul/21/local-authorities-spy-on-public, May 2014

Ó Dochartaigh, N., (2007), *Internet Research Skills*, London: SAGE Publications

O'Connor, H., Madge, C., Shaw, R. and Wellens, J., (2008), Internet-based Interviewing, in R. M. Lee, N. Fielding and G. Blank, (eds.), *The SAGE Handbook of Online Research Methods*, London: SAGE Publications

O'Carroll, L., (2013), Online piracy: ISPs ordered to block access to three file-sharing websites, *The Guardian*, Thursday 28th February, http://www.guardian.co.uk/media/2013/feb/28/online-piracy-isps-block-access, accessed May 2013

Office for National Statistics, (2013), *Internet Access: Households and Individuals 2013*, Statistical Bulletin, available online at: http://www.ons.gov.uk/ons/dcp171778_322713.pdf, accessed Nov 2013

Office for National Statistics, (2015), *Overview of Internet Retail Sales,* available online at: http://webarchive.nationalarchives.gov.uk/20160105160709/http://www.ons.gov.uk/ons/rel/rsi/retail-sales/december-2014/sty-overview-of-internet-retail-sales-in-2014.html, accessed May 2016

Ogura, T., (2006), Electronic government and surveillance-oriented society, in Lyon, D. (ed.), *Theorizing Surveillance: The Panopticon and Beyond*, Cullompton: Willan

Olson, P., (2013), Teenagers say goodbye to Facebook and hello to messenger apps, *The Guardian*, Sunday 10th November, available online at

http://www.theguardian.com/technology/2013/nov/10/teenagers-messenger-apps-facebook-exodus, accessed Nov 2013

Oltermann, P., (2013), Britain accused of trying to impede EU data protection law, *The Guardian*, available online at http://www.theguardian.com/technology/2013/sep/27/britain-eu-data-protection-law, accessed Nov 2013

Open Rights Group, (2012), Communications Data Bill/Draft/Commentary, *Open Rights Group Wiki*, available online at: http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill/Draft/Commentary#Filtering_arrangements_for_acquisition_of_data, Apr 2014

Open Rights Group, (2014), Data Protection Act 1998, *Open Rights Group Wiki*, available online at: https://wiki.openrightsgroup.org/wiki/Data_Protection_Act_1998, Apr 2014

Pew Research Centre, (2012), *Social Networking Popular Across Globe*, Global Attitudes Project, Wednesday 12th December, available online at: http://www.pewglobal.org/files/2012/12/Pew-Global-Attitudes-Project-Technology-Report-FINAL-December-12-2012.pdf, Aug 2014

Pilkington, E., (2013a), Bradley Manning gives evidence to court martial: 10 things to look out for, *The Guardian*, Thursday 28th February, available online at: http://www.guardian.co.uk/world/2013/feb/28/bradley-manning-testifies-10-things, accessed May 2013

Pilkington, E., (2013b), Jailed Anonymous hacker Jeremy Hammond: 'My days of hacking are done', *The Guardian*, Friday 15th January, available online at: http://www.theguardian.com/technology/2013/nov/15/jeremy-hammond-anonymous-hacker-sentenced, accessed Nov 2013

Plant, J., (2013), Anti-social behaviour orders could prove futile in fighting nuisance neighbours, *The Guardian*, Wednesday 20th February, http://www.guardian.co.uk/housing-network/2013/feb/20/antisocial-behaviour-laws-nuisance-neighbours, accessed May 2013

Porat, M. U., (1977), *The Information Economy: Definition and Measurement*, The Office of Telecommunications Special Publications, Washington D.C.: Government Printing Office

Poster, M., (1990), *The Mode of Information: Poststructuralism and Social Context*. Chicago, IL: University of Chicago Press.

Poster, M., (1996), Databases as discourse; or, Electronic interpellations, in Lyon, D. and Zureik, E. (eds.), *Computers, Surveillance, and Privacy*. Minneapolis, MN: University of Minnesota Press

Powles, J., (2014), UK's Drip law: cynical, misleading and an affront to democracy, *The Guardian*, Friday 18th July, available at: http://www.theguardian.com/technology/2014/jul/18/uk-drip-ripa-law-sceptical-misleading-democracy-martha-lane-fox, accessed Oct 2014

Prince, R., (2008), Jacqui Smith plans broad new 'Big Brother' surveillance powers, *Daily Telegraph*, Wednesday 15th October, available online at: http://www.telegraph.co.uk/news/politics/3202766/Jacqui-Smith-plans-broad-new-Big-Brother-surveillance-powers.html, accessed Apr 2014

Procter, R., Vis, F. and Voss, A., (2013), Reading the Riots on Twitter: Methodological Innovation for the Analysis of Big Data, *International Journal of Social Research Methodology*, 16 (3), 197-214

Raby, C., (2005), What is Resistance? *Journal of Youth Studies*, 8(2), 151-171

Riley-Smith, B., (2015), Too many useless and ineffective CCTV cameras in Britain, says surveillance commissioner, *The Telegraph*, Monday 26th January, available online at: http://www.telegraph.co.uk/news/politics/11369485/Too-many-useless-and-ineffective-CCTV-cameras-in-Britain-says-surveillance-commissioner.html, accessed Jan 2015

Robins, K. and Webster, F., (1999), *Times of the Technoculture*, New York, NY: Routledge

Rogers, R., (2009), *The End of the Virtual: Digital Methods*, Amsterdam: University of Amsterdam Press

Ruhleder, K., (2000), The Virtual Ethnographer: Fieldwork in Distributed Electronic Environments, *Field Methods*, 12 (1), 3-17

Royal United Services Institute, (2015), *A Democratic License to Operate: Report of the Independent Surveillance Review*, London: Stephen Austin and Sons

Sanchez, A., (2009), Facebook Feeding Frenzy: Resistance-through-Distance and Resistance-through-Persistence in the Societied Network, *Surveillance and Society*, 6 (3), 275-293

Savage, M. and Burrows, R., (2007), The Coming Crisis of Empirical Sociology, *Sociology*, 41 (5), 885-899

Save the Internet, (2015), *Net Neutrality*, available online at: http://www.savetheinternet.com/net-neutrality, accessed Dec 2014

Schneier, B., (2014), NSA robots are 'collecting' your data, too, and they're getting away with it, *The Guardian*, 27th February, availabl online at: http://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier, accessed Mar 2014

Schulz, W., (2008), Content Analyses and Public Opinion Research, in W. Donsbach and M. W. Traugott, *The SAGE Handbook of Public Opinion Research*, London: SAGE Publications

Scott, J., (1990), *A Matter of Record*, Cambridge: Polity Press

Scott, J., (2004), Types of Documents, in M. S. Lewis-Beck, A. Bryman and T. Futing Liao, *The SAGE Encyclopedia of Social Science Research Methods*, pp.687-682, Thousand Oaks, CA: SAGE Publications

Sedgwick, M. and Spiers, J., (2009), The Use of Videoconferencing as a Medium for the Qualitative Interview, *International Journal of Qualitative Methods*, 8 (1), 1-11

Sharp, J. P., Routledge, P., Philo, C. and Paddison, R. (eds.), (2000), *Entanglements of Power: Geographies of Domination and Resistance*, London: Routledge

Shaw, C., (1930/1966), *The Jack-Roller: A Delinquent Boy's Own Story*, Chicago, IL: University of Chicago Press

Shearing, C. and Stenning, P., (1981), Modern Private Security: Its Growth and Implications, *Crime and Justice*, 3, 193-245

Shearing, C. and Stenning, P., (1983), Private Security: Its Implications for Social Control, *Social Problems*, 30, 125-138

Shearing, C. and Stenning, P., (1985), From the Panopticon to Disney World: The Development of Discipline, in A. Doob and E. Greenspan (eds.), *Perspectives in Criminal Law*, Toronto, ON: Canada Law Books

Shearing, C. and Wood, J., (2003), Nodal Governance, Democracy and the New 'Denizens', *Journal of Law and Society*, 30 (3), 400-419

Shih, F. -J., (1998), Triangulation in Nursing Research, *Journal of Advanced Nursing*, 28, 631-641

Shirky, C., (2011), WikiLeaks has created a new media landscape, *The Guardian*, Friday 4th February, available online at: www.theguardian.com/commentisfree/2011/feb/04/wikileaks-created-new-media-landscape, accessed May 2012

Sloan, L., Morgan, J., Housley, W., Williams, M. L., Edwards, A., Burnap, P. and Rana, O., (2013), Knowing the Tweeters: Deriving Sociological Relevant Demographics from Twitter, *Sociological Research Online*, 18 (3)

Solove, D., (2007a), 'I've got Nothing to Hide' and Other Misunderstandings of Privacy, *San Diego Law Review*, 44, 745-772

Solove, D., (2007b), *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, New Haven, CT: Yale University Press

Spy Blog, (2013), *An Accessible Version of the Draft Anti-Social Behaviour Bill*, http://spyblog.org.uk/, accessed May 2013

Stenning, P. C., (2000), Powers and Accountability of Private Police, *European Journal on Criminal Policy and Research*, 8 (3), 325-352

Tarrow, S., (1998), *Power in Movement: Social Movements and Contentious Politics*, Cambridge: Cambridge University Press

Taylor, P., (2001), Hacktivism: In Search of Lost Ethics?, in D. S. Wall (ed.), *Crime and the Internet*, London: Routledge

Thelwall, M. and Stuart, D., (2006), Web Crawling Ethics Revisited: Cost, Privacy and Denial of Service, *Journal of the American Society for Information, Science and Technology*, 57 (13), 1771-1779

Toffler, A., (1980), *The Third Wave*, New York, NY: Bantam Books

Trottier, D., (2012), *Social Media as Surveillance: Rethinking Visibility in a Converging World*, Farnham: Ashgate

Turk, A., (1982), Social Control and Social Conflict, in J. Gibbs (ed.), *Social Control*, Beverley Hills, CA: Sage

Twitter, (2012), Twitter turns six, *Twitter Blog*, Wednesday 21st March, available online at: https://blog.twitter.com/2012/twitter-turns-six, accessed Sep 2014

Twitter, (2013), *About Twitter, Inc.*, available online at: https://about.twitter.com/company, accessed Nov 2013

Vandekerckhove, W., (2006), Whistleblowing and Organizational Social Responsibility: A Global Assessment, Aldershot: Ashgate

Vogel, D., (2012), *The Politics of Precaution: Regulating Health, Safety and Environmental Risks in Europe and the United States*, Princeton, NJ: Princeton University Press

Wakefield, J., (2013), Experts warn on wire-tapping of the cloud, *BBC News*, Thursday 31st January, available online at: http://www.bbc.co.uk/news/technology-21263321, accessed May 2013

Walker, P., (2011), Amnesty International hails WikiLeaks and Guardian as 'Arab Spring' catalysts, *The Guardian*, Friday 13th May, available online at: http://www.theguardian.com/world/2011/may/13/amnesty-international-wikileaks-arab-spring, accessed Jun 2014

Wall, D. S. (ed.), (2001), *Crime and the Internet*, London: Routledge

Wall, D. S., (1998), Policing and the Regulation of Cyberspace, *The Criminal Law Review*, Special Edition on Crime, Criminal Justice and the Internet, 77-91

Watt, N., Mason, R. and Traynor, I., (2015), David Cameron pledges anti-terror law for Internet after Paris attacks, *The Guardian*, Monday 12th January, available online at: http://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg, accessed Jan 2015

Webster, F., (1995), *Theories of the Information Society*, London: Routledge

Webster, F., (2014), *Theories of the Information Society*, (4th ed.), London: Routledge

Wells, H. and Wills, D., (2009), Individualism and Identity: Resistance to Speed Cameras in the UK, 6 (3), 259-274

WikiLeaks, (2013), *Secret US Embassy Cables*, available online at: https://wikileaks.org/cablegate.html, Jun 2014

WikiLeaks, (2014), *The Global Intelligence Files*, available online at: https://wikileaks.org/gifiles/, Jun 2014

WikiLeaks: Secrets and Lies, (2011), Channel 4, Tuesday 29th November, 22:00, available online at: http://www.channel4.com/programmes/wikileaks-secrets-and-lies

Williams, M., (2006), *Virtually Criminal: Crime, Deviance and Regulation Online*, Abingdon: Routledge

Willig, C., (2014), Discourse and Discourse Analysis, in U. Flick, *The SAGE Handbook of Qualitative Data Analysis*, London: SAGE Publications

Wood, J. and Shearing, C., (2007), *Imagining Security*, Cullompton: Willan

Yin, R. K., (1984), *Case Study Research: Design and Methods*, Beverly Hills, CA: SAGE Publications

Young, J., (1971), *The Drug Takers: The Social Meaning of Drug Taking*, London: Paladin

Zimmer, M., (2006), More on Facebook and the Contextual Integrity of Personal Information Flows, *michaelzimmer.org*, available online at: http://michaelzimmer.org/2006/09/08/more-on-facebook-and-the-contextual-integrity-of-personal-information- flows, accessed Dec 2014

Zimmer, M., (2010), 'But the Data is Already Public': On the Ethics of Research in Facebook, *Ethics Information and Technology*, 12 (4), 313-325

Zittrain, J., (2003), Internet Points of Control, *Boston College Law Review*, 44, 653-688

Zwitter, A., (2014), Big Data Ethics, *Big Data and Society*, 1 [online], 1-6

APPENDICES

APPENDIX A: THE ARCHITECTURE OF THE INTERNET

TCP/IP

Prior to the emergence of the World Wide Web, new standards in inter-network operability had been created, permitting more reliable and efficient communication across the Internet. In 1983, Vint Cerf and Robert E. Kahn's Transmission Control Protocol (TCP) and Internet Protocol (IP), commonly known as TCP/IP, were formally adopted by ARPANet. This protocol suite remains central to Internet communication. Its relevance to this discussion and to this research is that it establishes non-hierarchical relationships between any two Internet hosts (computers). As Hall (2000: 407) observes, 'IP uses an anarchic and highly distributed model, with every device being an equal peer to every other device on the global Internet.' This radical approach to connectivity is a key part of the foundation for many Internet activists' beliefs in freedom of communication and the ethos behind much of the development of the Internet and World Wide Web. However, TCP/IP is only one of two systems that govern access to the Internet and the Web. Galloway's (2004) exploration of protocol rests on the observation that while TCP/IP 'radically distributes control into autonomous locales' a second system, the Domain Name System (DNS) 'focuses control into rigidly defined hierarchies' (2004: 142).

DNS

Invented by Paul Mockapetris in 1983, DNS was a response to the problems of demand presented by a *centralised* system of recording all Internet addresses. It also overcame the problem of having to remember the numerical address (IP address) of a computer on the network, replacing these with more memorable names such as 'cardiff.ac.uk'. DNS is *decentralised* and it delegates authority for domain names on the Internet to separate servers based in different locations around the world. DNS is hierarchical; control over access to webpages is delegated. At the top are a handful of 'root' servers, mostly located in the United States. At the

next level are servers for the various domains such as 'com', 'org' and 'uk'. These are followed by servers with authority at each level over each respective part of a domain name. Removing a website from the Internet, for instance for censorship purposes, is therefore as simple as removing it from the indexing system of DNS; if the authoritative server cannot provide the IP address, the site cannot be accessed. For this reason, Berners-Lee has called DNS 'the one centralized Achilles' heel' by which the Web can be brought down or controlled' (1999: 126).

TCP/IP and DNS are at the heart of Internet operability. These dual systems and the philosophies they support connect with key ideas in the thesis regarding the negotiation of control, centralisation and decentralisation and the promotion of different values and forms of social order. Just as it allows for both surveillance and resistance, the regulation of the Internet allows for restrictive and liberating forms of communication.

The protocols that govern the Web originate from documents known as Requests for Comments (RFCs) produced by the Internet Engineering Task Force (IETF). All RFCs strive to achieve standardisation and organisation, regardless of whether the proposed protocol enables a radical open sharing of information, like with TCP/IP, or a hierarchical structuration like the DNS. However, the organisations responsible for governing the creation of protocols – for instance the Internet Corporation for Assigned Names and Numbers (ICANN), which manages DNS – are highly bureaucratic and centralised. Exemplifying this, several of the RFCs are concerned with laying out what RFCs constitute or how the IETF operates, and so on.

Wil Chivers

1-3 Museum Place

Cardiff University

Cardiff CF10 3BT

Email: ChiversWG1@cardiff.ac.uk

INFORMATION FOR RESEARCH PARTICIPANTS

I would like to invite you take part in a research study on surveillance, resistance and the Internet. Before you decide it is important you understand why the research is being done and what is involved in your participation. The following will hopefully address any queries you may have, so please read the information provided carefully.

Who am I?

My name is Wil Chivers and I am a third year PhD student in the School of Social Sciences (SOCSI) at Cardiff University. My research is funded by the Economic and Social Research Council (ESRC). My postgraduate researcher profile for Cardiff University can be accessed at the following web address:

http://www.cardiff.ac.uk/socsi/contactsandpeople/postgraduateresearchers/chivers-overview.html

I am supervised by Professor Martin Innes and Dr Matthew Williams, also from SOCSI. You can find links to their profiles via the web address above.

What is my research about?

My research is primarily concerned with the following areas:

- Individual and collective forms of resistance.
- New forms of surveillance enabled/facilitated by the Internet.
- How resistance occurs in online environments – what is it about the Internet that offers specific opportunities for resistance? How is surveillance shaped as a problem?

- The interaction between resistance and surveillance in online environments.
- The role of social media in this relationship.

The research study has received the approval of the School Research Ethics Committee (SREC).

What will the interview involve?

I would like to conduct interviews with people who have particular expertise or knowledge of the issues I am investigating. I anticipate that the interviews should last between 30 minutes and one hour. If you consent, interviews will be recorded so I have a record of what was said. Similarly, if you consent, I may contact you again by a method of your choosing to ask for clarification of some points.

What happens to the interview data?

The interviews will be confidential. I may, however, ask your permission to identify you in my research although this is entirely up to you and if you decline to be identified your responses will be anonymised. Interview transcripts will only be viewed by my supervisors and me. They will be kept in accordance with university data protection regulations. An analysis of the interviews will form part of my PhD thesis and may also be published in academic journals or books.

What if you decide to withdraw from the research?

Your participation in this study is entirely voluntary; you are therefore free to withdraw at any point without giving reason. Any data will be erased and you will not be identified in the research.

What if you have further questions or concerns?

Please feel free to contact me with any questions or concerns you have about my research, either before the interview or after. Should you decide at a later date that you do not want your responses to be included in my research, please do not hesitate to contact me at the email address above. If you would like to contact my supervisors, you will find their contact details as described above.

Thank you.

CONSENT FORM FOR RESEARCH PARTICIPANTS

- ☐ I confirm that I have read and understood the information sheet for the above study. I have had the opportunity to consider the information.

- ☐ I am willing to take part in an interview for this research and I am happy for this interview to be recorded.

- ☐ I am happy to be contacted by the researcher following the interview, should it be necessary.

- ☐ I understand that the interviews are confidential and that no one will have access to the recording or transcription with the exception of the researcher and his two supervisors.

- ☐ I understand that my participation is voluntary and that I am free at any point to withdraw if I should wish, without giving a reason.

*Anonymity (please tick **one**):*

- ☐ I am happy to be identified in the research.
- ☐ I am happy to be identified in the research, provided I am contacted prior to inclusion of any direct quotations.
- ☐ I would like to remain anonymous.

Name of respondent:……

Signature of respondent:……

Contact email:……

Date:……

APPENDIX C: NETWORK ANALYSIS DATA

ISSUE CRAWLER

Results of initial crawl: 55 organisations

www.cdt.org
www.creativecommons.org
www.publicknowledge.org
www.icann.org
www.democraticmedia.org
www.eff.org
www.fas.org
www.hrw.org
www.aclu.org
www.eff.org
www.effi.org
www.cpsr.org
www.gnu.org
www.gilc.org
www.epic.org
www.privacyrights.org
www.privacy.org
www.privacyinternational.org
www.edri.org
www.iris.sgdg.org
www.fipr.org
www.statewatch.org
www.efa.org.au
www.againstinternetsurveillance.org
www.no-cctv.org.uk
www.no2id.net
www.openrightsgroup.org
www.liberty-human-rights.org
www.indexoncensorship.org
www.justice.org.uk
www.cyber.law.harvard.edu
www.digitalrights.dk
www.mediasmarts.ca
www.digitalrights.ie
www.article19.org
www.accessreports.com
www.bigbrotherawards.org
www.bof.nl
www.cfoi.org.uk
www.cryptome.org
www.wikileaks.org
www.cyber-rights.org
www.freedominfo.org
www.gnupg.org
www.ifea.net
www.indymedia.org
www.internetsociety.org
www.jamesmadisonproject.org
www.nocards.org
www.privacyactivism.org
www.pogo.org
www.privacyjournal.net
www.realnightmare.org
www.spychips.com
www.tor.eff.org
www.wiki.vorratsdatenspeicherung.de

Ten starting points distilled from these:

http://www.aclu.org
http://www.bigbrotherwatch.org
http://www.edri.org
http://www.eff.org
http://www.epic.org
http://www.liberty-human-rights.org.uk
http://www.no2id.net
http://www.openrightsgroup.org
http://www.privacyinternational
http://www.statewatch.org

Example of network results from crawl on 4th January 2013

Title: Privacy Advocates (Core Actors) 329424
Crawl start: 2013-01-04 02:04:43
Crawl end: 2013-01-04 04:51:27

Rank	pRank	Rank chan	Actor	Inlinks	Inlink change
1	1	stable	twitter.com	1431	-736
2	3	1	creativecommons.org	1140	5
3	10	7	edri.org	827	466
4	-	n/a	fsf.org	643	643
5	7	2	cyber.law.harvard.edu	521	24
6	6	stable	soros.org	514	16
7	-	n/a	gnu.org	480	480
8	9	1	writetothem.com	462	-4
9	5	-4	gnso.icann.org	389	-118
10	11	1	gilc.org	266	-15
11	12	1	ec.europa.eu	260	2
12	84	72	parliament.uk	240	235
13	14	1	bbc.co.uk	235	13
14	13	-1	ccc.de	233	-2
15	15	stable	foebud.org	210	-4
16	16	stable	fiff.de	209	-2
17	17	stable	bigbrotherawards.ch	202	-2
18	18	stable	no2id.net	120	7
19	19	stable	privacyinternational.org	108	stable
20	20	stable	eff.org	100	6
21	-	n/a	intgovforum.org	86	86
22	21	-1	epic.org	83	7
23	22	-1	bigbrotherawards.de	63	-2
24	39	15	fsfe.org	58	30
25	23	-2	homeoffice.gov.uk	49	-6
26	32	6	cdt.org	46	10
27	25	-2	ffii.org	46	2
28	24	-4	aclu.org	44	-1
29	26	-3	theyworkforyou.com	43	stable
30	27	-3	europa.eu	41	stable
31	29	-2	efa.org.au	41	1
32	28	-4	fitug.de	41	stable
33	31	-2	aboutcookies.org	37	stable
34	30	-4	ico.gov.uk	36	-3
35	33	-2	fipr.org	35	1
36	34	-2	iris.sgdg.org	33	stable
37	36	-1	facebook.com	31	2
38	35	-3	statewatch.org	31	-1
39	43	4	hmrc.gov.uk	29	3
40	38	-2	vibe.at	29	stable
41	37	-4	icann.org	28	-1
42	40	-2	liberty-human-rights.org.uk	27	-1
43	41	-2	effi.org	26	stable
44	42	-2	openrightsgroup.org	26	stable
45	44	-1	bof.nl	25	stable

46	56	**10**	guardian.co.uk	22		7
47	46	**-1**	vorratsdatenspeicherung.de	21		-1
48	-	**n/a**	ftc.gov	20		20
49	48	**-1**	eurodig.org	19	stable	
50	49	**-1**	digitalrights.dk	19	stable	
51	47	**-4**	hrw.org	18		-2
52	51	**-1**	alcei.it	18	stable	
53	50	**-3**	dataretentionisnosolution.com	17		-1
54	53	**-1**	tacd.org	16		-1
55	55	**stable**	ael.be	16	stable	
56	54	**-2**	eur-lex.europa.eu	14		-2
57	57	**stable**	internautas.org	13	stable	
58	52	**-6**	article19.org	12		-5
59	58	**-1**	en.wikipedia.org	11		-1
60	59	**-1**	publicknowledge.org	11		-1
61	60	**-1**	itu.int	10	stable	
62	62	**stable**	quintessenz.org	10	stable	
63	67	**4**	globalvoicesonline.org	9		1
64	64	**stable**	justice.gov.uk	9	stable	
65	65	**stable**	education.gov.uk	9	stable	
66	61	**-5**	bis.gov.uk	9		-1
67	77	**10**	beuc.org	8		1
68	69	**1**	freedom-not-fear.eu	8	stable	
69	66	**-3**	flickr.com	7		-1
70	70	**stable**	bloglines.com	7	stable	
71	72	**1**	laquadrature.net	7	stable	
72	73	**1**	privacyrights.org	7	stable	
73	75	**2**	i-cams.org	7	stable	
74	76	**2**	ipjustice.org	7	stable	
75	68	**-7**	cfoi.org.uk	7		-1
76	78	**2**	internetforum.fi	7	stable	
77	79	**2**	nnm-ev.de	7	stable	
78	80	**2**	oecd.org	6	stable	
79	83	**4**	eisionline.org	6	stable	
80	-	**n/a**	mpaa.org	6		6
81	71	**-10**	gn.apc.org	6		-1
82	81	**-1**	state.gov	5		-1
83	85	**2**	archive.org	5	stable	
84	86	**2**	bigbrotherwatch.org.uk	5	stable	
85	87	**2**	wiki.dataretentionisnosolution.com	5	stable	
86	88	**2**	archrights.org.uk	5	stable	
87	89	**2**	biduk.org	5	stable	
88	63	**-25**	get.adobe.com	4		-5
89	-	**n/a**	apple.com	3		3
90	-	**n/a**	europarl.eu.int	3		3
91	90	**-1**	ifj.org	3		-1
92	91	**-1**	identitytheft.org.uk	3	stable	
93	-	**n/a**	edps.eu.int	3		3
94	-	**n/a**	internews.org	3		3

Top 64 network actors by in-degree (followers) – those with 100+ followers

	Twitter Name	Description	In-Degree	Out-Degree	Bet. Centrality
1	no2id	PrivAdv	1731	538	2198435.244
2	wikileaks	Journ Activ	665	0	127766.158
3	privateeyenews	Media/Satire	560	0	71418.439
4	policestateuk	Priv/Civ Lib Adv	559	36	79873.592
5	guidofawkes	Pol Blog	474	0	48879.592
6	openrightsgroup	Dig Rights Adv	460	164	60197.297
7	bbcr4today	Media	447	110	47519.378
8	guardiannews	Media	440	29	45535.858
9	bbw1984	PrivAdv	432	45	47851.631
10	carolinelucas	MP (Green)	411	27	33825.953
11	privacyint	Priv Adv	367	46	31892.366
12	mayoroflondon	BoJo	364	57	30517.641
13	jackofkent	Journ/Blog	358	45	25042.590
14	paullewis	Journ (Civ Lib)	333	23	20717.742
15	libcon	Left Activ	325	0	18095.597
16	thegreenparty	Pol Party	314	179	24276.884
17	guardiantech	Journ (Tech)	309	36	26723.962
18	unlockdemocracy	Democ Adv	306	272	18442.150
19	newsbrooke	Journ/Auth	296	37	15245.965
20	conservatives	Pol Party	278	256	17649.424
21	grantshapps	MP (Tory)	248	88	9225.698
22	copwatcher	Police Activist	247	36	11776.274
23	libertycentral	Journ (Civ Lib)	246	27	11941.733
24	yougov	Research	246	9	9037.130
25	old_holborn	Pol Blog	231	53	10630.821
26	twitpic	Social media	229	7	12908.728
27	vincecable	MP (Lib)	224	117	10068.707
28	libdemvoice	Pol website	208	47	5921.493
29	julianhuppert	MP (Lib)	201	11	5719.165
30	politics_co_uk	Media/Pol	200	41	5808.594
31	electoralreform	Democ Adv	186	144	6845.543
32	noaheverett	Founder TwitPic	170	1	6310.823
33	wallaceme	Campaigner	168	50	3241.601

		Blogger			
34	redpeppermag	Journ (Left Politics)	165	20	4675.738
35	markpack	Co-Editor LibDem Voice	160	46	2570.876
36	compassoffice	Democracy Advocate	153	134	4708.526
37	lossofprivacy	Priv/Civ Lib Advocate	138	25	4835.510
38	spyblog	Priv Adv	133	45	3702.296
39	boycottworkfare	Unpaid labour Adv	133	16	3615.642
40	republicstaff	Republic Campaign	125	45	3652.688
41	iconews	ICO	125	42	3412.424
42	aaronjohnpeters	Soc Move's, Deomcracy	124	60	2680.744
43	igeldard	CivLib Security Blogger	123	154	4539.463
44	mattwardman	Politic blog	122	90	2714.981
45	_nomap	Priv and ID researcher	121	25	2131.886
46	soclibforum	Forum	121	102	1629.673
47	lordbonkers	LibDem Blog and satire	121	65	1587.547
48	stevebakermp	MP (Tory)	120	40	1989.797
49	jimkillock	ExecDir ORG	118	73	2721.857
50	markjlittlewood	IEA Director	115	31	1631.948
51	jamesgraham	UnlockDemoc worker	113	56	1280.292
52	jonathanfryer	LibDem politician	112	128	1581.476
53	bridgetfox	LibDem campaigner	111	86	1574.465
54	no2id_groups	Priv Adv	109	93	4644.502
55	tbij	Inv Journo	109	35	2262.456
56	olivercooper	Journo	109	77	1676.979
57	mingyeow	Blogger	105	0	2903.202
58	ajcdeane	Tory Former Dir BBW	105	63	1765.541
59	hmpbritain	Civ Lib Adv	105	16	1750.513
60	matthew_elliott	Chief Exec TPA & BBW	105	21	984.752
61	cllrdaisybenson	LibDem councillor	104	87	1211.403

62	onmodernliberty	Civ Libs	102	95	3513.290
63	consfuture	Pol Party Youth Wing	102	112	1477.323
64	helenduffett	Comms Manager LibDem	102	15	689.724

Top 30 Actors ranked by Betweenness centrality: *(red/green indicates change up/down inrankings)*

Prev	Curr	Twitter Name	Role	Bet. Centrality	In-Degree	Out-Degree
1	1	no2id		2198435.244	1731	538
2	2	wikileaks		127766.158	665	0
4	3	policestateuk		79873.592	559	36
3	4	privateeyenews		71418.439	560	0
6	5	openrightsgroup		60197.297	460	164
5	6	guidofawkes		48879.592	474	0
9	7	bbw1984		47851.631	432	45
7	8	bbcr4today		47519.378	447	110
8	9	guardiannews		45535.858	440	29
10	10	carolinelucas		33825.953	411	27
11	11	privacyint		31892.366	367	46
12	12	mayoroflondon		30517.641	364	57
17	13	guardiantech		26723.962	309	36
13	14	jackofkent		25042.590	358	45
16	15	thegreenparty		24276.884	314	179
14	16	paullewis		20717.742	333	23
18	17	unlockdemocracy		18442.150	306	272
15	18	libcon		18095.597	325	0
20	19	conservatives		17649.424	278	256
19	20	newsbrooke		15245.965	296	37
26	21	twitpic		12908.728	229	7
23	22	libertycentral		11941.733	246	27
22	23	copwatcher		11776.274	247	36
25	24	old_holborn		10630.821	231	53
27	25	vincecable		10068.707	224	117
21	26	grantshapps		9225.698	248	88
24	27	yougov		9037.130	246	9
31	28	electoralreform		6845.543	186	144
32	29	noaheverett		6310.823	170	1
28	30	libdemvoice		5921.493	208	47
30	31	politics_co_uk		5808.594	200	41

Hi Daniel,

Here is the information sheet for my research if you would like to have a look over it - there are some points at the bottom by way of a consent form which can verbally agreed when we chat.

Thanks,

Wil

****
Wil Chivers
PhD Student (SOCSI)
Cardiff University
1-3 Museum Place
Cardiff
CF10 3BD
ChiversWG1@cardiff.ac.uk

On 16 Oct 2012, at 12:58, daniel domscheit-berg wrote:

> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
>
> Hi Wil,
>
> Friday 1100 sounds great. I assume that's UK time, so I should be one
> hour ahead of that?
>
> Skype is fine also, can install it. My handle is domscheitberg
>
> All the best
>
> daniel
>
> On 10/16/12 1:49 PM, William Chivers wrote:
>> Hi Daniel,
>>
>> Not to worry about the delay - thanks very much for responding again,
>> I appreciate it. I hope the technical issues get resolved soon for
>> you!
>>
>> Friday would be good for me to talk if that suits you. Shall we say

>> about 11:00? How is best for you - do you use Skype? Or would you
>> prefer another means?
>>
>> Best,
>>
>> Wil
>>
>> ********** Wil Chivers PhD Student (SOCSI) Cardiff University 1-3
>> Museum Place Cardiff CF10 3BD
>>
>>
>>
>> -----daniel domscheit-berg <daniel@domscheit-berg.de> wrote: -----
>> To: ChiversWG1@cardiff.ac.uk From: daniel domscheit-berg
>> <daniel@domscheit-berg.de> Date: 10/16/2012 12:38PM Subject:
>> touching base
>>
>> Hi Wil,
>>
>> so sorry for not getting back any earlier. We are having some DNS
>> issues right now, meaning I have no access to my mail, and it will
>> take a few more days until fixed. In that sense thanks for contacting
>> Anke and providing her with your contact.
>>
>> If you want, to make this story short, we can speak this week, either
>> Thursday or Friday. I would be available all day, whenever it suits
>> you.
>>
>> All the best
>>
>> daniel
>
> - --
> daniel domscheit-berg
> daniel@domscheit-berg.de
> -----BEGIN PGP SIGNATURE-----
> Version: GnuPG/MacGPG2 v2.0.18 (Darwin)
> Comment: GPGTools - http://gpgtools.org
>
> iQIcBAEBAgAGBQJQfUvNAAoJEB1wUXUsz/8XxTcP/025vuifKArvWch6pJfRs5BH
> upfFSAy8K5+gFhvUIkzvg9rDSSKQ7/5eQjaO+Eyi+JE7Ic/dFtS0OSkgbDswPKn/
> Lx18NEQ6eHvvESG8RoCyCxtYYwjGTwwpqcBwPmjuVjTbc0GT8u4hl/exbZzJFMVP
> puwIQqNqHRRfm2ykhTlirP3uADpVW2XDP3MXiC+nN3wfvak2FG8JwFMqpiLX7234
> viFtWTJqP4tbbHMZpslwyJgZQHJZODeYmqOcsLOIrsIuV2EdAEfjX+RHrvZF2WRV
> mgQKfFxfqAqbbfySegGA5XlH2mdgPhCGWwkSr+f2BwFo1/MITyAM5sncmIqyiCvZ
> q8M1Ze+rSE2/tldSux4fe96H1XCkNWpgohzuDZQi8MnZt+FcI7dKZA9cPtkwjygc
> ac5il3HviX5/jV63LOi5Gh2HaJNhuZ60+r5bHjR73S4bgSFkzM3Fz+eu0QfDIoLT
>
LAzn6O60ZphVWnRRvdpdmbVv9Vjr5uLVV6pMYe5NEUppOwGvegMubf8K43eXfysY
> sEjxW1QYupa6781vA026eGGgCITjo8Tj8T6LivCCtXcS9CjAKzrTUca/5ruCtcoD

> AVYUstm0zDtnz4MuYZhusSk7E2VeAdUrPVgFL5AomS3WtV9kYWpUvIAhJJrn7SXP
> YrJhx7JIJp3aYmg318jv
> =lq1A
> -----END PGP SIGNATURE-----

Hi Daniel,

Thanks for getting back to me. The 5th is fine for me - shall we say midday? I am free all day however if there is another time more suitable for you.

My Skype name is wilchivs if you would like to chat via Skype, or alternatively I will add you if you want to pass on your contact details.

All the best for your trip.

Wil

****

Wil Chivers

PhD Student (SOCSI)

Cardiff University

1-3 Museum Place

Cardiff

CF10 3BD

ChiversWG1@cardiff.ac.uk

On 24 Sep 2012, at 11:13, daniel domscheit-berg wrote:

Hi Wil,

sorry for missing out on you last time. I will leave or Norway and Sweden on

Wednesday, and will be back on the 5th. Does the 5th work for you?

Best
daniel

On Mon, Sep 17, 2012 at 01:04:02PM +0100, William Chivers wrote:

Hello Daniel

Sorry to keep bombarding your inbox but I thought I would follow up our discussion about my PhD research as it would be really useful to hear your thoughts on the issues I am investigating and to learn more about OpenLeaks.

If you are still interested, is there a time over the next two weeks that you would be free to chat? The only day I am unavailable is this Thursday as I am attending a conference but any other time would be great. Do you use Skype? If not is there a chat room you use where we could talk?

Hope to hear from you soon, best wishes,

Wil

****

Wil Chivers

PhD Student (SOCSI)

Cardiff University

1-3 Museum Place

Cardiff

CF10 3BD

-----daniel domscheit-berg <ddb@openleaks.org> wrote: -----

To: Wil Chivers <chiverswg1@cf.ac.uk>

From: daniel domscheit-berg <ddb@openleaks.org>

Date: 08/22/2012 12:57PM

Subject: Re: Cardiff University PhD Research

Hi Wil,

thanks for getting in touch, and sorry for not replying any earlier. that must have slipped my attention.

i am more than happy to help out -- either by chat or mail. as you think is best. what timeframe are you looking at?

best

daniel

On Wed, Aug 22, 2012 at 10:54:58AM +0100, Wil Chivers wrote:

Dear Mr Domscheit-Berg,

I recently contacted OpenLeaks regarding PhD research I am carrying out at the School of Social Sciences at Cardiff University. I received a couple of helpful responses from Max, who offered some of his thoughts on the brief outline of my research that I provided. He also said that he forwarded my original email to you; my intention was to find out if there was a possibility that I could interview you as part of my research.

I realise you must be very busy and I hope you will excuse my following up the original email. I am however very interested in speaking to you about some of the topics that I am investigating, namely online forms of resistance, the relationship

between collective action and state power in this environment and the role of social media in both of these.

If you are able to spare any time for an interview I would be very grateful. I think electronic communication would likely be the most sensible option if so given our respective locations - either via email or chat perhaps? As I discussed with Max, I am not (yet) au fait with encrypted communication via email and the like but if there is a method of communication you would prefer to maximise privacy I am certain we would be able to do that.

I look forward to hearing from you.

Kind regards,

Wil Chivers

****

Wil Chivers

PhD Student (SOCSI)

Cardiff University

1-3 Museum Place

Cardiff

CF10 3BD

ChiversWG1@cardiff.ac.uk

[attachment "atty8hch.dat" removed by William Chivers/ssowgc/CardiffUniversity]

22nd August

Hi Daniel,

Thanks for the response, great to hear you are available to help out - thank you very much.

I am currently formulating interview schedules and need to run them by my supervisors next week. Would it be OK to get back in contact with you once I have done this? I would anticipate doing interviews in a few weeks time - mid-September perhaps, is this suitable for you? I will also be able to send you an information sheet via email letting you know some more details of my research.

Do you have a preference for chat software/facility? That might work best in terms of timescale. If there is anything to follow up afterwards, or ask a bit more detail about that could be done via email.

Best,

Wil

****

Wil Chivers

PhD Student (SOCSI)

Cardiff University

1-3 Museum Place

Cardiff

CF10 3BD

ChiversWG1@cardiff.ac.uk

Dear Max,

Thank you for your previous response - apologies I did not respond until now. The blurring of the boundary between public and private data is a working theory at the moment, although I do expect it to be of some use in framing my arguments. I see it as useful when thinking about the role that the Internet has come to play in resistance and also for considering the ways in which governments and state agencies interact with the public. For instance, the open data movement and how this could be said to represent a move towards making public what was previously private data. You are right to mention the idea of modern surveillance societies too which are in essence about collecting private data. The role of the Internet cannot be ignored here - much of the private data of interest to corporations and state departments is now volunteered by the public via social media and can be harvested relatively easily. On the reverse side, groups such as OpenLeaks and WikiLeaks demonstrate the ability to use the Internet to make private data public. As you can see, there is a lot here I am working through!

I haven't heard from Daniel yet - would it be possible for me to contact him directly? I notice on your original response his address was cc'd - is it possible to contact him on this address and if so should I do this via GPG?

Many thanks once again, all the best,

Wil

****

Wil Chivers

PhD Student (SOCSI)

Cardiff University

1-3 Museum Place

Cardiff

CF10 3BD

ChiversWG1@cardiff.ac.uk

On 2 Aug 2012, at 05:05, contact@openleaks.org wrote:

On Wed, Aug 01, 2012 at 11:52:53AM +0100, William Chivers wrote:

Dear Max,

Thanks for your response and comments and I look forward to hearing from Daniel.

I realise I may have been rather brief with the outline of my research and you are correct - it is a broad area - and I have begun to identify the substantive topics that will be the basis of my analyses. One such topic I am interested in bringing to bear on my research is the blurred boundary between public/private data in the modern era.
There may be some social phenomenon at work here, but in what way is the boundary between public and private now blurred? (Of course, this is the era of the modern surveillance state, which has already been on the rise for many decades and should be compared to what was going on pre-20th century.)

In respect of your last comment, I have come across GPG/OpenPGP before but as yet have not begun to use it (part of the problem with being a social science student as opposed to a computer science student is that it takes me rather longer to puzzle out the intricacies of certain pieces of software etc!) It is quite a steep learning curve. I do have an interest in this however and am starting to see where I can use measures to protect myself online - such as Tor for example.
So you see for yourself--- if you are confused, put yourself in the place of a potential whistle-blower, or social activist/revolutionary, or average bloke for that matter. At the same time digital and communications technology is becoming ubiquitously cheap and useful, it is not necessarily obvious how to use it properly and not put oneself at danger.

By the way, GPG is available at <http://www.gnupg.org>

Many thanks once again!

You are welcome

Regards,

Wil

****

Wil Chivers

PhD Student (SOCSI)

Cardiff University

1-3 Museum Place

Cardiff

CF10 3BD

APPENDIX E: LETTER TO JULIAN ASSANGE

Julian Assange
c/o The Embassy of Ecuador
Flat 3b, 3 Hans Crescent
London
SW1X 0LS

9th November 2012

Dear Mr. Assange,

I write to you to request the opportunity to meet with you at the Ecuadorian Embassy in London. I am a final year doctoral research student studying at the School of Social Sciences at Cardiff University. My PhD thesis is concerned with the interaction facilitated by the Internet between surveillance and resistance in contemporary society.

One aspect of my research is a case study of WikiLeaks. Your publications and efforts to reveal undemocratic and censored practices within powerful organisations from 2007 to the present day represent a form of resistance that has had an unprecedented impact. I have explored WikiLeaks in this context and naturally, given my substantive interest in surveillance studies, have been keen to investigate the impact of the publication of *The Spy Files* in 2011.

I have located several secondary sources of data that have allowed me to gain an insight into your motivations behind WikiLeaks in general and also for publishing specific documents (such as *The Spy Files*). I have already interviewed your former colleague Mr. Domscheit-Berg in relation to my research interests and have spoken with others who have worked with WikiLeaks over the years. However, it would add tremendous value to my research and would permit me to present a balanced argument if I could talk to you in person. My position is purely one of academic objectivity.

This letter represents my fourth attempt to make contact with you – two emails sent to the Embassy have not yet been met with a response and I yesterday visited Hans Crescent to no avail (I met someone from inside the Embassy who took my ID but informed me I could not come in to meet you). I am visiting London again on the weekend of the 16th-18th November and I will call at the Embassy again to request a meeting if I have not received a response in the meantime. Failing that I will formulate another approach – I am nothing if not determined. I have learned during the course of my research that you do not get anywhere without asking. In this case, I know I will not get anywhere if I do not continue asking.

I understand that your present situation may place demands on your time that are not compatible with granting requests from everyone who wishes to visit you. If you

think a visit in person is not possible, perhaps we could talk over the telephone instead? My contact details are listed below.

If we do not get the opportunity to talk, I hope for a speedy resolution to your predicament.

Yours sincerely,

Wil Chivers

1-3 Museum Place, Cardiff, CF10 3BT
Email: ChiversWG1@cardiff.ac.uk
Tel: (07920) 408064

At that time Assange had been in the Ecuadorian Embassy for approximately four months, having taken refuge there following an unsuccessful appeal against his extradition to Sweden. I was in London carrying out another two interviews ('Bert' and 'Ernie') and as I headed back towards Paddington it occurred to me that the Embassy, near Knightsbridge, was en route. I was curious to see the place and the extent of police presence and consequently made a beeline for Hans Crescent through the crowds of visitors to Harrods. Police were in evidence – although not to a huge extent – and it was this that made me decide to be proactive rather than wandering aimlessly up and down outside the embassy; I was unsure whether I was paranoid to suspect I could attract attention by my mere presence. Approaching the front door I spoke to the police officer on duty and asked if it would be possible for me to go inside to talk to Assange. Rather than denying the request, he seemed to find it amusing and went into the building reception to ask. At this point I was caught somewhat off guard, having not factored this in to my plans let alone considered it a possibility. The police officer beckoned me inside and I explained the situation to the receptionist. He asked whether I had an appointment or had contacted them prior to this – I said no, feeling a little less hopeful – but he nevertheless said 'well you never know' and went over to a large vault-like door. He knocked and told me they would be out in a moment. A second police officer was stationed at this entrance to the embassy and I struck up a conversation with him. He too found it amusing I was trying my luck but acknowledged the sense in my action: 'well you know he's not going anywhere!' Eventually the embassy door opened a crack. An Ecuadorian man peered around and asked what I wanted. I explained perhaps a little lamely that I wanted to come inside to talk to Assange about my research. He asked for my 'documents' and again feeling like I was unprepared handed him my university ID and driving license, instantly regretting handing these over as the door clicked shut. Several minutes later, the man reappeared and handed me my ID.

'No', he said bluntly.

'Could I make an appointment to come back?' I enquired.

‘No.’ The door shut.

Unproductive though it may have been, this was another enjoyable and formative experience. Moreover, it did not dissuade me from pursuing an interview with Assange. On returning to Cardiff, I wrote a formal letter to Assange outlining my desire to speak with him. I received no response to this and after a month of waiting I emailed The Sunshine Press (WikiLeaks’ official publishing name) instead. On Christmas Day, I received a response informing me Julian Assange was not giving any interviews at that time. Over the following months, I noticed Assange appearing infrequently in online news articles and videos and taking this as evidence he was actually willing to be contacted I set about a different route, drawing on my experience of contacting Daniel. I located an email address for Assange’s mother, Christine. Based in Assange’s native Australia, Christine Assange campaigns on Julian’s behalf for the appeal against his extradition. Christine kindly responded to my request, forwarding an email to Julian but informing me he received thousands of emails and not to be disappointed by any lack of reply. Once again The Sunshine Press responded in the same manner as before. I counted it as a battle well fought but ultimately doomed to failure.

APPENDIX G: THE PRIVACY ADVOCATES

The table below details some of the prominent organisations that featured in the network visualisations in Chapter Five. The information regarding the purpose and strategies of each organisation was drawn from their respective websites.

Organisation	Location/URL	Description/Philosophy/Strategies
American Civil Liberties Union (ACLU)	USA *aclu.org*	A nonpartisan, non-profit organization whose stated mission is "to defend and preserve the individual rights and liberties guaranteed to every person in this country by the Constitution and laws of the United States." It works through litigation, lobbying, and community empowerment. The ACLU has over 500,000 members and has annual budget of over $100 million.
Big Brother Watch	UK *bigbrotherwatch.org.uk*	Founded in 2009 with the intention of exposing the true scale of the surveillance state by challenging the policies which threaten privacy, freedoms and civil liberties. Big Brother Watch campaigns on behalf of the individual, to educate and encourage more control over personal data. We work to ensure that those who fail to respect our privacy, whether private companies, government departments or local authorities are held to account. We produce unique research that shines a light on the dramatic expansion of surveillance powers in the UK, the growth of the database state and the misuse of personal information.
Chaos Computer Club	Germany *ccc.de*	The Chaos Computer Club (CCC) is Europe's largest association of hackers. For more than thirty years we have provided information about technical and societal issues, such as surveillance, privacy, freedom of information, hacktivism, data security, technology and hacking issues. As the most influential hacker collective in Europe we organize campaigns, events, lobbying and publications as well as anonymizing services and communication infrastructure. Many hackerspaces in

		and around Germany which belong to or share a common bond to the CCC.
Don't Spy On Us[214]	UK *dontspyonus.org.uk*	*Don't Spy On Us* is a coalition of the most influential organisations who defend privacy, free expression and digital rights in the UK and in Europe. Don't Spy On Us is calling for an end to mass surveillance in line with our six principles. We want new legislation that will mean: surveillance is only targeted at those suspected of crimes; the security agencies are accountable to our elected representatives; and judges not politicians will decide when surveillance is justified.
Electronic Frontier Foundation (EFF)	USA *eff.org*	The Electronic Frontier Foundation is the leading non-profit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF uses the unique expertise of leading technologists, activists, and attorneys in our efforts to defend free speech online, fight illegal surveillance, advocate for users and innovators, and support freedom-enhancing technologies. Together, we forged a vast network of concerned members and partner organizations spanning the globe. EFF advises policymakers and educates the press and the public through comprehensive analysis, educational guides, activist workshops, and more. EFF empowers hundreds of thousands of individuals through our Action Center and has become a leading voice in online rights debates.
Electronic Privacy Information Center (EPIC)	USA *epic.org*	EPIC is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom

[214] Executive members: Article 19, Big Brother Watch, English PEN, Liberty, ORG, Privacy International. Affiliate members: Open Democracy, Public Concern at Work, Access Now, EFF, ifex, Index on Censorship, Fight for the Future, WWW Foundation, Open Media, Sum of Us, Centre for Investigative Journalism

		of expression, and democratic values in the information age. EPIC pursues a wide range of program activities including policy research, public education, conferences, litigation, publications, and advocacy. EPIC maintains one of the most popular privacy web sites in the world.
European Digital Rights Initiative[215] (EDRi)	Belgium *edri.org*	We are an association of civil and human rights organisations from across Europe. We defend rights and freedoms in the digital environment. We ensure that citizens' rights and freedoms in the online environment are respected whenever they are endangered by the actions of political bodies or private organisations. EDRi's key priorities for the next years are privacy, surveillance, net neutrality and copyright reform. EDRi distribute a fortnightly email newsletter to subscribers with news regarding privacy-related developments across Europe.
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIFF)	Germany *fiff.de*	We warn the public of developments in our field, which we believe are harmful; we fight against the use of information technology for control and surveillance; we are committed to a disarmament of computer science in military applications; we encourage the development of environmentally sustainable economic circuits using information technology; we are committed in design and use of information technology for the equality of persons with disabilities; we are working against the discrimination of women in science.

[215] Members: Access Now (International), Association for Technology and Internet (Romania), Article 19 (UK), ALCEI (Italy), Alternatif Bilişim Derneği (Alternatif Bilişim) (Turkey), Bits of Freedom (Netherlands), Chaos Computer Club (Germany), Digital Rights (Ireland), Digital Courage (formerly Foebud) (Germany), Digital Gesellschaft (Germany), DFRI (Sweden), Electronic Frontier Finland (Finland), Electronic Frontier Foundation (USA), Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (Germany), Foundation for Information Policy Research (UK), Förderverein Informationstechnik und Gesellschaft (FITUG e.V.) (Germany), Internet Society (Bulgaria), IT-Political Association of Denmark (Denmark), Iuridicum Remedium (Czech Republic), Initiative für Netzfreiheit (Austria), Liga voor Mensenrechten (Belgium), Metamorphosis (Macedonia), Modern Poland Foundation (Poland), Nodo50.org (Spain), Open Rights Group (UK), Panoptykon Foundation (Poland), Privacy International (UK), Quintessenz (Austria), Statewatch (UK), VIBE!AT (Austria), Vrijschrift (Netherlands).

Global Internet Liberties Campaign[216] (GILC)	International *gilc.org*	The member organizations of GILC have joined together to protect and promote fundamental human rights such as freedom of speech and the right of privacy on the net for users everywhere. GILC advocates: insisting that on-line free expression not be restricted by indirect means such as excessively restrictive governmental or private controls over computer hardware or software, telecommunications infrastructure, or other essential components of the Internet; ensuring that personal information generated on the global information infrastructure for one purpose is not used for an unrelated purpose or disclosed without the person's informed consent and enabling individuals to review personal information on the Internet and to correct inaccurate information; allowing on line users to encrypt their communications and information without restriction; and prohibiting prior censorship of on-line communication.
Liberty	UK *liberty-human-rights.org.uk*	Founded in 1934, we are a cross party, non-party membership organisation at the heart of the movement for fundamental rights and freedoms in the

[216] Members: ALCEI - Associazione per la Libertà nella Comunicazione Elettronica Interattiva; American Civil Liberties Union; Applied Research and Communications Fund; Arge Daten; Association des Utilisateurs d'Internet; Association Electronique Libre (AEL) ASBL; Association for Progressive Communications; Association pour la Promotion d'Internet en Polynésie Française; Bevcom Internet Technologies; Bits of Freedom; Bulgarian Institute for Legal Development; Buro Jansen & Janssen; Canadian Journalists for Free Expression; Campaign Against Censorship of the Internet in Britain; Center for Democracy and Technology; Chaos Computer Club; CITADEL-EF France; Committee to Protect Journalists; CommUnity - The Computer Communicators Association; Computer Professionals for Social Responsibility; CryptoRights Foundation; Cyber-Rights & Cyber-Liberties; CypherNet; Derechos Human Rights; Digital Freedom Network; Digital Rights; Equipo Nizkor; Electronic Frontiers Australia; Electronic Frontier Canada; Electronic Frontier Finland; Electronic Frontier Foundation; EFF-Austin; Electronic Privacy Information Center; Federation Nationale des Associations de Consommateurs du Quebec; Feminists Against Censorship; Forum InformatikerInnen fuer Frieden und gesellschaftliche Verantwortung (FIfF) e.V.; Förderverein Informationstechnik und Gesellschaft (FITUG); Foundation for Information Policy Research (FIPR); Human Rights Education Associates (HREA); Human Rights Network; Human Rights Watch; Hungarian Civil Liberties Union; Imaginons un Réseau Internet Solidaire (IRIS); Index on Censorship; Internet Freedom; Internet Society; Kriptopolis; Liberty (National Council of Civil Liberties); The Link Centre, Wits University; Netwokers against Surveillance Taskforce (NaST); NetAction; Online Policy Group; OpenNet; Open Society Institute; Peacefire; PEN American Center; Privacy International; Privacy Ukraine; Public Interest Advocacy Center, Ottawa; quintessenz; Reporters without borders (RSF); Singapore Internet Community (SInterCom); Statewatch; stop1984; Swiss Internet User Group (SIUG); Technika az Emberert Alapitvány (TEA); Verein für Internet Benutzer (VIBE!AT); XS4ALL Foundation.

		UK. We promote the values of individual human dignity, equal treatment and fairness as the foundations of a democratic society. Liberty campaigns to protect basic rights and freedoms through the courts, in Parliament and in the wider community. We do this through a combination of public campaigning, test case litigation, parliamentary work, policy analysis and the provision of free advice and information.
Open Rights Group (ORG)	UK *openrightsgroup.org*	Open Rights Group is the UK's only digital campaigning organisation working to protect the rights to privacy and free speech online. With almost 3,000 active supporters, we are a grassroots organisation with local groups across the UK. Digital technology has transformed the way we live and opened up limitless new ways to communicate, connect, share and learn across the world. But for all the benefits, technological developments have created new threats to our human rights. We raise awareness of these threats and challenge them through public campaigns, legal actions, policy interventions and tech projects. We campaign, lobby, go to court — whatever it takes to build and support a movement for freedom in the digital age. We believe in coalition, and work with partners across the political spectrum to support an informed population of Internet users who understand and fight for their rights in the digital age.
Privacy International	UK *privacyinternational.org*	Privacy International is committed to fighting for the right to privacy across the world. We investigate the secret world of government surveillance and expose the companies enabling it. We litigate to ensure that surveillance is consistent with the rule of law. We advocate for strong national, regional, and international laws that protect privacy. We conduct research to catalyse policy change. We raise awareness about

		technologies and laws that place privacy at risk, to ensure that the public is informed and engaged. Privacy International envisions a world in which the right to privacy is protected, respected, and fulfilled. Privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right.
Statewatch	UK	Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from 18 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe the fields of the state, justice and home affairs, civil liberties, accountability and openness. One of Statewatch's primary purposes is to provide a service for civil society to encourage informed discussion and debate - through the provision of news, features and analyses backed up by full-text documentation so that people can access for themselves primary sources and come to their own conclusions.

APPENDIX H: CATEGORISATION OF RESPONDENTS TO COMMUNICATIONS DATA BILL

Draft Communications Data Bill – Content Analysis Framework of Respondents

Total respondents: 145 (multiple responses combined)

Groups

- *Advocates/Non-Profits/Charities*
  - AVAAZ, Big Brother Watch, Caspar Bowden, Civil Liberties Organisations Letter, Demos, Foundation for Information Policy Research, Index on Censorship, Just West Yorkshire, JUSTICE, Liberty, No2ID, Open Rights Group, Public Concern at Work, Privacy International, The Tor Project, Wikimedia UK
- *Computer Science/IT Professionals*
  - Simon Adlem, Richard Ash, Steve Ball, Alex Burr, Alec Muffet, Zoe O'Connell, Marisha Ray, Robbie Simpson, Richard Smith, David Walker, Andrew Watson
- *Academics*
  - Prof. Ross Anderson FRS FREng, Dr Paul Bernal, Peter Buneman FRS FRSE & Michael Fourman FRSE FBCS, Clement Guitton, JANET, Prof. Robin Mansell, Dr Ashley Savage, Prof. Peter Sommer, Dr Eric Stoddart, Dr John Welford
- *Legal*
  - The Bar Council of England and Wales, Lord Carlile of Berriew, Crown Prosecution Service, The Law Society
- *IT Organisations*
  - BCS The Chartered Institute for IT, The Coalition for a Digital Economy, The Global Network Initiative
- *Governmental*
  - European Commission, Charles Farr, Home Office, Home Secretary Rt. Hon. Theresa May, Local Government Authority, Oliver Colville MP, Rt Hon David Willetts MP
- *Independent /Statutory/Public Authorities*
  - The Information Commissioner, Sir Paul Kennedy (Interception of Communications Commissioner), The Financial Services Authority, Equality and Human Rights Commission, National Anti-Fraud Network
- *Telecoms and Industry*

    - The Direct Marketing Association, ISPA, ITSPA, LINX, Telefonica UK Ltd, Three, Timico Ltd, Twitter Inc., Virgin Media, Vodafone, ADM Shine Technologies (Defence Research and Tech)
- *Policing and Law Enforcement*
    - National Crime Agency, SOCA, UK Border Agency, HM Revenue and Customs
- *News Media/Journalists/Authors*
    - Paul Bradshaw, Greg Callus, Glyn Moody, The Newspaper Society, Society of Editors, Robin Tudge
- *Individuals/Non-Professional*
    - Rodney Aistrop, Nathan Allonby, Martin Ammann, Daniel Beckett, Mark Benson, Jonathan Birkitt, Robert M K Brereton, Graeme Carter, Sean Cheshire, Wendy Cockroft, Paul Connolly, Roger H Cook, Joe Corrall, Ray Corrigan, Simon Cramp, Mr P Cromie, Patrick Cunningham, Chris Davey, N Dove, Mark Drury, Keith Edkins, Bruce Elliot, Cliff Fowkes, Thomas Frampton, Mike Gerbrais, Y Guinan, William Heath, Roger Heathcote, George Hoggarth, Lucian Holland, Dr Dominic Jackson, Andrew James, Peter John, Lisa Kavanagh, J R S Kistruck, George Lawrence, Stacey Leigh Ross, Sorcha Lenagh, George Logan, Alastair Macmillan, P Main, Awad Mackie, Peter Marcham, Lorna Mitchell, Barbara Moody, Giles Murchiston, Jim Nash, M Neal, Richard Owens, Anne Palmer, Charlie Pearce, George Pender, J Richardson, Duncan Roy, Dr Peter Saul, Robert Smith, Robert Stirrups, Steven Taylor, Ernest F Thornton, Montgomery Vaughan, Phil Vellender, David Walter, J Wheeler, S Wheeler, Nic Wisttreich, Ben Woodling, Andy Wrigley, T Wright

FINAL 7 CATEGORIES

- **OFFICIAL** (11)
    - *Government (7):* European Commission, Charles Farr, Home Office, Home Secretary Rt. Hon. Theresa May, Local Government Authority, Oliver Colville MP, Rt Hon David Willetts MP
    - *Policing/Law Enforcement (4):* National Crime Agency, SOCA, UK Border Agency, HM Revenue and Customs
- **INDEPENDENT AUTHORITIES** (5): The Information Commissioner, Sir Paul Kennedy (Interception of Communications Commissioner), The Financial Services Authority, Equality and Human Rights Commission, National Anti-Fraud Network

- **TELECOMS INDUSTRY** (11): The Direct Marketing Association, ISPA, ITSPA, LINX, Telefonica UK Ltd, Three, Timico Ltd, Twitter Inc., Virgin Media, Vodafone, ADM Shine Technologies
- **EXPERT** (28):
    - *Technical (Individual and Organisational) (14):* Simon Adlem, Richard Ash, Steve Ball, Alex Burr, Alec Muffet, Zoe O'Connell, Marisha Ray, Robbie Simpson, Richard Smith, David Walker, Andrew Watson, BCS The Chartered Institute for IT, The Coalition for a Digital Economy, The Global Network Initiative
    - *Academic (10):* Prof. Ross Anderson FRS FREng, Dr Paul Bernal, Peter Buneman FRS FRSE & Michael Fourman FRSE FBCS, Clement Guitton, JANET, Prof. Robin Mansell, Dr Ashley Savage, Prof. Peter Sommer, Dr Eric Stoddart, Dr John Welford
    - *Legal (4):* The Bar Council of England and Wales, Lord Carlile of Berriew, Crown Prosecution Service, The Law Society
- **ADVOCACY/NON-PROFIT** (16): AVAAZ, Big Brother Watch, Caspar Bowden, Civil Liberties Organisations Letter, Demos, Foundation for Information Policy Research, Index on Censorship, Just West Yorkshire, JUSTICE, Liberty, No2ID, Open Rights Group, Public Concern at Work, Privacy International, The Tor Project, Wikimedia UK
- **MEDIA** (6): Paul Bradshaw, Greg Callus, Glyn Moody, The Newspaper Society, Society of Editors, Robin Tudge
- **INDIVIDUAL/NON-EXPERT** (68): Rodney Aistrop, Nathan Allonby, Martin Ammann, Daniel Beckett, Mark Benson, Jonathan Birkitt, Robert M K Brereton, Graeme Carter, Sean Cheshire, Wendy Cockroft, Paul Connolly, Roger H Cook, Joe Corrall, Ray Corrigan, Simon Cramp, Mr P Cromie, Patrick Cunningham, Chris Davey, N Dove, Mark Drury, Keith Edkins, Bruce Elliot, Cliff Fowkes, Thomas Frampton, Mike Gerbrais, Y Guinan, William Heath, Roger Heathcote, George Hoggarth, Lucian Holland, Dr Dominic Jackson, Andrew James, Peter John, Lisa Kavanagh, J R S Kistruck, George Lawrence, Stacey Leigh Ross, Sorcha Lenagh, George Logan, Alastair Macmillan, P Main, Awad Mackie, Peter Marcham, Lorna Mitchell, Barbara Moore, Giles Murchiston, Jim Nash, M Neal, Richard Owens, Anne Palmer, Charlie Pearce, George Pender, J Richardson, Duncan Roy, Dr Peter Saul, Robert Smith, Robert Stirrups, Steven Taylor, Ernest F Thornton, Montgomery Vaughan, Phil Vellender, David Walter, J Wheeler, S Wheeler, Nic Wisttreich, Ben Woodling, Andy Wrigley, T Wright

Government and law enforcement emphasised a 'capabilities gap' in their ability to effectively obtain and utilise communications data. Their framing of the problem was therefore that technological advances had made previous regulation defunct. The accuracy of government estimates of inaccessible data was contested by opponents of the CDB in a number of sessions but in general the data required were of three kinds: IP resolution, weblog data and third-party communication data.

Evidence provided by law enforcement was largely uniform in three respects: current oversight is satisfactory and comprehensive; communications data has been crucial in a large number of investigations and; requests for data are always assessed in terms of necessity, proportionality and 'collateral intrusion'. The theme of keeping pace with technological developments was echoed from law enforcement respondents; both HMRC and SOCA (CDB Written Evidence, pp.260 and 518) did not see the Bill as granting 'new powers', rather updating current capabilities[217]. SOCA added that a resultant rebalancing of civil liberties was unnecessary as effective investigation of crime itself safeguards civil liberties – Agamben's (2005) state of exception in practice. Obtaining communications data was framed as the least intrusive of a range of investigatory powers; other methods were equated with greater intrusion and more time and expense[218].

TELECOMS INDUSTRY

While acknowledging the need to adapt to a new technological environment, telecoms representatives (i.e. the vital private sector collaborators) were critical insofar as the Bill lacked precision. It presented several problems in need of addressing: security and feasibility of the data processing arrangements; the potential for overlap/disjoint with existing UK and European data protection and retention regulation and; problems related to the retention of third-party data (both the jurisdictional aspect to this and the possibility of damaging commercial

[217] SOCA outlined a 'Day in the Life' scenario to illustrate the reasons why current capabilities are insufficient because of the variety of communications an individual engages in on a daily basis (CDB Written Evidence, pp.521-22). While enlightening, it was arguably the case that just such an example was indicative of the concerns other individuals may have had about the personal detail access to communications data can reveal (see Section 6.4).

[218] See UK Border Agency (CDB Written Evidence, p.572)

relationships). Thus while current regulation was framed as having shortcomings in the technological environment, the proposals in the CDB over-played the government's hand. Communications enterprises will be fully aware of the value of the data they can retain but also of their obligations to service users. These organisations inhabit a messy, trans-jurisdictional regulatory domain and so their resistance to the CDB is understandable; any developments affecting their role as data intermediaries must be carefully negotiated. Private corporations' resistance to mediation is an important outcome from these findings. In future, advocates might benefit from nurturing relationships with private corporations given their capability to counteract government surveillance developments. Of course this will be difficult to manage given the simultaneous positioning of CSPs and their ilk as powerful surveillance agents in their own right.

ADVOCACY/NON-PROFIT

As expected, there was a high degree of collaboration between these organisations as well as consultation with expert advisors. On a formal level, a joint letter was submitted to the Committee whilst behind the scenes, a strategic approach was adopted to ensure maximum impact. Consequently, the written evidence provided by the advocacy community was comprehensive and spoke to all of the themes drawn out above. Supplementary to this, the Open Rights Group and 38 Degrees actively encouraged their member base to sign online petitions and send emails to their local MPs and the Joint Committee expressing dissatisfaction with the Bill. The result was a petition[219] signed by just under 200,000 people and 19,000 pre-written emails[220] to the Joint Committee. This category of respondents thus demonstrated a strong presence in the debate, directly and indirectly.

INDIVIDUAL/NON-EXPERT

Individuals/non-experts accounted for the majority (26%) of written evidence submitted to the consultation. Moreover, combined with the overwhelming number of emails sent at the behest of the ORG and 38 Degrees, the scale of public

[219] https://secure.38degrees.org.uk/page/s/stop-government-snooping#petition
[220] http://blog.38degrees.org.uk/2012/09/12/snooping-our-voices-have-been-heard/

disquiet about the CDB cannot have failed to draw the attention of the Joint Committee. Although the emails were unpublished, the Committee issued a summary[221] which stated that 'we have not seen a single email supporting the draft Communications Data Bill, or even agreeing that there may be a case for the security services and law enforcement agencies having greater access to communications data than they do at present.' While some of those who sent emails added their own arguments, others copied extracts verbatim from Liberty's website. There was to some extent, therefore, a blurring between the opinions of individual respondents and those of advocacy groups. Nevertheless, we should overlook neither the role that individuals played in shaping the general nature of the response to the CDB, nor the level of engagement they displayed. As the findings showed, it is at the individual level where popular constructions of surveillance take root. Consequently, it is perhaps by examining individual attitudes towards regulation of surveillance that we can best appreciate how persuasive official justifications for extended surveillance are.

[221] http://www.parliament.uk/documents/joint-committees/communications-data/Written%20evidence%20-%20summary%20of%20chain%20emails.pdf

APPENDIX I: JOHN PERRY BARLOW'S DECLARATION ON THE INDEPENDENCE OF CYBERSPACE

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract . This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the

commonweal, our governance will emerge . Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

Davos, Switzerland

February 8, 1996